LOCKSPORT

A HACKER'S GUIDE TO LOCKPICKING, IMPRESSIONING, AND SAFE CRACKING

JOS WEYERS, MATT BURROUGH, WALTER BELGERS, BandEAtoZ, AND NIGEL K. TOLLEY

no starch press

PRAISE FOR *LOCKSPORT*

"A comprehensive overview of everything there is to know about the emerging hobby known as locksport. . . . Highly recommended!"

—ANTHONY THOMPSON, *THE LOCK SPORTSCAST*

"Locksport is a shared passion; a community of knowledge, collaboration, and celebration of achievement. This fantastic book embodies that spirit, with some of the most influential and respected people in the locksport community."

—LOCK NOOB, YOUTUBE.COM/LOCKNOOB

"How to succeed in Locksport 101."

—LOCKPICKINGDEV

LOCKSPORT

A Hacker's Guide to Lockpicking, Impressioning, and Safe Cracking

Jos Weyers, Matt Burrough, Walter Belgers, BandEAtoZ, and Nigel K. Tolley

no starch press®

San Francisco

First printing

28 27 26 25 24   1 2 3 4 5

ISBN-13: 978-1-7185-0224-6 (print)
ISBN-13: 978-1-7185-0225-3 (ebook)

Published by No Starch Press®, Inc.
245 8th Street, San Francisco, CA 94103
phone: +1.415.863.9900
www.nostarch.com; info@nostarch.com

Publisher: William Pollock
Managing Editor: Jill Franklin
Production Manager: Sabrina Plomitallo-González
Production Editor: Jennifer Kepler
Developmental Editor: Rachel Monaghan
Cover Illustrator: Gina Redman
Interior Design: Octopod Studios; SPG
Technical Reviewer: Peter South
Copyeditor: Sharon Wilkey
Proofreader: Liz Wheeler

Library of Congress Control Number: 2023030099

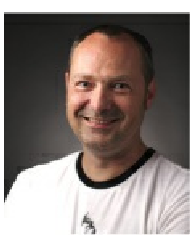
For customer service inquiries, please contact info@nostarch.com. For information on distribution, bulk sales, corporate sales, or translations: sales@nostarch.com. For permission to translate this work: rights@nostarch.com. To report counterfeit copies or piracy: counterfeit@nostarch.com.

Dedicated to all lockpickers past, present, and future.
You are our hacker family.

About the Authors

Jos Weyers is a world-record holder in the field of lock impressioning and a mainstay participant at locksport events around the world. Jos is president of TOOOL (The Open Organisation of Lockpickers) in the Netherlands, a key figure at the Hack42 hackerspace in Arnhem, and the mastermind behind the beehive42.org initiative. Sometimes known as the "Dutch kilt guy," he's been featured in the *New York Times* and was voted #2 in the Hackers and Security category of the *Vrij Nederland* Nerd 101 list in June 2015.

Matt Burrough is a devoted locksport hobbyist who has competed multiple times at TOOOL NL's LockCon, TOOOL US's LockFest, and the ShmooCon Lockpick Village. He also co-leads the Seattle Locksport group. During the day, Matt manages a professional red team. He holds a bachelor's degree in networking, security, and system administration; a master's degree in computer science; and a variety of industry certifications from GIAC (SANS), Microsoft, and Offensive Security. He is the author of *Pentesting Azure Applications* (No Starch Press, 2018).



Walter Belgers is a former president and honorary member of TOOOL. He got involved in locksport over 25 years ago. He has held many physical security lectures and workshops over the decades and has won competitions in several countries in several disciplines. Walter holds a master's degree in computing science and is a professional hacker, testing computers, humans, and physical devices. In his free time, he enjoys drifting and rally driving, sailing, reading, traveling, and photography.

BandEAtoZ is a GSA-certified safe technician with years of experience opening safes around the world. He regularly publishes articles of interest in the locksmithing magazines *Keynotes* and *Safe & Vault Technology*. He is an active member in the Safe and Vault Technicians Association, the National Safeman's Organization, and numerous professional forums.

Nigel K. Tolley was picking locks and subverting security as a schoolboy, long before he had ever heard of locksmiths or locksport. As a locksmith for over 17 years, he has taught thousands to pick locks, including many other locksmiths. Nigel has presented at corporate icebreaker events, lock meetups, and everything in between. He has also consulted with lock manufacturers and designers and found many exploits for physical security devices. He is a dedicated maker of many things, especially tools.

About the Technical Reviewer

Peter South (aka yakMedic) began his journey into the world of lockpicking at an early age, shortly after downloading an ASCII-illustrated lockpicking guide from a BBS (bulletin board system). He was able to pick his first lock with homemade tools. After a career in public service, he moved to the Seattle area, became involved with Seattle Locksport, and began working as a locksmith specializing in high-security locks. He has been a speaker at BSides Seattle, DEF CON LPV (Lockpick Village), and the Infosec Campout. In addition, he has done virtual locksport presentations on safe manipulation and lock impressioning for ShellCon and LayerOne. Historically, he's been spotted working the LPVs at HushCon, DEF CON, ShellCon, BlueHat, Disobey, and BSides Seattle. He's currently the co-leader of Seattle Locksport.

BRIEF CONTENTS

CONTENTS IN DETAIL

PART III: IMPRESSIONING

Other Books and Papers

INDEX

ACKNOWLEDGMENTS

We would like to thank our families for their support, patience, and love as we worked through writing and editing this work. We'd also like to thank all our friends in the locksport community who have competed with us, advised us, or shared stories with us over a beer or Club-Mate. There are too many of you to name, but we appreciate each and every one of you, and we look forward to seeing you at the next competition!

INTRODUCTION

Back in 2011 at the No Starch booth at DEF CON, Bill Pollock asked me if I would be interested in writing a book about lockpicking. Knowing full well my ego would agree wholeheartedly to having my name on a bookshelf, I still respectfully declined. What could I possibly bring to the table that hasn't been said already? Several books on lockpicking already exist, and other publications can be found online.

Fast-forward to the world in quarantine mode. In a virtual lockpick meetup spanning three continents (and even more time zones) that Matt organized, we began discussing books. Matt had recently published a wonderful book with No Starch, *Pentesting Azure Applications*, and they would be happy to have him write another—maybe on lockpicking this time? While we were discussing this informally, we quickly noticed that our group included several experts in various lockpicking fields, and suggestions for chapters kept pouring in.

But still, why a new book? When BandEAtoZ suggested it should be a group effort on locksport specifically, something clicked. Yes, lockpicking and impressioning information is out there, but nothing has really focused on the *sport* aspect. Books on lockpicking or covert entry often overlook information that is critical to competing in locksport competitions. Locksmithing references tend to concentrate on minutiae that is irrelevant to hobbyists.

That's where this book comes in. We've gathered a group of rock stars from the world of locksport, each with our own area of expertise.

—Jos Weyers

Locksport Origin Stories

Every locksporter has a different reason why they became interested in this rather unique hobby. Your reason might be that you saw lockpicking on YouTube and thought it looked fun. Maybe you are a locksmith and decided to see if you were the fastest person in your shop to open a lock, or maybe you ran into one of us at a conference and spent some time learning to open locks. Lockpicking is a superpower, and just like comic book heroes, your reason for joining this community is your *origin story*. We wanted to share ours with you.

Jos Weyers

Since a very young age, I have been curious about all things mechanical. I ruined a multitude of alarm clocks in the process of figuring out their inner workings. Recently, I progressed to doing the very same with way more expensive wristwatches. (Apparently, some kids never learn.)

Jos taking care of someone's browser history. Photo by Dennis van Zuijlekom (CC BY-SA 2.0).

Being technically schooled in IT, I gravitated toward learning how to secure all the cyberz. With that interest in mind, I visited several of the Dutch, open-air hacker camps, where I was first introduced to the concept of locksport. This, of course, reignited my interest in physical things that shouldn't be tinkered with and therefore shall be tinkered with. Buying gear on the internet wasn't really a thing in those days, so being able to buy an actual lockpick set at these events was a very welcome concept.

After opening a serious number of locks, I came across a simple padlock that just wouldn't budge (I hadn't yet heard about the wonders of security pins). Rather intrigued with this little puzzle, I decided to visit a TOOOL meeting to get some tips and tricks. They can't get rid of me . . . and that was almost 20 years ago.

During that time frame, I was elected board member and president of TOOOL, won more than a dozen championships impressioning keys, organized several LockCons, tried to buy an actual panopticon prison, lectured rather frequently about physical security and how it relates to the cyber domain, and figured out a new and novel way to easily circumvent most master-key systems by using just one key.

When I am not hosting impressioning workshops somewhere on this globe, I can frequently be found in Arnhem, Netherlands, at Hack42, generally considered to be the most awesome hackerspace in existence.

And yes, I'm devilishly handsome.

Matt Burrough

When I was growing up, Ian Fleming's novels were my guilty pleasure. After completing the assigned reading for English class, I'd often grab whatever James Bond novel I had borrowed from the library out of the bottom of my backpack and escape into a world of espionage. While a cool-under-pressure spy who makes women swoon is an obvious and perhaps cliché choice for a hero as a teenage boy, I appreciated Fleming's work for two other reasons: the tradecraft and the gadgets.

I loved finding bits of tradecraft—spy tricks and methods—in the books. These details elevated the books for me from mere pulp fiction to a new way of thinking about how things in the world are not always what they first appear. Of course, I was also fascinated by the gadgets on which 007 relied and was amused seeing which of these fictionized implements had made it into real, everyday devices some four or five decades after they appeared in print. This curiosity dovetailed nicely with my interest in all things tech related.

Despite my love of these books, alas I was not cut from the right cloth to be a spy. Instead, I focused on my infatuation with technology and pursued a career in information technology.

A few years after college, I was invited to attend my first ShmooCon by a friend who lived in Washington, DC, where I encountered my first real-life lockpicks at the TOOOL lockpick village. As fun as it was popping open my first Master Lock without a key and feeling a bit Bond-like, I left the lockpicks at the conference and returned to my typical tech-worker life.

It wasn't until I pivoted my career into cybersecurity several years later that I dove headfirst into the world of locksport. Shortly after I joined a red team, a fellow penetration tester invited me to a small lunchtime demonstration he had arranged in the office. Visiting Seattle from the Netherlands was Jos Weyers, who was accompanied by locksmith and locksporter Holly Poer. The two taught several of us how to pick locks, and it was then that I bought my first set of picks from Jos. That week, I attended a lock impressioning class taught by Jos and Holly at a local hackerspace and was hooked.

This was fantastic—as a penetration tester, I had a career that not only allowed but also encouraged me to use these newfound skills to gain access to rooms or computers that were locked away. I finally got to use the Bond skills I most admired.


Matt impressioning a lock during competition at LockCon. Photo by Dennis van Zuijlekom (CC BY-SA 2.0).

From that point on, I attended every locksport meetup and conference I could. I enjoyed placing in contests and learning new opening techniques and about different locks I had never seen before. But even better, I got to befriend some of the most talented, most interesting, and friendliest people I've ever met. I hope our hobby brings you as much joy as it has me.

Walter Belgers

I believe hackers are born that way. I certainly was. I wanted to know how everything worked from as far back as I can remember. Technology has always had my interest, and keys too. After visiting my grandparents, we would get a call asking if I'd taken some keys. I did take them. I was four.

Walter competing in an impressioning championship. Photo by Dennis van Zuijlekom (CC BY-SA 2.0).

In 1980, I spent a vacation with an Exidy Sorcerer computer my dad had taken home from work, writing programs in BASIC with my older brother. The first English words I learned were BASIC commands. The computer was magical to me and a great opportunity to learn. Three years later, I had convinced my parents to buy me a home computer.

I learned a ton just by reading and trying out stuff. Things got really interesting when I went to college, where I was introduced to UNIX and got access to the internet when just 100,000 academic computers were connected. The internet opened up a whole new world to explore. I became a computer hacker. No computer crime laws existed yet.

Several hacker groups were around that were abiding by the "hacker ethos." I felt at home in these groups and read everything I could. *Phrack* magazine was the leading hacker e-zine, and in the Netherlands, we had *Hack-Tic* magazine. In it, I read about lockpicking (which is just hacking locks, if you ask me) for the first time. Online shops or the World Wide Web did not yet exist, so I couldn't buy tools. I tried to make my own but failed to open anything. I got so frustrated that I stopped trying.

I have been going to real-life hacker conventions since that time, the first ones being Hacking at the End of the Universe in the Netherlands in 1993 and Access All Areas in London in 1995. Many would follow. In 1997, I did my first real lockpicking at the Hacking in Progress event, also in the Netherlands. Finally, I had success, and I was hooked! I became a member of the newly founded Dutch lockpicking group and later started a chapter in my hometown, which I still lead 15 years later.

Meanwhile, I got a few jobs in IT security. I eventually joined friends to run our own penetration testing company. I could finally hack again, to improve the security posture of our clients. I also did social engineering and physical penetration testing assignments in which I picked locks guarding critical infrastructure. In the true hacker ethos, I gave back to the community by sharing knowledge at conferences, and I have spoken at a few hundred over the years.

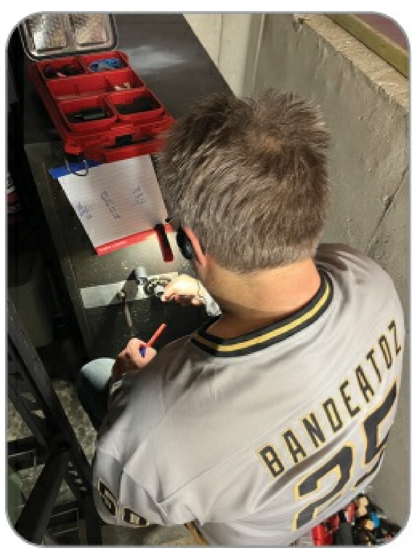
I have stayed a member of the Dutch lockpicking group ever since its conception, eventually becoming president. I have been involved in organizing LockCons and am very proud of getting Tim Jenkin, who picked his way out of a South African jail, to speak at one a few years back. During these events, I've learned impressioning, lever lockpicking, and safe cracking. It is with pride that I now share, together with my friends, my knowledge of lockpicking with you in this book. I hope that you, in turn, will pass on the knowledge you gather in your journey.

BandEAtoZ

I've been a longtime professional breaker of things, and locks have always been paramount in that mix. Sometimes finesse is best applied instead of brute force, and locks often provide the opportunity to apply that finesse. Automotive and heavy machinery is where I cut my teeth with picking, but it didn't take long to add other locks to my skill set. My initial foray into opening a safe deserves a story in itself, but that is for another time.

After more than 20 years in the safe-technician field, I was attending some required professional development classes when I first listened to a few of the instructors bad-mouthing lockpickers on the internet. All the typical complaints, including revealing industry insider secrets, teaching criminals, and using only fake locks, were brandished about.

The thing was, I had long been watching very competent locksporters crush difficult locks and knew these curmudgeons' arguments were full of hot air. I sensed that the idea of non-locksmiths wanting to fuss with locks absolutely didn't compute in their minds. They didn't see locks as the wonderfully engineered puzzles that they are. Their loss.



BandEAtoZ manipulating a safe lock in the wild. Small indications made this a slow and deliberate opening.

While I would love to expound on my numerous locksport interactions over the years, I am authoring this under a pseudonym in an attempt to keep me from losing access to the safe-technician cool kids club, which is still populated with many who believe that even an unauthorized gaze at a safe lock is tantamount to heresy and worth a burning at the stake. This kerfuffle over technicians' concerns about security is still in full force despite 80 years of these common safe-manipulation techniques being prolific in print, the hundreds of videos available online, and more importantly, the continued improvements to locks that make these techniques virtually impossible.

So, after a handful of years skulking in the back of locksport meetings, I am now tiptoeing out. A bit.

Nigel K. Tolley

What was the first lock I picked? I'm not completely sure, but I have at least three memories of picking locks from my childhood.

There was an old vending machine for hot drinks at my dad's workshop. One day I watched an employee pull out some tools, jiggle something in the lock, and open the machine. He took out one of the 10-pence coins and inserted it into the coin slot to buy himself a drink. Intrigued partly by his alarm at realizing I had seen what he'd done, I investigated the lock and soon found I could do the same by using the plastic coffee stirrers.

I like to think that was the first lock that I picked, but there are other possibilities from around the same time. I had a younger brother, so I put a bolt on my bedroom door and a padlock on my shed. (Yes, I had my own shed! It probably explains a lot.) It was a cheap padlock, and I was lazy, so I quickly got into the habit of picking the lock rather than walking all the way into the house to get the key. I recall picking it open many, many times. With what tool, I have no idea—probably something I made in my dad's workshop.

Nigel in his workshop. Photo by Morgan Tolley, 2021.

Around that same time, my school got new computer equipment, which was stored inside our school desk drawers. One day I watched a handyman installing the little "locks" I now know to be nothing more than a star key driving a bolt, designed for windows. After he had finished installing the lock on my desk, I asked what he was doing, and he told me he was adding locks so we couldn't play with the equipment. I picked up his Phillips screwdriver and unlocked the drawer. His jaw dropped. I can only hope, looking back, that he was a handyman and not a locksmith.

I continued playing with locks over the next couple of decades, through university and a short career in aerospace, eventually starting up a locksmithing business in 2005, the same year that I first went to a TOOOL event—the Dutch national lockpicking championships at a hacker camp. I've never looked back.

The tiny niche of physical security (PhySec) is still, once you look closely, a vast, vast arena with a thousand genuine niche disciplines. Rarely do I see the same thing twice. In addition to locks, I cover alarms and CCTV, plus some aspects of information security (InfoSec)—primarily testing Internet of Things (IoT) devices for physical attack vectors. I have advised on books and film and have appeared on TV. I've created new CAD methods for copying the largest antique keys, and I've worked on photogrammetry methods for copying modern restricted keys. I've designed and sold several locksmith tools, one of which I bothered to patent and a few of which I've managed to sell to other companies. I have seen much more than just lever locks in my day-to-day work: everything people have made and fitted over hundreds of years on everything from cars to vaults, castles to mobile homes, including more than a few custom creations by aspiring lock designers, well-known manufacturers, and even drug dealers!

I've recently relocated; it will be interesting to see what challenges the doors of my new home, Edinburgh, Scotland, bring.

How This Book Is Organized

The book is divided into parts that focus on various types of competitions found in locksport championships. In each part, we describe how to get started, what tools you'll need, how to progress from beginner to advanced, and what to expect in a competition setting. If you're new to picking locks, we suggest reading the parts in order, but more advanced locksporters should feel free to jump to a part that most interests them.

Part I: The Basics (Chapters 1–5) This part introduces you to the world of locksport, starting with the history of lockpicking and a thorough description of various competitions around the globe, the groups that host them, and the laws that govern the sport. Then you'll learn about types of locks; their inner mechanisms and high-security elements; and how to disassemble, troubleshoot, and maintain your practice locks.

Part II: Pin Tumbler Lockpicking (Chapters 6–8) This first hands-on part of the book focuses on pin tumbler locks, the most common and budget-friendly type and thus a good introduction to locksport. You'll see several models and learn how to work around various security elements. We'll take a brief look in Chapter 7 at a few locks other than the standard pin tumbler, but the principles of picking them remain largely the same.

Part III: Impressioning (Chapters 9–11) In this part, we'll turn to impressioning, the art of fashioning a working key from a blank by reading marks made by the lock. Once a common skill among locksmiths, impressioning is now rarely used in the field, but it has gained in popularity since its arrival on the locksport scene in the early 2000s.

Part IV: Safe-Lock Manipulation (Chapters 12–14) The focus of this part is manipulating safe locks, a much more detailed and nuanced process than spy movies would have you believe. You'll learn all about how to get feedback from safe locks, chart the clues you find, and zero in on the lock's combination.

Part V: Lever Lockpicking (Chapters 15–17) In this final hands-on part, we'll explore the lever lock, an old but sophisticated lock style found primarily in the UK and mainland Europe. You'll see many examples of intricate key and lock designs and then apply much of the knowledge you acquired in previous chapters to manipulate levers instead of pins in order to open these locks.

Appendixes Two appendixes close out the book. The first covers locksport games and events not included in their respective sections, and the second tells where to source lockpicking supplies in your area.

Who This Book Is For

This book is intended for anyone with an interest in locksport. Those who are just starting will learn the basics, such as tools and techniques to use. Seasoned lockpickers who are not yet competing will get information about how competitions are organized, where they are held, and how to perform well at them. Experienced locksporters will probably also learn something new, as this book covers the four main fields in locksport: picking cylinders, impressioning cylinders, opening combination safe locks, and opening lever locks.

Regardless of your level of experience, the tools and techniques described in this book are intended solely for the purposes of locksport. We'll detail the rules and laws surrounding lockpicking in Chapter 1, but it's worth stating now that you should pick only locks that you own and only according to the laws of your particular area.

Now, without further ado, let's get started!

PART I

THE BASICS

Welcome to the world of locksport! We're excited to have you join the global family of people who see locks as a puzzle to be solved. It is our sincere hope that you find our hobby as entertaining as we do, and that one day you might join us at a local meetup or even an international competition!

This section will provide you with a strong foundation on which to build your lock-opening skills. We'll start with a look at where locksport began, as well as current groups you can join and the locksport rules and local laws you should be aware of as you get started. From there, we'll cover what makes a lock click, components of locks that make them harder or easier to pick, and finally, how to disassemble, reassemble, and care for the locks in your collection. It's going to be a fun ride; let's get going!

1
THE WORLD OF LOCKSPORT

When was the first time you saw someone pick a lock? Perhaps it was in a spy movie. Maybe you stumbled upon a YouTuber talking through the process. Or maybe you happened upon a lockpick village at a hacker conference. Regardless of where it was, you probably felt some mix of excitement, intrigue, and perhaps skepticism. For some of us, these feelings led to pursuing lockpicking for fun, which turned into a hobby, and that hobby became a sport.

Locksport is the nondestructive opening of locks in ways the manufacturer never intended. We use this term to describe both the hobby of opening locks and the competitions to see who can do so the fastest. While *lockpicking* is the best-known form of locksport, the sport includes other types of lock opening, such as *impressioning* (creating a working key for a lock without access to or knowledge of the original) and *safe-lock manipulation*, or *safe cracking* (determining a safe's combination based on feedback from the safe's dial).

The goal of this book is to teach you the basics of these techniques and then ramp up your skills until you're ready to participate in locksport competitions.

The History of Locksport

Lockpicking has a long history, but in the days before the World Wide Web, it was hard to get information about it, much less find the tools. Lockpicking was known in the world of locksmiths, but they preferred not to talk about it to outsiders.

> When I started lockpicking, I talked about it with my local locksmith, Mr. de Kok. He was very reluctant to discuss the subject. Mr. de Kok sold Mul-T-Lock cylinders that he assembled himself. Sometimes he would make a mistake, leaving him with unusable cylinders. Only after I started picking them open for him so he could reuse the parts did he start slowly opening up to me, revealing that he knew about lockpicking and had tried it himself. Still, he'd only talk about it when no other customers were in his shop.
>
> —WALTER

In the 1980s and 1990s, you could find a few resources on lockpicking if you knew where to look. One early example was Ted the Tool's 1991 paper "The MIT Guide to Lockpicking," a nicely illustrated guide that was many people's introduction to lockpicking and that has now been translated into many languages. A few lockpicking books were available, such as those written by Eddie the Wire (it seems you need a pseudonym to write about lockpicking) and published by Loompanics Unlimited, a US book seller specializing in other controversial topics such as weapons, anarchism, and sex. Eddie's introduction to *The Complete Guide to Lock Picking* (1981) reads, "When Eddie the Wire was twelve, his dad gave him three padlocks and no keys. The resulting frustration of a twelve-year-old led to Eddie's early interest in escape artists, locks, and picks." Eddie must have been that age sometime in the 1960s. One can only guess where he got his information, if he didn't figure it all out himself.

Even earlier, lockpicking was studied by the Tech Model Railroad Club (TMRC), founded at the Massachusetts Institute of Technology (MIT) in 1946. The group's interests encompassed more than just railroads; members also investigated computers, radios, and phone systems. They also liked *roof and tunnel hacking*, which sometimes involved lockpicking or lock bypassing. One TMRC member was theoretical physicist Richard Feynman, who, later in his career at the Los Alamos National Laboratory, opened colleagues' safe locks as a hobby. Truth be told, this was more a matter of smart tricks and social engineering than actual lock manipulation. He describes his safe-cracking adventures vividly in his autobiography *Surely You're Joking, Mr. Feynman!* (W.W. Norton, 1985).

Hacker culture is the legacy of the TMRC, and lockpicking can be seen as a type of hacking: the intellectual challenge of opening a lock in a way that the manufacturer hadn't envisioned. Hacker culture thrives today, and many cities now have their own hackerspaces where you'll find curious people with an interest in technology, art, science, and more. It's no wonder that quite a few people who visit hackerspaces are also interested in lockpicking.

It's hard to know what those in the lock industry knew of lockpicking prior to those early documents, but old patents on lockpicking tools might give us a clue. Take the *pick gun*: a gun-shaped device to quickly open locks (we'll talk more about this tool in Part II). Figure 1-1 shows its patent from 1943. Those in the lock industry have known for a long time about the pick gun, but it took many decades to become public knowledge.

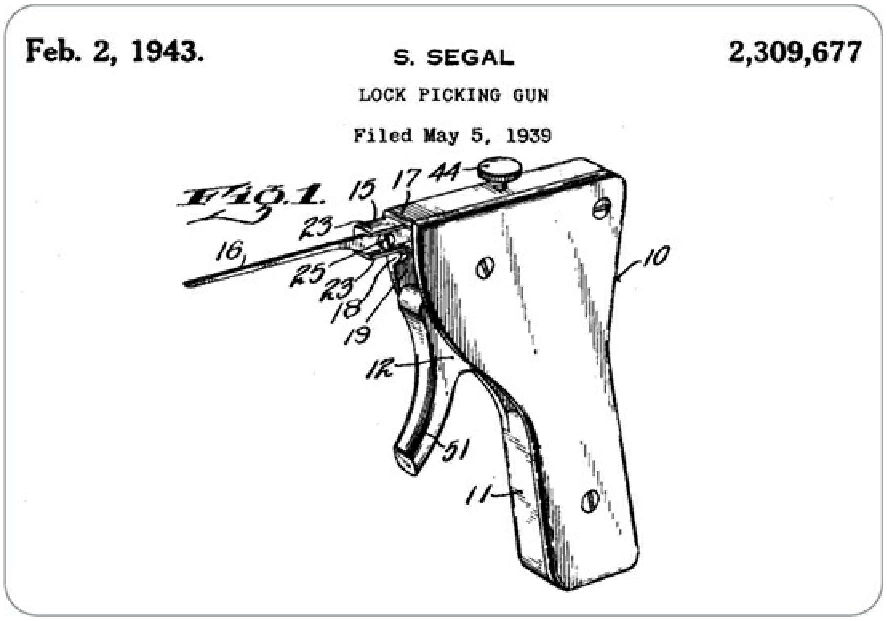


Figure 1-1: Patent 2,309,677 for a "Lock Picking Gun"

Another example is the *bump key*, a cut or filed-down key that can be used to open some locks when tapped in with a hammer. Its patent from 1928 is shown in Figure 1-2. The bumping technique was unknown in the locksport world until it was described in the 2005 article "Bumping Locks" by Barry Wels and Rop Gonggrijp, although those in the lock industry had known about it for decades by then.

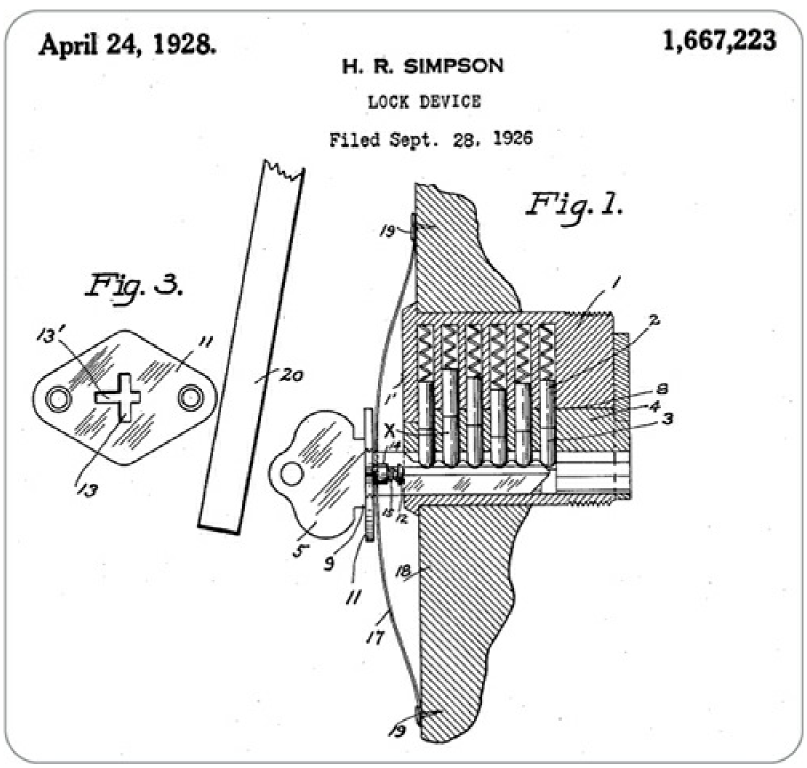


Figure 1-2: Patent 1,667,223 for a "Lock Device"

Probably the oldest well-known lockpicking story is that of the *challenge lock* created by Joseph Bramah. In 1790, Bramah put a lock in his store window, mounted on a board inscribed with “The artist who can make an instrument that will pick or open this lock shall receive 200 guineas the moment it is produced.” In 1851, locksmith Alfred C. Hobbs was the first to pick the Bramah lock, using a special tool he made himself. This 2-in-1 pick and tension tool is still called a *Hobbs hook* in several languages. (We’ll explain picks and tensioners in Chapter 6.)

It’s clear that lockpicking is probably as old as locks themselves. But lockpicking as a sport is much more recent.

Lockpicking Groups and Hackers

Founded on February 9, 1997, the Sportsfreunde der Sperrtechnik—Deutschland e.V. (SSDeV) is the oldest official lockpicking sport group. The name means “sport friends of lockpicking” in German; being the first lockpicking group ever, members included the word *sport* to make it clear that they weren’t just a bunch of shady people talking about breaking locks.

SSDeV originated from the Chaos Computer Club (CCC), a Hamburg-based hacker group founded in 1981. In 1994, Steffen Wernéry, one of CCC’s founders, attended the first Hackers on Planet Earth (HOPE) conference in New York, where he bought his first lockpick set. Back in Germany, he found books by Eddie the Wire in the CCC library and became fascinated with lockpicking. Two years later, at the yearly CCC congress, Wernéry co-hosted a lockpicking lecture and some workshops. These were a success, and a few months later, he and other enthusiasts founded SSDeV. By 1999, Germany had 10 local lockpicking groups; at the time of this writing, there are 14.

SSDeV has inspired locksport groups in other countries. Every four years since 1994, members of the Dutch hacker group Hack-Tic have organized a large outdoor hacker camp. In 1998, SSDeV hosted a tent at this camp to teach lockpicking. One attendee, Dutch hacker Tim Matthews, officially registered the Dutch lockpicking group Nederlandse Vereniging van Hang en Sluitsport (NVHS), which translates to “Dutch Association for Hinges and Locksport,” in Amsterdam a year later. (The acronym NVHS was chosen as a joke: the Dutch Society for Sexual Reform is abbreviated NVSH.) The locksport group, with its close connections to the Dutch hacker scene, met in Amsterdam at the Hippie Hangout, a space rented by the hacker group Hippies from Hell and a precursor to modern-day hackerspaces.

In 2002, NVHS was disbanded because of internal disagreements, and a splinter group founded The Open Organisation of Lockpickers (TOOOL). That year, TOOOL co-founder Barry Wels started the Dutch Open, an annual lockpicking championship with lectures and workshops.

The annual Las Vegas hacker convention DEF CON began impromptu lockpicking competitions in 2003, organized by the Colorado Springs DC719 DEF CON group. The term *lockpick village* was first used in 2005, when TOOOL hosted a dedicated lockpicking tent at the What The Hack Dutch hacker conference.

Also in 2005, Josh Nekrep, Kim Bohnet, and Devon McDormand, contributors to the Lock Picking 101 website, formed a club for lockpicking hobbyists and coined the term *locksport* to differentiate it from locksmithing organizations. Their group, Locksport International, has several chapters around the US.

In 2006, a TOOOL chapter opened in Eindhoven (Netherlands). Barry Wels's personal blog, Blackbag (*https://blackbag.nl*), had gained a lot of attention, making TOOOL a household name in locksport. At that time, Blackbag was one of the only places on the internet discussing lockpicking.

Blackbag's popularity prompted lockpicking groups in other countries (such as the US, UK, Belgium, Norway, and Australia) to adopt the TOOOL name. These groups are independent entities but operate under the same basic rules and share the TOOOL logo as well as the name. TOOOL NL in the Netherlands controls the usage of the TOOOL name, and its website (*https://TOOOL.nl/Toool*) lists TOOOL organizations around the world.

TOOOL US officially formed in 2006 at the conclusion of the sixth HOPE conference, with Wels naming HOPE's lockpick village organizers—Babak Javadi, Eric Michaud, Eric Schmiedl, and Schuyler Towne—members of the board.

Since the founding of SSDeV and TOOOL, many more lockpicking groups have formed around the world. For instance, the Association of Czech Lockpickers (ACZ, *http://lockpicking.team*) was created in 2010. Schlösser Picken Als Schweizer Sport (SPASS, *https://lockpicking.ch*), which translates to "lockpicking as Swiss sport," started in Switzerland in 2011. In some countries, the illegality of lockpicking made starting a sport group problematic. In France, for example, a lockpicking forum has been active since 2006, but another eight years passed before the law allowed the possession of lockpicking tools, and the Association des Crocheteurs de France (ACF, *https://crocheteursdefrance.fr*), or Association of French Lockpickers, formed two years later in 2016.

Many more lockpicking sport groups exist nowadays, either as national or local groups. If you live somewhere that lockpicking is legal but that has no local lockpicking group, consider finding a local hackerspace group (*https://wiki.hackerspaces.org*) and introducing lockpicking. You may well find other interested people and be credited with introducing locksport to your region!

Competitions

These days, plenty of lockpicking competitions take place around the world. The first competitions were held as early as 1997—not surprisingly, by SSDeV. The group held competitions in three styles: *Handöffnung*, traditional lockpicking; freestyle, which allows the use of tools such as pick guns; and *Blitzöffnung*, a knockout system with a time limit of one minute per lock. In 2000, the SSDeV added *Hangschlossöffnung*, padlock opening.

In those early days, impressioning was still a bit of a mystery. Impressioning is the art of creating a working key for a given lock by wiggling a blank key in the lock, looking at the tiny marks that result, and then filing them away. Back then, lockpickers tried out techniques such as using marker pens and chemicals on the key to help better identify the marks. (We'll explain how to master this skill in Part III.) In 2005, SSDeV added an impressioning competition to its portfolio, and Oliver Diederichsen of SSDeV dedicated his time to methodically figuring it out. He compiled his findings, along with fabulous pictures, in his self-published book *Impressioning*, enabling many more people to become successful in the technique. TOOOL introduced its impressioning championship in 2007.

Many lockpicking groups have yearly competitions, the exact rules of which differ for each group. Some groups may use only cylinders, whereas others might include padlocks or have an entirely separate padlock competition. Locks can be limited to regular pin tumbler locks, include dimple locks, or be exclusively dimple locks. (We'll look at types of locks in Chapters 2, 3, and 4.) In some cases, competitors bring their own locks; in others, the locks are provided. Sometimes all contestants pick a lock at the same time, while other times they take turns opening multiple locks in succession.

Lever lockpicking is a relatively new kind of competition that's gaining interest. The basic techniques for opening regular locks can also be applied to lever locks, although differences exist, as we'll discuss in Chapter 3. One notable difference is that lever lockpicking requires expensive tools. The locks themselves are also expensive, which is why lever locks and tools are often provided by the organizers of such competitions.

Additionally, cracking safe locks has crossed over from the world of locksmiths and safe technicians. These competitions are rarer because of the organizational difficulties: opening a safe lock takes considerable time, and the contestants must be opening exactly the same lock(s), because different locks will take vastly different times to open. As a result, these competitions aren't typically held at a specific time but instead over a lengthier period, with the same safe lock given to the participants in turn.

Other competitions are held as well, such as escape room–style competitions. These are especially popular at hacker conferences. Check your local locksport group to see what it has to offer.

Rules

Most locksport conferences—and the organizations that run them—have rules that participants must follow or risk being asked to leave. These rules are meant to protect locksporters, locks, lock owners, and locksport clubs. After all, a few bad members could easily tarnish the reputation of an entire club.

While rules vary among locksport clubs and organizations, a few are common to almost all groups:

- Pick only locks you own or have the owner's permission to pick. This rule is simple; not following it is breaking and entering.
- Don't pick locks that are in use. While the techniques discussed throughout this book

are generally nondestructive, the possibility always exists that a lock can be damaged and rendered inoperable during picking or impressioning. If you lock yourself out, call an actual locksmith.

- Don't claim to be a locksmith. Many municipalities have specific licensing requirements for locksmiths. Offering these services outside of a proper locksmithing business can get you into trouble.
- Be mindful of who you teach. Don't demonstrate lock-opening techniques to anyone who intends to use them to break the law.

Be sure you're following these rules and any others set by your club or competition organizers, or you won't make it very far in locksport!

Legality

When you first tell people that you pick locks, a common initial reaction is "Isn't that illegal?" While this response is somewhat understandable given the way lockpicking is often portrayed in media, the answer is usually no. In much of the world, simply possessing lockpicking tools isn't a crime. Having the tools becomes a legal issue only when they're used to commit a crime. Indeed, many tools sold at hardware stores are legal to own but illegal to use for nefarious purposes. Lockpicks are usually no different.

That said, not all countries (or even states, provinces, counties, cities, and so on) view lockpicking tools in this light. In Poland and Japan, for example, such tools are prohibited. In this section, we'll highlight laws from some of the countries where locksport competitions or conferences are routinely held.

NOTE

We aren't lawyers! While the locksport community has done extensive research into the legality of possessing and using lockpicking tools in many regions, laws are subject to change. Be sure to do your research and make sure you're staying safe and legal.

US Laws

Federally, the US doesn't have a blanket rule banning the possession or use of lockpicking tools. US laws prohibit sending these tools by mail or other shipping services to non-locksmiths (39 US Code § 3002A and 18 US Code § 1716A), but to the best of our knowledge, these laws aren't enforced. Most manufacturers do, in fact, ship their tools by mail.

While the lack of a federal ban is good news, the downside is that each state is free to make its own laws, resulting in a patchwork of regulations across the country. Fortunately, TOOOL US has put together a fabulous page detailing the laws for each state (*https://TOOOL.us/lockpicking-laws.php*). This page also contains a convenient reference map, shown in Figure 1-3.

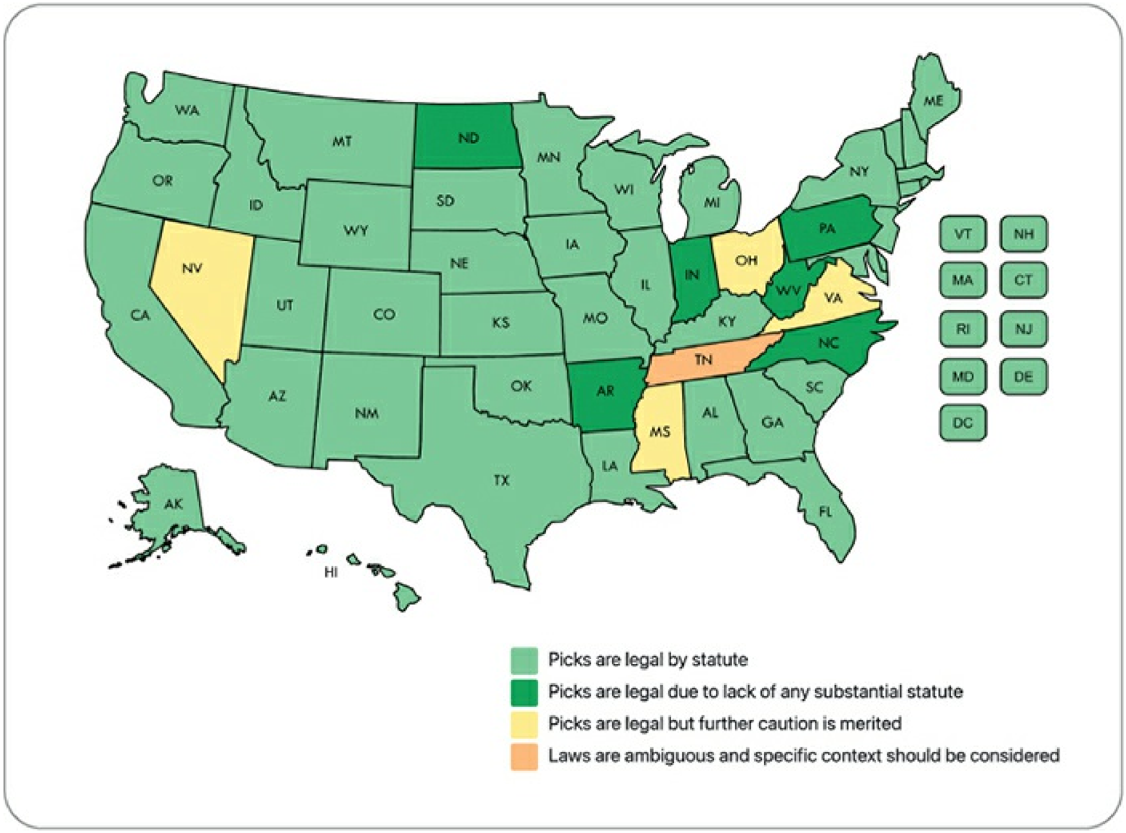


Figure 1-3: TOOOL US lockpicking laws map

As you can see from the map, possessing lockpicking tools is legal in most states as long as the carrier demonstrates no intent to use those tools for a crime. That said, exercise additional care when carrying or using these tools in Virginia, Ohio, Mississippi, Tennessee, or Nevada. Laws in these states often require you to prove your innocence rather than having a prosecutor prove your guilt. Tennessee had a similarly restrictive law, but it appears to have been revoked in June 2021 (see *https://www.tn.gov/content/dam/tn/commerce/documents/regboards/lock/posts/Locksmith-Letter_6-7-2021.pdf*). This change has not yet been reviewed by the TOOOL US legal team and is therefore not yet reflected on their map.

NOTE

This material was prepared based on research performed by the TOOOL legal team in 2012. While we can speak with relative confidence as to the accuracy of the quoted statutes as reflected in law at the time, TOOOL naturally makes no guarantees about the completeness of those citations or of the examples in case law included. This map and any included notes do not constitute legal advice, and TOOOL encourages all sport pickers to consult with an attorney for more concrete knowledge of laws and regulations that may affect participation in this hobby.

LockWiki.com also maintains a list of laws (*https://lockwiki.com/index.php/Legal_issues*). These two sources are your best bet for information about laws that impact locksport in the US.

Dutch Laws

No law in the Netherlands forbids the possession of lockpicking tools. If you use them without permission on a lock you don't own, however, that's obviously illegal.

Cities in the Netherlands sometimes have additional municipal laws called *Algemene Plaatselijke Verordening*, or *APV*. In Amsterdam and Eindhoven, where TOOOL NL resides, Articles 2:77 and 2.44, respectively, state that a person isn't allowed to possess lockpicking tools in a public space unless they can demonstrate on the spot and to an officer's satisfaction that they don't intend to use the tools to gain unlawful entry, unlawfully open or break closures, or facilitate or obscure traces of theft. To our knowledge, you can carry lockpicking tools and use them to practice locksport anywhere in the Netherlands.

UK Laws

England and Wales have a different legal system from Scotland, and neither system specifically prohibits lockpicking tools. The only offense that you could be committing for simply carrying such tools would be "going equipped" for stealing, as per Section 25 of the Theft Act 1968.

If you're found carrying lockpicking tools outside your home, for it to be considered a crime, the police must prove that you intend to use the tools to commit either theft or burglary. That's a pretty high bar, so simple possession shouldn't cause you any issues as long as you can demonstrate, to either the police or a court, that you're interested in the hobby and participate in locksport groups or contests. Concurrent possession of a hard copy of this book would, for instance, show you were likely a sport picker. Concurrent possession of a balaclava and crowbar would tilt the opinion in the opposite direction. If you're just sitting in a local pub in the afternoon with several others, picking locks peacefully, you'll be fine. If the pub is closed and you're caught sitting in the bar? Busted.

We know of only one case where this offense has been taken to court, and the defendant was found not guilty.

German Laws

Germany has no generic law that forbids the possession or use of lockpicking tools, whether in a public or private environment. If you use them without permission on a lock you don't own, again, that's clearly illegal.

Australian Laws

Australian law appears to state that possession of "housebreaking" tools is allowed if the possessor has a legitimate reason. Specifically, Section 3.5 of the *Review of Maximum Penalties for Preparatory Offences Report* states:

> A person who, without lawful excuse, has an implement of housebreaking in his or her possession is guilty of an offence. The onus is on the person to prove the lawful excuse for having the implement in his or her possession.

We're not aware of any locksporter facing trouble for possessing lockpicking tools in Australia.

Groups and How to Find Them

You've read the rules and the laws and are ready to begin your locksport journey. The best way to get started is to join a local group of fellow lock enthusiasts. Don't rush ahead and order your tools just yet! We'll get into choosing the right ones in later chapters.

Locksport is about community much more than it is about competition or bragging rights (though plenty of room remains for that as well). An afternoon spent with a handful of picking tools and a tableful of locks is best enjoyed with friends—and maybe a few frosty beverages. As long as you bring a genuine interest in the challenge of opening locks, the locksport community is one of the most helpful, accepting, and friendly groups you can find.

US Groups

The largest and best-known locksport group in the US is TOOOL US (*https://TOOOL.us/meetings.xhtml*). It has chapters in more than two dozen cities and runs locksport villages at numerous information security conferences, such as DEF CON and ShmooCon. TOOOL US also hosts the annual LockFest conference and competition.

Locksport International, or LI (*http://locksport.com/index.php/discover-l-i/local-chapters*), is another organization with chapters in several states. One of its most popular chapters is the Longhorn Lockpicking Club in Austin, Texas.

If none of these groups meet in your area, you can check a few other places. Try searching for *locksport* or *lockpicking* on Meetup (*https://www.meetup.com*); most clubs list their meetings there. Alternatively, check with any local hackerspaces, since a big crossover occurs among makers, hackers, and lockpickers. If you find nothing at all in your area, consider forming your own group. Once you find a few others who are interested, check the national organizations' sites to learn how to become an official chapter.

Dutch Groups

TOOOL NL (*https://TOOOL.nl*) currently has chapters in Amsterdam and Eindhoven that hold biweekly meetings. The group has hosted the Dutch Open lockpicking championship since 2002. These competitions have evolved into an annual three-day event called *LockCon*, which includes the Dutch Open as well as many workshops and lectures. LockCon is held in the Netherlands in autumn.

UK Groups

The TOOOL UK group (*http://www.TOOOL.uk*) open meeting has been running for over a decade at fizzPOP, the Birmingham makerspace, on the first Wednesday of every month. The group also runs an active Discord server called *TOOOL UK* (*https://discord.gg/mp2fhED*) and holds a virtual meeting once a week.

German Groups

SSDeV (*https://blog.ssdev.org*) has local chapters all around Germany as well as a special interest group dedicated to underwater lockpicking. Each SSDeV chapter has its own meetings. Some of these are *lockpicknicks*, outdoor gatherings for lockpickers to eat, socialize, and of course pick locks. Lockpicking and impressioning championships are held yearly. SSDeV lists all competing lockpickers and their scores—*Listung der Meister*, or *Listing of Masters*—on its website.

Australian Groups

Australia has its own TOOOL organization, founded in 2019 (*https://www.TOOOL.com.au*). It hosts regular meetups in Melbourne, Canberra, Sydney, and Newcastle; check the website to find the next meetup or join the group.

OzSecCon (*https://www.ozseccon.com*) is Australia's original conference devoted to physical security. It is held almost every year in Melbourne. In addition to talks and workshops, it also includes lockpicking and impressioning competitions.

Summary

In this chapter, you've learned a bit about locksport history, some lockpicking rules and laws, and how to find resources such as national organizations and local groups.

In the next chapter, we'll start getting into the hardware itself by examining various types of locks you might encounter and how they work.

2
TYPES OF LOCKS AND CYLINDERS

Before we dive into picking, it's worth taking some time to examine the locks themselves. Locks come in a huge variety of designs based on factors including what the lock will be used on, how it's attached, how secure it needs to be, and even the country where it will be used. These criteria matter greatly to someone installing a lock but are largely irrelevant to locksporters. Since we're concerned only with opening a lock, locksporters usually set aside any accessories, such as the hardware to mount it to a door. In fact, locksporters typically save only the lock's cylinder, the part normally operated with a key. The exception is locks with a cylinder that can't be removed from the rest of the lock hardware, such as some padlocks.

But while the shape of the lock or cylinder isn't as important to locksporters as the lock mechanics, it can still play a part in the way a lock is picked. Being familiar with the various types of locks and cylinders, as well as the lockpicking tools you might need for them, is also helpful when you're buying, trading, researching, or discussing locks.

Padlocks

The most recognizable and ubiquitous lock is the *padlock*. Of all the lock types, padlocks are the most diverse. They include everything from suitcase zipper locks the size of a thumbnail to behemoths like the Sargent & Greenleaf (S&G) 951, which weighs several pounds and can withstand a barrage of bullets—an important trait for a lock used to secure military depots. Figure 2-1 shows an assortment of padlocks.

Figure 2-1: Left to right: a Lockwood luggage lock, a Master Lock #1, and an S&G 951

Padlocks are a great place to start picking, as they're readily available in hardware stores, big-box stores, and even supermarkets and convenience stores. Most are reasonably sized, making them easy to hold while picking. Because they vary significantly in both their locking mechanisms and security features, you can find padlocks to challenge lockpickers of any skill level. And, best of all, padlocks often make a very satisfying *clang* when you get them open.

There are a few things to know about picking padlocks. In most cases, you can open them only by turning their *plug* (the part that rotates) clockwise, whether you're picking or using the key. Also, once you've picked a padlock, the force required to turn and open it varies considerably depending on the lock's brand and model. Whenever possible, test a padlock with a key first to get a feel for the amount of force you'll need. Finally, since padlocks vary so much in size and weight, it's a good idea to have a vise on hand to hold the lock while you're picking it.

Cylinder Locks

If you've locked or unlocked any door, the odds are good that you've used a *cylinder lock*. Lock cylinders come in a variety of shapes and sizes to accommodate multiple styles of doors and door hardware (such as doorknobs) that are used in different countries. In this section, we'll look at some of the most common types of door cylinders: Euro profile, key-in-knob, interchangeable core, rim, and mortise cylinders.

Euro Profile Cylinders

While not common in the US, *European profile cylinders*—usually shortened to *Euro profile*, *Euro cylinders*, or even just *profile cylinders*—are, as their name indicates, found throughout much of Europe, most often in doors. Euro profile cylinders vary considerably in both length and locking mechanism but can be recognized by their signature shape, which looks somewhat like an upside-down exclamation point, as shown in Figure 2-2.

Figure 2-2: Euro profile cylinders mounted in a door (left) and unmounted (right)

Many Euro profile cylinders are double-sided, meaning they have a *keyway* (the hole to insert the key) on both sides of the lock. However, some have a *thumb turn* (a small knob to lock or unlock the lock without a key) on the interior side and a keyway only on the exterior side. In picking competitions that include Euro profile cylinders, double-sided locks are the norm, and typically the contestant can pick either side. When not mounted in a door, many cylinder types, including Euro profile cylinders, can be picked clockwise or counterclockwise.

Double-sided locks are less common in the US, where fire safety often takes precedence over door security. Single-sided locks with a thumb turn can be quickly opened from the inside, but they make it easier for thieves to break a nearby window and reach in to unlock the door.

The Euro profile cylinder's shape fits well in most people's palms, so many locksporters prefer to hold it rather than use a vise when picking. For extended picking sessions, such as long competitions, however, using a vise can help prevent hand cramps.

> I designed a holder to make it easy to secure Euro profile cylinders with a vise or clamp; you can download the 3D model at *https://www.thingiverse.com/thing:3610868*. I use a plastic, 3D-printed version of this holder in picking and impressioning competitions.
>
> —MATT

The Euro profile cylinder has a few variations. The *Swiss cylinder* format looks similar to a Euro profile cylinder, except that the bottom area where the lock screws into the door is centered in the cylinder rather than extending its full width, as shown in Figure 2-3.

Figure 2-3: A Swiss cylinder lock

Several *oval-shaped cylinders* exist, including UK, Australian, and Norwegian variants. Each is similar to a single- or double-sided Euro profile cylinder, but the top and bottom of the lock are the same width. Figure 2-4 shows a single-sided Australian oval cylinder.

Figure 2-4: An oval-format BiLock cylinder

The main difference between the oval variants is in the way they're screwed into a door, which is inconsequential to locksporters.

Key-in-Knob Cylinders

In the US, *key-in-knob (KIK) cylinders*, also known as *key-in-lever cylinders*, are extremely popular. These small locks fit inside a doorknob or lever handle, hence their name. Like Euro profile cylinders, unmounted KIKs can be picked clockwise or counterclockwise.

Typically, KIK cylinders look like a Euro profile cylinder that's been snapped in half and slightly shrunk. Their shape is a bit less recognizable, though, because everything except the plug is hidden inside the knob. For example, only the silver portion of the KIK cylinder shown in Figure 2-5 would be visible when the lock is installed.

Figure 2-5: An unmounted KIK cylinder

Higher-end padlocks that can be disassembled and rekeyed also often contain a cylinder that looks like a slightly shrunken KIK. Examples include many American-brand locks and their clones.

KIK cylinders can be hard to hold while picking because of their small size and sharp edges, so some pickers prefer to mount them in a vise. Others go so far as to 3D print a plastic shell to make them easier to hold. If you have access to a 3D printer, searching *KIK holder* on your favorite 3D-model-sharing repository should turn up several options.

Interchangeable Core Cylinders

An *interchangeable core (IC) cylinder* looks like a figure eight or a snowman with a metal bar protruding from the side, known as a *control lug*. ICs are common in office and commercial buildings because they can easily be removed and replaced using nothing more than a *control key*, a special key that retracts the control lug into the core. When someone loses a key or leaves the company, rekeying the office takes 5 seconds instead of 30 minutes because a new core can simply be swapped in using the control key. The old cores are typically rekeyed and set aside for the next time they're needed.

NOTE

Many people, even locksmiths, use the terms cylinder *and* core*—and sometimes even* lock*—synonymously. We'll explain the subtle differences between these terms in the next chapter, but don't be surprised if you hear them used interchangeably.*

ICs are made in multiple sizes and configurations, such as *small-format interchangeable core (SFIC)*, *large-format interchangeable core (LFIC)*, and *removable core (RC)*. While SFIC is an industry-standard term used to describe a very specific size and shape originally designed and created by the BEST Lock Corporation (now part of Dormakaba), LFICs come in many shapes and sizes. SFICs are made up of two symmetrical circles and are smaller than LFICs and RCs. LFICs and RCs are less standardized and vary depending on the brand, but they often have a core comprising two circles of slightly different sizes. Figure 2-6 shows an LFIC (left) and an SFIC (right).

Figure 2-6: Corbin Russwin LFIC (left) and BEST SFIC (right)

Picking ICs can be tricky, because the same mechanism that enables the control key to easily remove the lock can also interfere with picking. We suggest holding off on picking ICs until you've successfully picked some more basic locks.

Rim and Mortise Cylinders

Rim cylinders are frequently used in deadbolts, and *mortise cylinders* are often found on commercial doors. While they vary in size, the most common ones are about 3.5 cm or 1.25 inches in length and width. The two types look similar from the front, but they differ in the way they're installed in a door, as you can see from the side views shown in Figure 2-7.

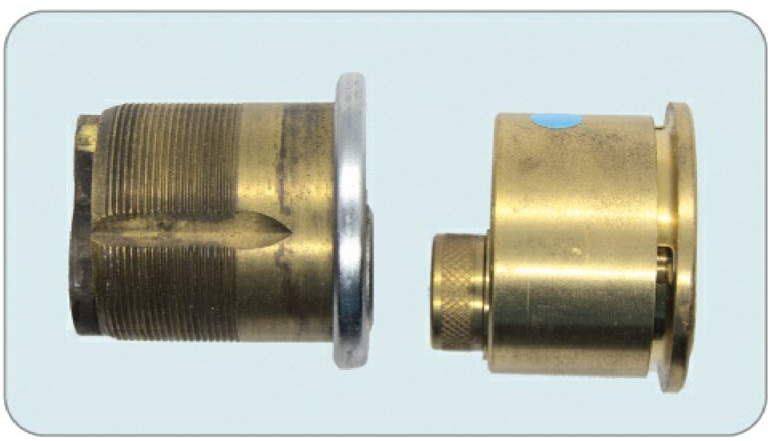


Figure: 2-7: A mortise cylinder (left) and a rim cylinder (right)

Rim cylinders are smooth but have two threaded holes in the back to screw the lock to the surface of the door. Mortise cylinders, on the other hand, have a threaded housing that allows the entire cylinder to be threaded into the lock hardware, which is then inserted into a cutout in the door, known as a *mortise*. Once the mortise cylinder is threaded into the lock, one or more set screws are used to hold the cylinder in place so it can't be backed out.

Mortise Locksets

Finally, the *mortise lockset* is a mortise lock with a cylinder that is integrated into the mortise hardware and is not removable; that is, the security locking features are incorporated into the mortise lock body itself. It's most commonly found in England and in antique doors elsewhere. As Figure 2-8 shows, these locks are large, rectangular boxes that fit into a mortise in the edge of a door.

Figure 2-8: A mortise lockset installed in a door

Mortise locksets are frequently associated with lever lock and warded lock mechanisms, which we'll discuss in the next chapter. While not terribly common in lockpicking circles, lever locks in mortise lockset form have been a part of the Dutch Open competition for the past several years. We'll cover these locks extensively in Part V.

Summary

This chapter examined a variety of common lock and cylinder types and discussed their distinguishing characteristics. We also touched on terms for parts of a lock like *keyway*, *plug*, and *core*. In the next chapter, we'll take a deeper dive into those and other lock internals as we cover common lock mechanisms.

3
LOCK MECHANICS

To be able to pick or impression a lock successfully, first you have to understand how it works. To that end, in this chapter we'll define the common terms for the parts of a lock and then explore a variety of locking mechanisms and how they operate.

Elements of a Lock

In this section, we'll discuss the most common parts you'll find on locks. Even if you're pretty comfortable with this topic, we still suggest perusing it. People tend to use a lot of lock-related terms interchangeably, but they have subtle differences. Having a shared vocabulary will help you follow along with the rest of the book.

The Housing or Cylinder

Let's start with the most visible part of any lock: the *housing*, or the body of the lock. The term *cylinder* is also commonly used to refer to the housing or to the entire lock including the housing. As Figure 3-1 shows, on a padlock you can see the entire housing, whereas only the face of the housing is visible on an installed door-mounted rim cylinder, like a deadbolt.

Figure 3-1: The housing of a padlock (left) and deadbolt (right)

The Shackle or Bolt

The name of the piece used to secure the lock differs depending on the lock's type. On a padlock it's typically a U-shaped part, called a *shackle* or a *shank* (Figure 3-2).

Figure 3-2: A padlock's shackle

On a door lock or safe lock, this part juts out from the side of the door and into the door frame or safe (as shown in Figure 3-3) and is known as a *bolt*.

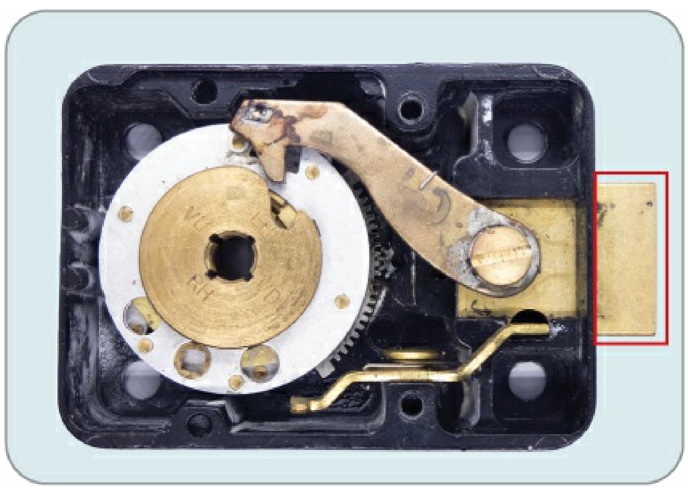


Figure 3-3: A safe lock bolt

The bolt isn't always built directly into a lock. Sometimes it's part of the hardware mounted to the door (known as the *lockset*) and then connected to the lock cylinder by a cam or tailpiece, described later in this chapter.

In lockpicking competitions with padlocks or safe locks, releasing the shackle or retracting the bolt constitutes an *open*—a successfully picked lock. Competitions using Euro profile cylinders typically don't include the bolt, so competitors achieve an open by rotating the plug, described next.

The Plug

The *plug* is a round, cylindrical piece of metal that rotates when the correct key is inserted and turned (Figure 3-4). Only the face of the plug is visible when the lock is assembled. As we'll discuss shortly, lock mechanisms that commonly use plugs include pin tumblers, wafers, and dimples. Inside a lock, the plug is surrounded by a metal sleeve called a *shell*.

NOTE

The term shell *can refer to different things for different locks. In Euro profile cylinders, for instance, the shell is just the actual housing of the lock. In some designs, such as KIK cylinders mounted inside a padlock, the shell is a separate part altogether.*

Figure 3-4: A plug removed from a KIK cylinder

The Core

You'll often hear people refer to a lock's plug as its *core*, but that isn't exactly right. On most types of locks, the plug and the core aren't distinct parts. However, on interchangeable core locks like SFICs, the core is the figure-eight-shaped part of the lock that fits into the housing, and the plug, in turn, fits into the core (see Figure 3-5). ICs contain most of the lock's inner workings, including the pins and springs.

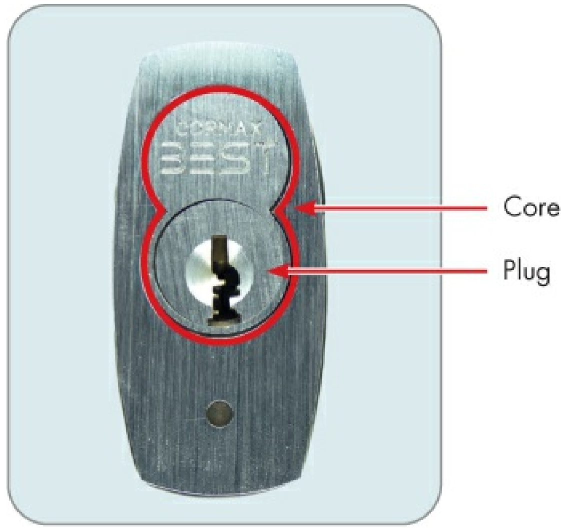


Figure 3-5: An SFIC core in a padlock

The Keyway

The *keyway* of a lock is the slot cut into the plug where you insert a key or picking tools. Keyways vary in size and shape depending on the lock's brand and model. A typical keyway, originally created by the Schlage lock company, is shown in Figure 3-6.

Figure 3-6: A typical keyway

As a security feature, some keyways are designed to be particularly tight or oddly shaped to limit the space available for picking tools. For example, the keyway in the IKON lock shown in Figure 3-7 is off-center, or *paracentric*. We'll talk more about keyways in Chapters 4, 6, and 7.

Figure 3-7: A paracentric keyway

Pins, Wafers, Discs, and Levers

Keyed locks rely on a series of metal pieces that align with the key to open the lock. These metal pieces can be *pins*, small cylinders that come to a point; *wafers*, flat, oblong plates with a hole in the center; *discs*, round plates with a hole in the center and a notch on the edge; or *levers*, long, pivoting arms (see Figure 3-8 for some examples). Regardless of the exact mechanism, these are the parts you manipulate with your picking tool.

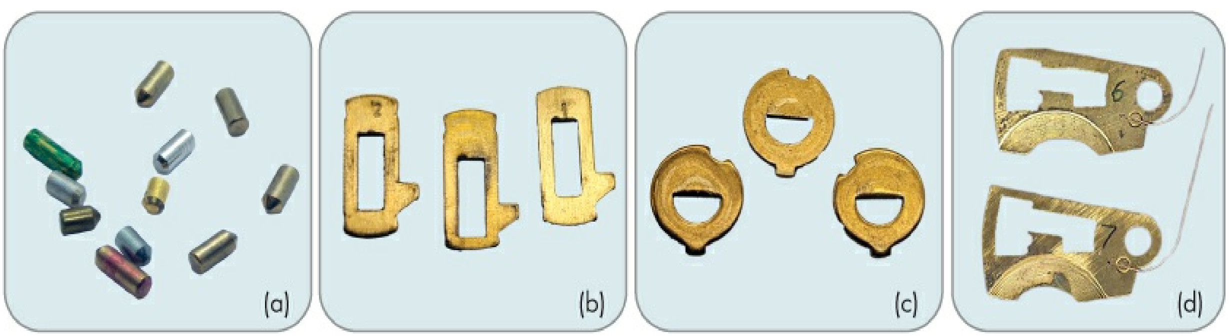


Figure 3-8: An assortment of key and driver pins (a), wafers (b), discs (c), and levers (d)

Springs

Most locks contain *springs* to keep the pins, levers, or wafers in place. In pin tumbler and dimple locks, each pin stack has a small spring that presses the pins up or down, depending on the lock's orientation (see Figure 3-9). Similarly, wafer locks use springs to position wafers, and lever locks use larger springs to tension the levers.

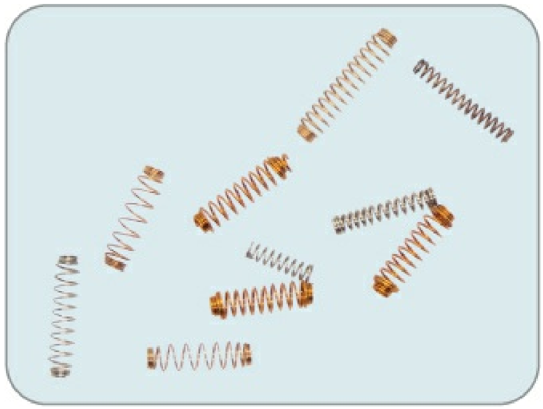


Figure 3-9: A variety of pin tumbler springs

Even locks that don't use springs as part of the locking mechanism often contain them for other purposes. Safe locks can have a springy, bent metal washer to tension the wheel pack (see the later section "The Wheel Pack and Drive Cam"). Padlocks, regardless of the locking mechanism, often have springs to pop open the shackle once it's unlocked. Because of all these springs, parts can easily go flying if you're taking apart a lock for the first time! We'll cover how to avoid that in Chapter 5.

The Bible

The *bible* contains chambers that hold the springs and driver pins in a pin tumbler lock. On a KIK or Euro profile cylinder, the bible protrudes above or below the plug, as shown in Figure 3-10. Although technically part of the housing, the term *bible* gets used enough to warrant mention.

Figure 3-10: The bible of a KIK cylinder

The Wheel Pack and Drive Cam

Combination locks, such as those found on safes, typically don't use keys. These locks don't have pins, keyways, plugs, or even cores. Instead, inside the housing sits a *wheel pack* containing one wheel for each number in the combination. (Combination lock competitions use three-wheel locks exclusively.) On top of the wheel pack is the *drive cam*, which is responsible for spinning the wheels when someone turns the dial and for retracting the bolt (see Figure 3-11).

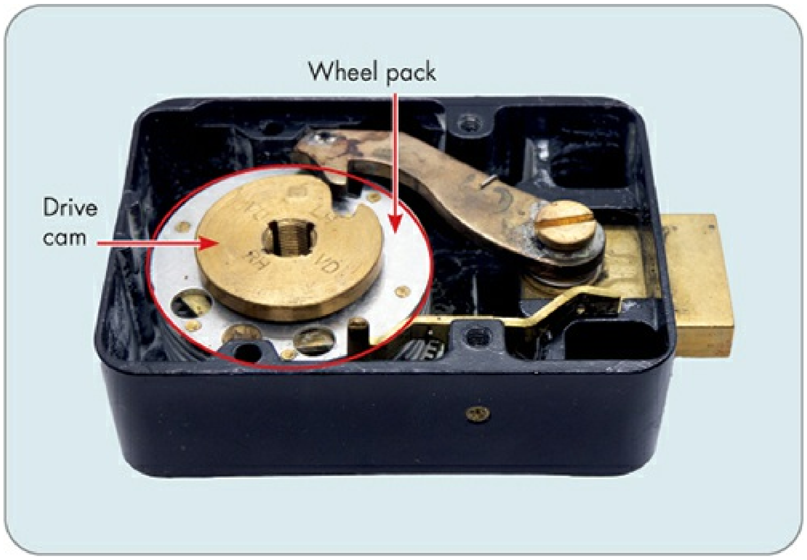


Figure 3-11: The wheel pack and drive cam in a safe lock

Each wheel has a notch, called a *gate*. When the gates of all the wheels align with the gate of the drive cam, a metal bar called the *fence* drops into the groove they create, allowing the bolt to be retracted and the lock to be opened. We'll talk more about this mechanism in "Combination Locks" on page 38.

NOTE

Some combination locks have a key to change the combination or bypass it entirely (such as a manager key for hotel safes). Some safes also require a key and *a combination—two-factor authentication for the physical world.*

Cams, Tails, Latches, and Ball Bearings

In most locks, the key (and even the plug) doesn't directly interact with the bolt or shackle. Instead, rotating the plug moves a small element on the lock, which is what actually moves the bolt or releases the shackle. This element's name depends on the lock.

On a Euro profile cylinder or mortise cylinder, it's called a *cam*. On a double-sided Euro profile cylinder, the cam is in the middle of the lock (as shown in Figure 3-12), while on a mortise, the cam is on the back.

Figure 3-12: The cam on a Euro profile cylinder

On rim and KIK cylinders, this mechanism is called a *tail* or *tailpiece*, which is a long, flat piece of metal mounted to the back (see Figure 3-13).

Figure 3-13: The tail of a rim cylinder

Padlocks are typically a little different. Cheaper padlocks have one or two wedge-shaped, spring-loaded latches that snap into notches on the shackle to lock the padlock, and then retract when the plug is turned to unlock it. Instead of latches, higher-end padlocks use *ball bearings* that mate with half-circle cuts on the shackle. Figure 3-14 highlights the difference. The balls roll into the housing when the correct key is used, releasing the shackle.

Figure 3-14: A padlock that uses ball bearings to secure the shackle (left) and one that uses latches (right)

Padlocks with ball bearings are typically more secure. The latches' wedge-like shape lends itself to *shimming attacks*, in which a thin piece of metal is slipped next to the shackle and into the housing in order to depress and release the latch. This isn't possible with the ball bearing mechanism.

Locking Mechanisms

A wide variety of locking mechanisms are used throughout the world. Certain types have a reputation for being more secure, but generally there are secure and insecure examples of every type of lock. In this section, we'll look at the most widespread locking mechanisms: pin-based locks, wafer locks, combination locks, lever locks, warded locks, and disc detainer locks.

Pin-Based Locks

Several styles of locks use pins for their locking mechanism, including pin tumbler, dimple, and tubular locks. We'll start with pin tumblers, arguably the most common type of lock in the world.

Pin Tumbler Locks

You probably use several pin tumbler locks almost every day, as the vast majority of homes and businesses throughout the world rely on them. While the mechanism known today as a *pin tumbler* has been around since the mid-1800s, more primitive versions have existed for thousands of years.

The plug of a pin tumbler lock has a series of holes that align with holes in the lock's bible. Each hole contains two or more pins and a spring. The *key pin* touches the surface of a key inserted into the plug's keyway and often has a conical tip. The *driver pin* sits between the key pin and the spring and is flat on both ends. Usually, the driver pins are all the same length, while the key pins vary in length to match the different cut depths on a key. Together these pins and springs make up one *pin stack*, as shown in Figure 3-15.

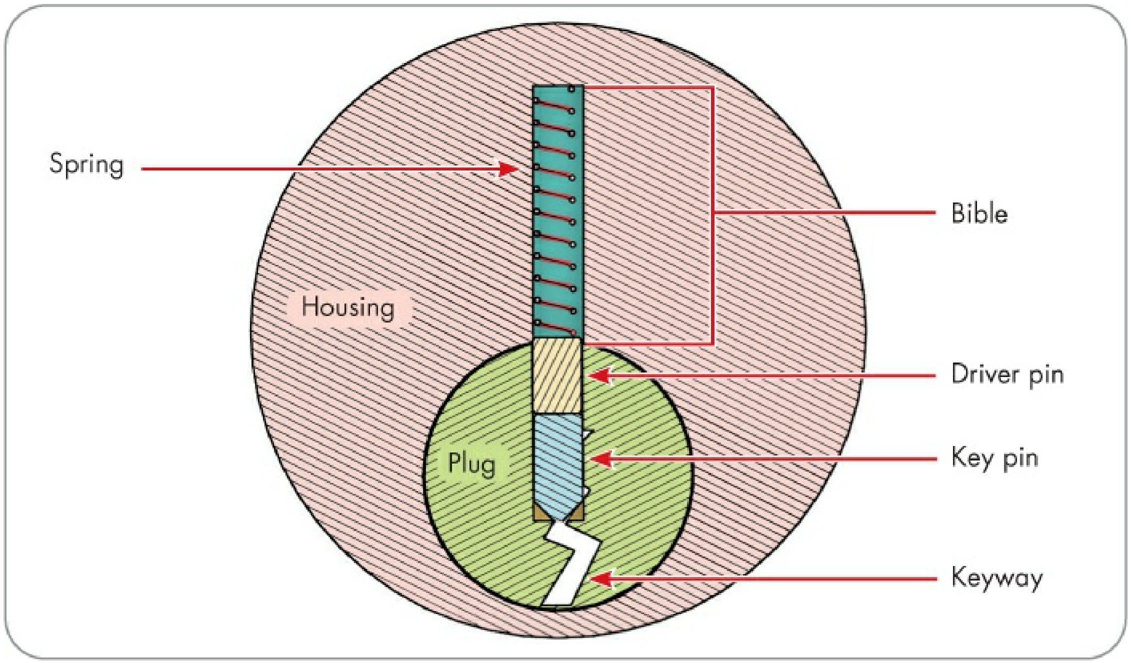


Figure 3-15: The pin stack

When a key is inserted, if it's cut to the correct height for the pin stack's position, the key pin will be flush with the edge of the plug, and the driver pin and spring will be entirely inside the bible. This point where the plug and the bible meet is called the *shear line*. Figure 3-16 shows the cross section of a single pin stack aligned with the shear line; notice how the key pin (blue) ends at the very edge of the plug (green), while the driver pin (yellow) is in the bible (pink).

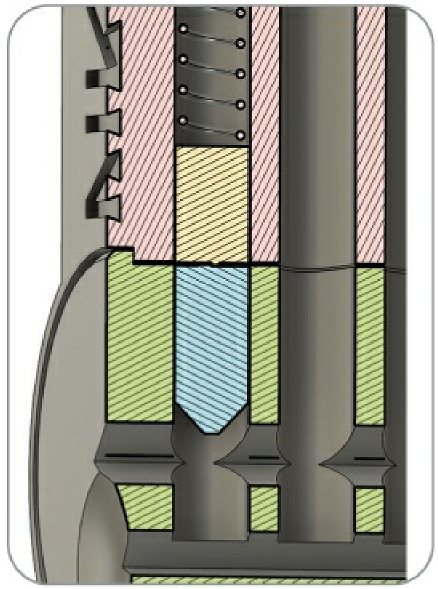


Figure 3-16: A pin stack aligned with the shear line

MASTER-KEY SYSTEMS

Locks in pin tumbler master-key systems are pinned a bit differently. A *master-key system* is a group of locks that have been pinned to allow some keys to open multiple locks (e.g., those keys handled by a security guard, manager, or maintenance person), while still allowing users to have their own key that works on just a single lock, such as on one office door.

The locks usually have three pins in one or more pin stacks: the driver pin and key pin are separated by a third pin of varying length. This increases the number of possible interfaces among pins that could open the lock. For example, the original key might push the pins such that the shear line for a particular pin stack is above the master pin, while the master key, which has a different cut depth at that pin stack position, might push them such that the shear line is below the master pin. Either way, the lock will open. The number of key combinations that can open the lock grows exponentially with the number of pin stacks containing master pins.

Master keying is a complex topic that would take an entire book to fully explain, and one that locksmiths take a long time to learn. Luckily, such locks don't usually appear in competitions, so we won't go into detail about them in this book.

If the key's cut for a particular pin stack is too shallow (that is, the key is too tall in this position), the key pin is *overset*, meaning part of it is being pushed past the edge of the plug and is now protruding into the bible (see Figure 3-17). Attempts to turn the plug will fail because the key pin is blocking its rotation.

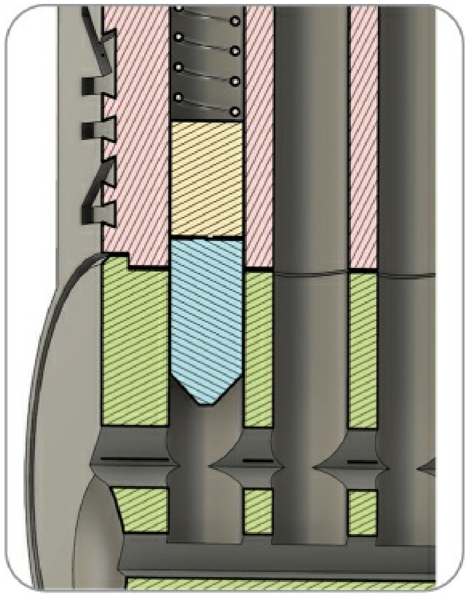


Figure 3-17: A key pin blocking the plug's rotation

If the key's cut is too deep (so the key is too short in this position), the driver pin will extend down out of the bible and sit partially in the plug, as shown in Figure 3-18. This is also the default state of the lock when no key is inserted. Attempting to turn the plug in this state will also fail, as the driver pin prevents the plug from rotating.

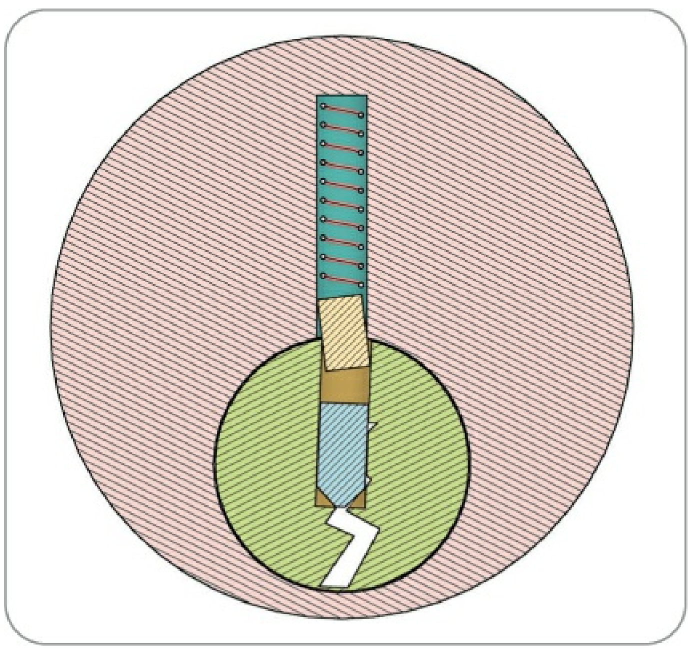


Figure 3-18: A driver pin blocking the plug's rotation

If all the key's cuts correctly correspond to the key pin length for every pin stack in the lock, then all the key pins and driver pins align at the shear line. The plug can then rotate freely, and the lock will open. This is shown in Figure 3-19. The depths of the key cuts are collectively known as the key's *bitting*.

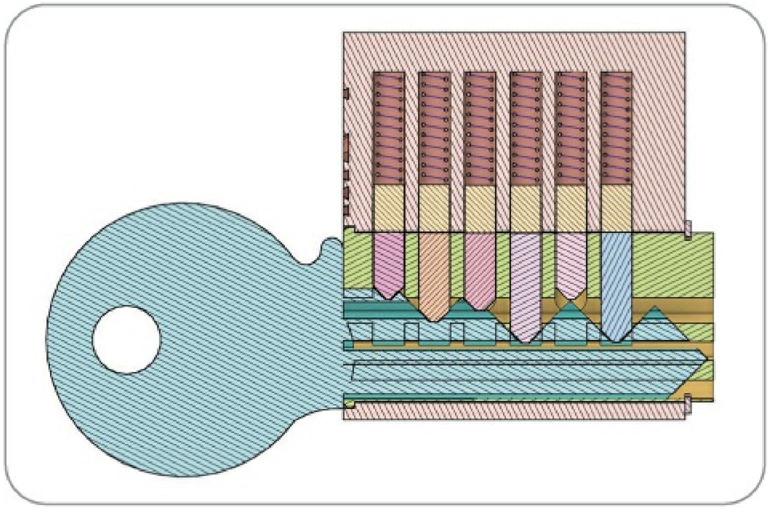


Figure 3-19: The correct key aligning all six pin stacks at the shear line

Two sets of numbers are used to describe the bitting of a pin tumbler key: the position and the depth. Almost all pin tumbler brands refer to the cut closest to the *head*, or *bow*, of the key (the part that you typically grasp to use the key) as position 1, the next pin stack as position 2, and so on. Thus, position 1 on the key corresponds to the pin stack closest to the face of the lock. We'll be using this convention throughout this book.

Most brands use the number 0 to describe the shallowest possible key cut (corresponding with the shortest key pin), and a number like 5, 6, or 9 to describe the deepest possible cut and longest key pin. Therefore, a bitting of 2-5-3-1-3 describes a key for a lock containing five pin stacks, with a cut depth of 2 closest to the bow and 3 on the tip of the key. As you might have noticed, a key can use the same depth (3 in this example) at multiple positions.

Figure 3-20 shows a key with a bitting of 1-3-2-5-1-5; the pin stack positions are labeled in purple, and cut depths are labeled in red.

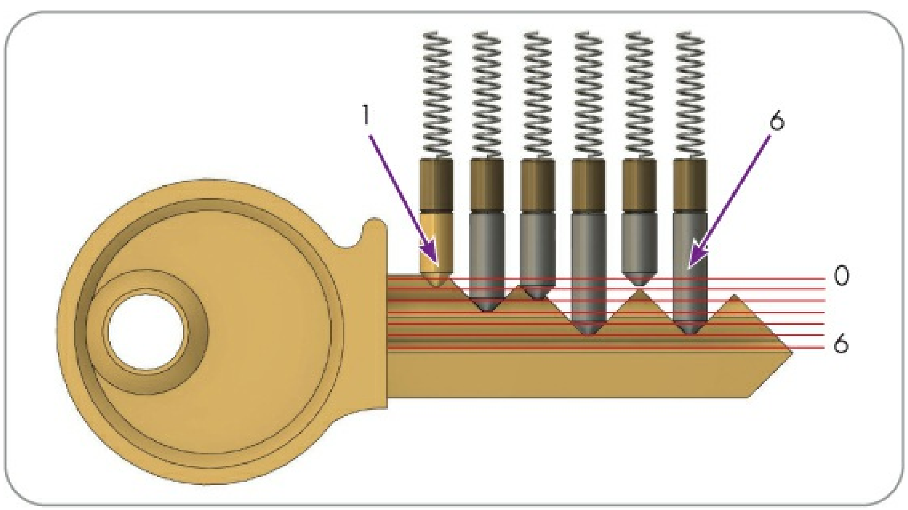


Figure 3-20: A key with a bitting of 1-3-2-5-1-5

NOTE

Cut depths vary from brand to brand; a 2 cut on a Kwikset is unlikely to be the same depth as a 2 cut on an ABUS. The spacing between cuts also varies. It's important to look up the specifications for a lock brand before impressioning, cutting keys, or repinning a lock. We'll discuss the specifications for locks used in impressioning competitions in Chapter 11.

Pin tumbler locks vary in the number of pin stacks they contain. Theoretically, more stacks mean a more secure lock, but a well-made lock with a few stacks is probably more secure than a poorly made lock with many stacks. Having more pin stacks also means you can have a higher number of unique keys, which is important for *systems* (installations of multiple locks) that might need many distinct locks, like on a large campus. Generally, in the US, pin tumbler locks used on homes have five pin stacks, while padlocks have four, though this varies considerably by brand and model. In the UK, six-pin locks are more common.

Dimple Locks

Dimple locks operate much like pin tumbler locks, except that the cuts are made on the broad, flat side of the key instead of the edge. This has advantages and disadvantages. Because the flat side's surface area is much larger, dimple locks can have more pin stacks than pin tumbler locks without requiring a longer key. However, the cut depths are far more limited, since these keys are usually no thicker than pin tumbler keys. Figure 3-21 shows a typical dimple lock and key.

Figure 3-21: A six-pin dimple lock and key

Figure 3-22 shows a more advanced set with over a dozen cuts.

Figure 3-22: A high-end Euro profile cylinder dimple lock and key

Many dimple lock keys are made to be reversible so they can be inserted with either face up, but this limits the cut depths even further. As a result, while many pin tumbler locks have about 7 to 10 possible cut depths, dimple locks may have only 2 to 4.

Tubular Locks

Tubular locks have the same parts as a pin tumbler, though they are organized differently. The pin stacks are arranged in a circle, with the key pins all pointing toward the face of the lock. A tubular lock's key is a metal tube with the bitting usually notched in a circle on the tip, as shown on the right in Figure 3-23. The bitting for the key on the left is inside the tube.

Figure 3-23: Two styles of tubular keys

Tubular locks are typically found on vending machines, gas pumps, and arcade games; bicycle locks and laptop locks also are often tubular. The number of pins varies by brand, but seven-pin locks like the one shown in Figure 3-24 are the most common (the seventh pin in this image, at the 3 o'clock position, may be difficult to see). Tubular locks are sometimes referred to as *Ace locks* or *Chicago locks*, because the Chicago Lock Company, now known as CompX, has manufactured a popular tubular lock model called the ACE (and later, the ACE II) for decades.

Figure 3-24: A tubular lock with seven pins

In the early 2000s, tubular locks got a bad reputation after several videos and news articles showed that low-end laptop and bike locks could be opened simply by jabbing the barrel of a cheap ballpoint pen into the keyway. Quality tubular locks like the ACE II aren't susceptible to this kind of attack, but the perception that all tubular locks are bad still persists.

While tubular locks can be picked with standard picking tools, the process is tedious, as you must pick each pin stack multiple times while rotating the plug. Using specialty tubular picking tools that keep the picked pin stacks at the shear line is much easier but can be expensive, as you'll need different tools for tubular locks of different diameters.

Wafer Locks

A *wafer lock* also works similarly to a pin tumbler lock, but instead of pins, it contains flat, spring-loaded wafers that move up and down, riding along the surface of a key. A bit of metal protrudes from the top and bottom of each wafer, blocking the plug from rotating if the wafer is too high or too low. Figure 3-25 shows a wafer plug with five wafers protruding from the top, and a sixth wafer-like clip that keeps the plug in the housing.

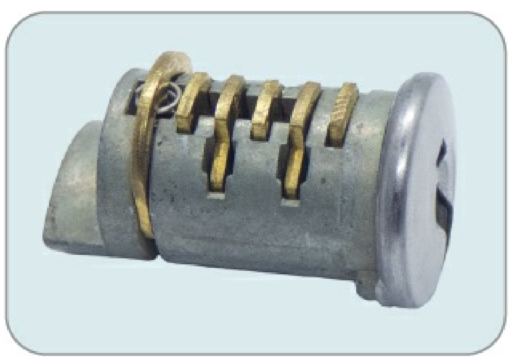


Figure 3-25: A wafer lock plug

Wafer locks are frequently found on automobiles and on furniture such as file cabinets. Low-end safes, like fire-rated document boxes and cash boxes found in big box stores, often feature cheap—and therefore exceptionally poor—wafer locks.

Wafers are thinner than pins, so a wafer lock can hold more wafers than the number of pins in a pin tumbler lock of the same size. It's common to find 10-wafer automotive locks. However, like dimple locks, wafer locks are typically limited to only three or four possible key cut depths. Figure 3-26 shows a wafer lock cylinder and key.

Figure 3-26: A DOM wafer lock cylinder and key

Combination Locks

Instead of using a key, you unlock dial-based, or *combination*, locks by dialing a series of numbers. Combination locks range from the cheap padlocks ubiquitous in gym locker rooms to high-end safe locks used to secure secret government documents and vault doors in large banks. The method of inputting the combination and the internal mechanism varies among locks, so we'll focus on safe locks—those found on decent safes, not the cheap, allegedly fireproof boxes you can buy at an office supply store.

A safe lock has a dial on the face that you spin clockwise and counterclockwise to input a numeric combination. Behind this dial is a *dial ring*, which has an opening index mark, often at the 12 o'clock position, to indicate where you should stop when entering a number before changing direction to enter the next number in the combination. The dial ring also usually has a change index, typically at the 11 o'clock position, where you can enter a new combination if the lock is in its combination change state. (You do so by first unlocking the lock, then inserting a special *change key* into the back side.) Figure 3-27 shows a dial ring and dial.

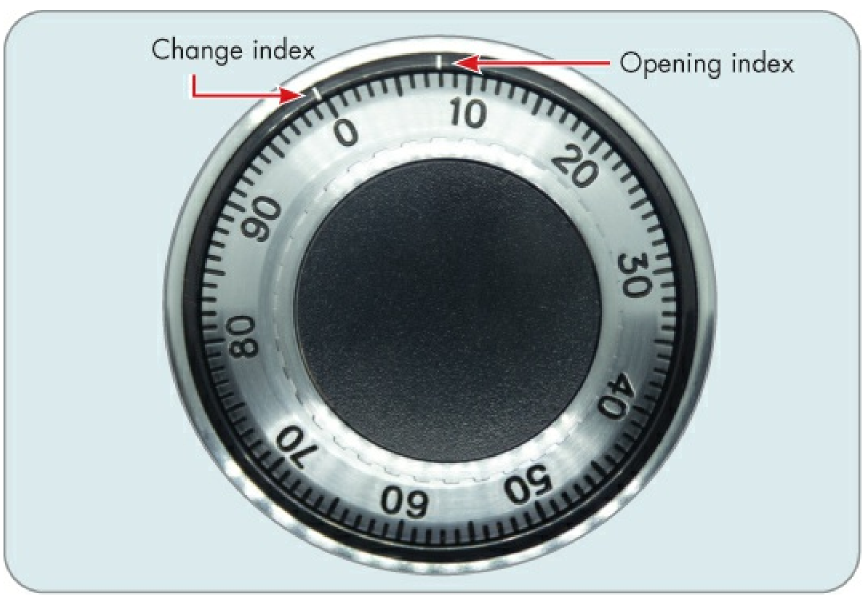


Figure 3-27: The dial and dial ring of a safe lock

Inside the lock, the spinning of the dial rotates the wheels within the wheel pack. When all the wheels are aligned in the correct position, the fence drops into the groove created by their gates. With the fence in the gates, rotating the dial will pull a lever connected to the fence, which is connected to the bolt and opens the lock. Figure 3-28 shows the wheel pack and fence of a cutaway safe lock. We'll discuss opening safe locks in Part IV.

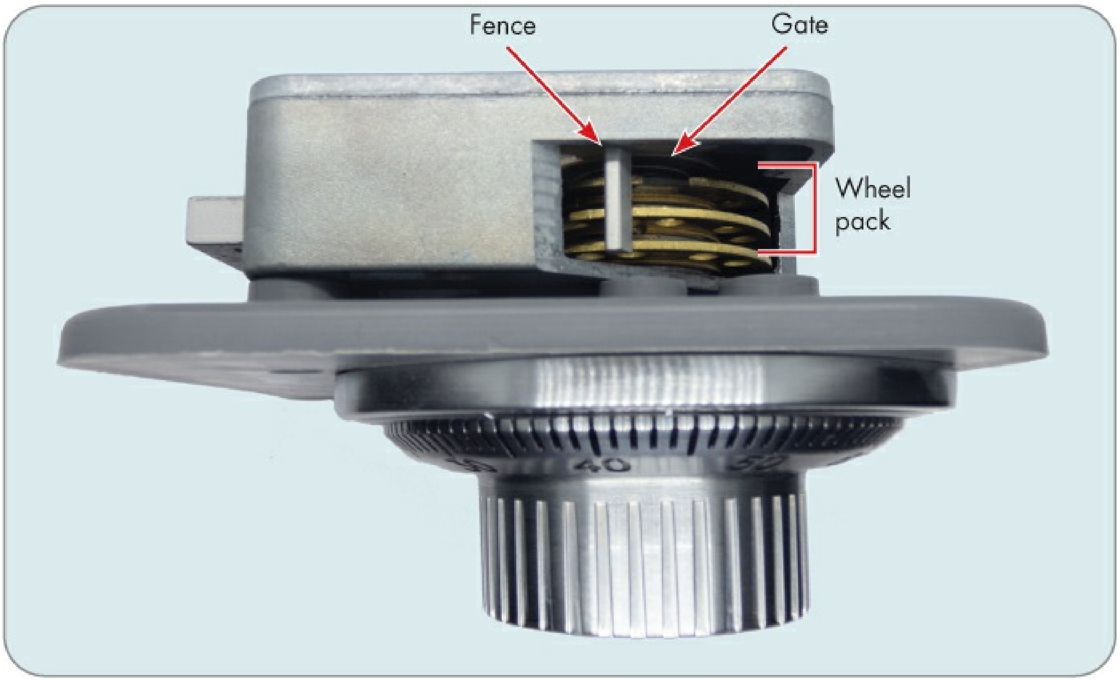


Figure 3-28: A safe lock cutaway showing the wheel pack and fence

Lever Locks

Rather than using pins, *lever locks* have metal levers that pivot and are lifted by a key. Each lever has a slot and a gate where a metal protrusion on the lock's bolt, called the *stump*, rests and can pass through. When the slots on each lever align, the stump can pass through to unlock the door. Lever locks come in padlock format, but the mortise lockset format, shown in Figure 3-29, is the most common type.

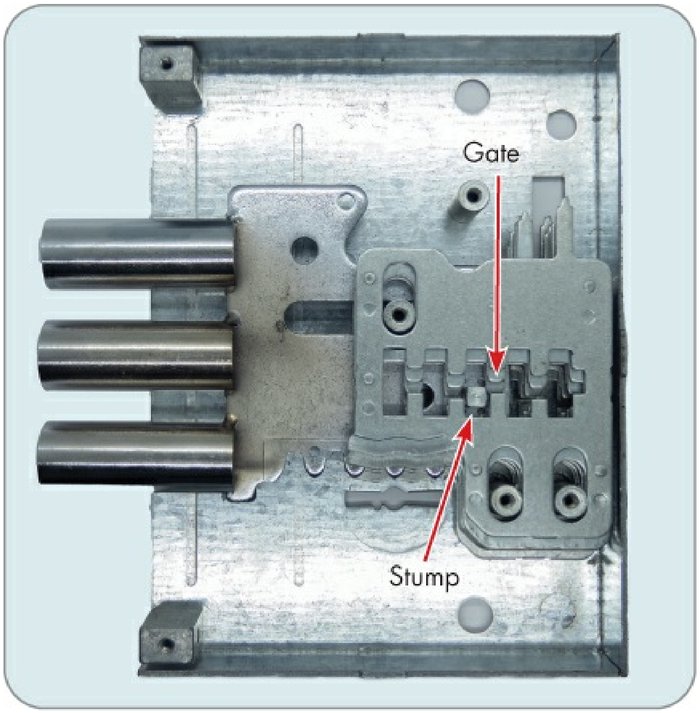


Figure 3-29: A Russian-style mortise lever lock with its case removed

Generally, the more levers a lock has, the more pick resistant it is. Many lever locks have five levers, though models with as few as three or as many as eight are also common. Figure 3-30 shows a key lifting the levers of the lock in Figure 3-29. This lock normally contains eight levers, but four have been removed here to better show how the key and levers interact.

Figure 3-30: The bitting of a key lifting the levers

We'll discuss lever locks in depth in Part V.

Warded Locks

Warded locks are similar to lever locks, but they have only a single lever that opens the lock.

While that might not sound very secure, these locks also rely on *wards*—obstacles within the lock that block pieces of metal other than the key from activating the lever. Figure 3-31 shows a warded lock and key.

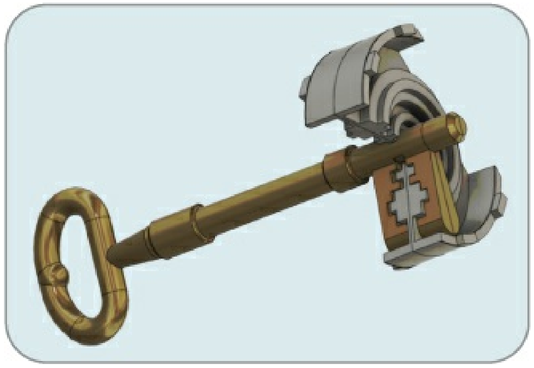


Figure 3-31: A warded lock and its key

Skeleton keys originated from warded locks. The idea of a skeleton key is to remove as much material as possible (leaving only the "skeleton" of the key) while still allowing the key to contact the lever and open the lock. Removing the excess material increases the likelihood that the key will work in other warded locks, as the metal that may have gotten bound up in the wards is gone.

Many older warded locks are quite beautiful, with intricately designed wards and keys. Warded locks are still made today; Master Lock sells a warded padlock, shown in Figure 3-32.

Figure 3-32: A modern warded lock

While warded locks can't compete with more modern mechanisms, they're sufficient for some applications, like furniture locks or as part of a multilayered security system. And with fewer moving parts than most other locking mechanisms, they're sometimes purchased for low-security outdoor or industrial uses, such as lighting controls in public parks.

Since opening such an easy lock doesn't involve much sport, warded locks generally don't appear in locksport competitions. That said, a good understanding of warded locks can be helpful for picking lever locks. We'll discuss them further in Chapter 15.

Disc Detainer Locks

Finally, the *disc detainer* is a unique locking mechanism that uses thin, round discs not unlike the wafers in wafer locks. However, instead of using springs and being lifted, the discs rotate into position. Each disc has a small gate in its outer edge, similar to that in a safe lock's wheels. If the gates on every disc align, a *sidebar*—a metal bar that normally blocks the plug from rotating, somewhat akin to a fence—drops into the groove, and the plug can then rotate to open the lock (see Chapter 7). The bitting on a disc detainer key is a series of angled cuts designed to align the discs.

Because of their unique design, picking disc detainer locks requires specialty tools. In addition, different models often require different tools because of variations in the way the locks are tensioned or in the shape of the keyway. The number of discs in each lock can range from a few in basic models to more than 10 in higher-end offerings.

The disc detainer locking mechanism is found in some high-quality bicycle locks, a few models of padlocks from German manufacturer ABUS, and, most commonly, in offerings from the ABLOY brand of locks.

ASSA, ABLOY, AND ASSA ABLOY

Disc detainers were first created and sold by the ABLOY lock company in Finland in the early 1900s. ABLOY is still the leading manufacturer of disc detainer locks, and its high-end disc detainer models, such as the ABLOY Protec^2 shown here, are considered some of the most pick-resistant locks sold today.

If ABLOY sounds vaguely familiar, that's probably because Swedish lock company ASSA merged with it in the mid-1990s, forming the ASSA ABLOY Group. In the years since, ASSA ABLOY has acquired many other lock manufacturers, including Yale, Medeco, Vachette, UNION, Lockwood, KESO, Corbin Russwin, and Mul-T-Lock, making it one of the largest lock manufacturers in the world.

Summary

This chapter covered basic terminology for the parts of a lock and examined how those parts work together in common locking mechanisms. In the next chapter, we'll look at specialized components and mechanisms that make locks high security or pick resistant.

4
HIGH-SECURITY LOCK ELEMENTS

Nearly every lock manufacturer touts the strength and security of its locks, often using rugged-sounding slogans like Master Lock's "Tough Under Fire" on basic locks. But what really makes a lock high security? This chapter addresses that question by looking at the most common elements manufacturers add to locks to increase their pick resistance.

For banks, governments, militaries, and other entities with significant security concerns, a *high-security* lock is one that takes a lot of time and effort to open without the correct key. Such a lock will be resistant to cutting, drilling, hammering, and sawing, and maybe even bullets, acids, X-rays, and extreme temperatures. Every lock will eventually give way to a barrage of attacks; a high-security lock must simply survive longer than the time needed for someone to notice the breach and sound the alarm.

As locksporters, we're less interested in the strength of a lock's body, bolt, or shackle; rather, we care about the resistance of its internal mechanism to picking, impressioning, and decoding. Luckily for us, some lock designers have invested as much effort in hindering picking as they have thwarting drills, which means we have a wide variety of challenging locks with interesting internals to pick. As a rule, the more elements a lock has, the harder it will be to pick. A high-end lock may have two or three locking mechanisms, all of which need to be defeated before it will open. The main variables that affect a lock's pick resistance are *double-acting* (moving) elements—its pins, sidebars, interactive elements, and so on—and wards or intricate keyways, the obstacles within a lock, introduced in Chapter 3. We'll start by looking at the moving elements.

NOTE

Some manufacturers have designed hybrid electromechanical locks for their high-security offerings. These locks usually rely on the standard mechanical elements plus additional electronic components, such as radio frequency identification (RFID) transponders, Bluetooth, or infrared signals. We won't be investigating these hybrid systems, as they are outside the realm of locksport, and this book focuses exclusively on mechanical locking elements.

Off-Axis Pins

The most obvious aspect that determines pick resistance is the number of parts that prevent the plug from rotating, known as *blocking elements*. Typically, these are pins. In the past, four- and five-pin locks were common. Today, even most low-end door locks have at least five pins, though six is common in Europe. Some manufacturers have taken pin counts to the extreme, such as the Swiss brand Kaba; the Kaba Penta has about 15 pins, and the Kaba 20 has up to 20 pins coming from multiple directions!

If you're a beginner, you'll typically remove some pins in practice locks. You might pick a one- or two-pin lock as your first challenge and then graduate to more pins as you gain experience (we'll discuss how to repin locks in Chapter 5). Even the best pickers frequently remove some parts from their new target lock while they learn how to manipulate it, slowly working their way up to the full lock.

Increasing the number of pins in a lock has practical limitations, however. First, a key has room for only a limited number of cuts. You can't lengthen keys significantly, since no one wants to carry around a key that's more than about 6 cm (about 2.5 inches) long. You also can't greatly decrease pin size to fit more cuts on a key, as the pins become too weak to prevent *forcing attacks*—brute-force efforts to turn the plug, often with a screwdriver or pliers.

NOTE

Not all manufacturers have shied away from long keys. Some of the locks in Mauer's Redline series use keys that are about twice the length of typical keys. These locks are double-sided Euro profile cylinders, but to open the lock, the key must actuate both the inside and outside portion of the cylinder at the same time! For more details, see "Mauer Locking Systems Thinking Outside the Box" by Barry Wels (https://blackbag.toool.nl/?p=42).

To work around these limitations, manufacturers add pins by placing them on other axes of the plug, taking advantage of unused real estate. This method has two common approaches: using side pins and using trap pins.

Side Pins

Side pins, sometimes called *finger pins*, are usually smaller or shaped differently than standard pins (see Figure 4-1).

Figure 4-1: A side pin from a Schlage Primus lock

As their name indicates, side pins aren't located on the primary shear line (the 12 o'clock or 6 o'clock position). Figure 4-2 shows their placement in one model of lock.

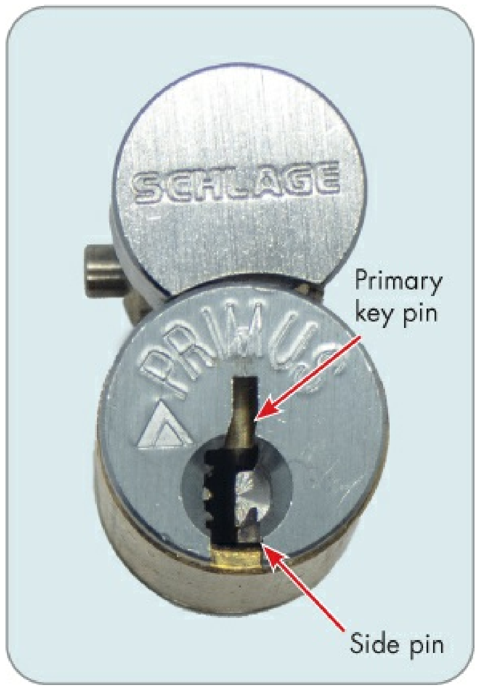


Figure 4-2: A Primus lock with the location of the primary key pin and side pin highlighted

Instead of interacting with the primary bitting of the key, side pins check additional cuts, often located on the broad side of the key blade in pin tumblers, or the narrow edge of the key in dimple locks. Figure 4-3 shows the cuts checked by the side pins in the Primus lock from Figure 4-2.

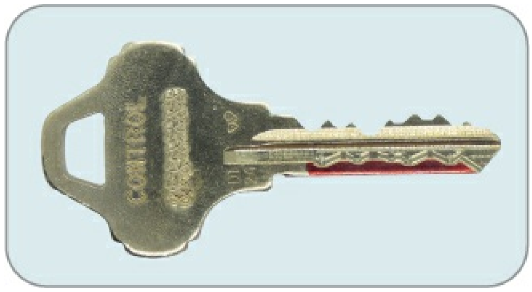


Figure 4-3: The side cuts on the blade of a Schlage Primus key, highlighted in red

Side pins can be placed almost anywhere in a lock. The BEST Cormax series has a side pin at the back of the keyway, with a corresponding cut on the tip of the key. The Australian Lock Company's BiLock brand has some models with two side pins on the face of the lock. Some of the most common locks with side pins are the Schlage Primus (shown in Figures 4-1 through 4-4) and the ASSA Twin series.

Figure 4-4 shows a disassembled Schlage Primus.

Figure 4-4: A disassembled Schlage Primus showing the bottom of the plug, where the five side pins are inserted

These pins serve multiple purposes aside from increasing the difficulty of picking. They can increase the number of possible lock-and-key permutations in a large lock system, and they're ripe for adding new patents to a lock system. They can also be useful for adding some high-security locks to an existing lock system, as keys with these additional cuts often still work in versions of the lock without the side pins.

NOTE

Many high-security locks rely on patents to prevent third parties from making key blanks, thus restricting the supply of keys available to authorized sellers for as many years as the patent is valid. Since a blank key is needed for various attacks on a lock, such as impressioning, a restricted key supply increases the lock's security. When patents are close to expiring, making a few changes to the lock and key, such as adding side pins, can allow companies to get fresh patents and reset the clock.

Trap Pins

Trap pins are just that—a trap for lockpickers. They're an additional row of driver pins typically located a few degrees away from the primary pins. Trap pins permanently disable a lock that has been picked, even if someone later tries to use the proper key, which alerts the owner to the unauthorized access attempt. Locks with trap pins are useful when the desire for high security outweighs the inconvenience of having to replace the lock.

The way trap pins work is simple. When you use a key to turn the plug of a lock with trap pins, the key holds the key pins at the shear line. However, when you're using a picking tool to turn the plug, there's no key to hold the key pins in place, so they move around in their chamber. A trap pin that aligns with that chamber can shoot into it, preventing the plug from turning.

But why can't you then simply pick the trap pins to allow the plug to rotate? Unlike driver pins, under normal operation trap pins never enter the pin chambers in the plug—they're always resting on the plug, held up by the key pins. This means manufacturers can make them more aggressive than typical driver pins by placing them at odd angles, making them in odd shapes or unusual sizes, and giving them different spring weights. All these factors combine to make trap pins incredibly hard to pick.

Determining whether trap pins are in play can be hard. The face of a lock or even its key usually gives no indication. A seasoned lockpicker may know from experience or research that a given brand and model contains trap pins, but otherwise, the best way to tell is by looking at the lock when it isn't mounted. If trap pins are present, you should see an additional row of pin stacks on either side of the lock's bible. Unlike side pins, which are usually set at 90° from the primary pin stacks, trap pins are usually only a few degrees away and have fewer stacks, as shown in Figure 4-5. They're also typically smaller than standard driver pins.

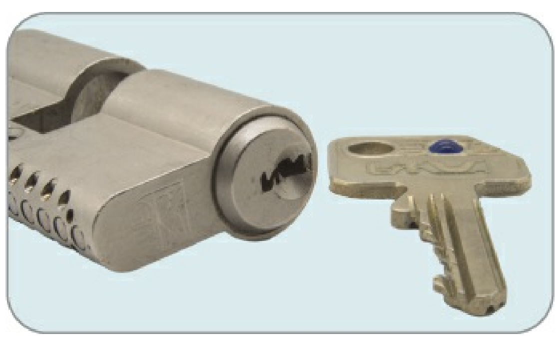


Figure 4-5: A GTV brand lock with a row of trap pins seen on the bible

Most people don't want to be locked out if someone attempts to pick their lock, so fortunately for lockpickers, trap pins aren't terribly common.

Security Pins

Another way a manufacturer can improve a lock's pick resistance is to upgrade the standard pins to *security pins* (also known as *pick-resistant*, or *antipick*, pins). These pins have unique shapes that make them harder to pick. Pins are inexpensive and often designed to be replaceable to allow for rekeying, and a simple change to the pin's shape can greatly increase the difficulty of picking without requiring any other changes to the lock. With this approach, lock companies can offer higher-security versions of existing locks for only cents more in manufacturing costs. (Despite having a bit less material, these pins cost more to make because they require additional manufacturing steps.)

Security pins can be driver pins, key pins, or both. Some manufacturers place them in one or two pin stacks, while others use them in almost every stack. They come in a wide variety of shapes, but we'll focus on the designs typically used.

Spool Pins

The most common security pin is the *spool pin*, so named because it looks like a tiny spool of thread: wide at the top and bottom, with a large groove cut around the middle, as shown in Figure 4-6. Spool pins are most often used as driver pins and have become so common that even inexpensive store-brand deadbolts now often contain one to three spools.

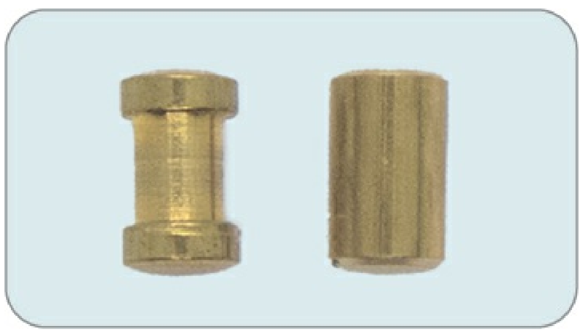


Figure 4-6: A spool driver pin (left) next to a standard driver pin (right)

Spool pins are effective at slowing beginners and moderately skilled pickers. They allow a pin stack to be placed into a *false set*, in which the plug rotates a bit as if that pin stack has been properly picked, when in reality it hasn't. This occurs when you lift the spool pin partway past the shear line into the bible while the plug is being tensioned, as the groove in the spool pin allows it to turn at a slight angle, and its wider top and bottom will *bind* (be wedged or jammed) in the plug and the bible, as shown in Figure 4-7.

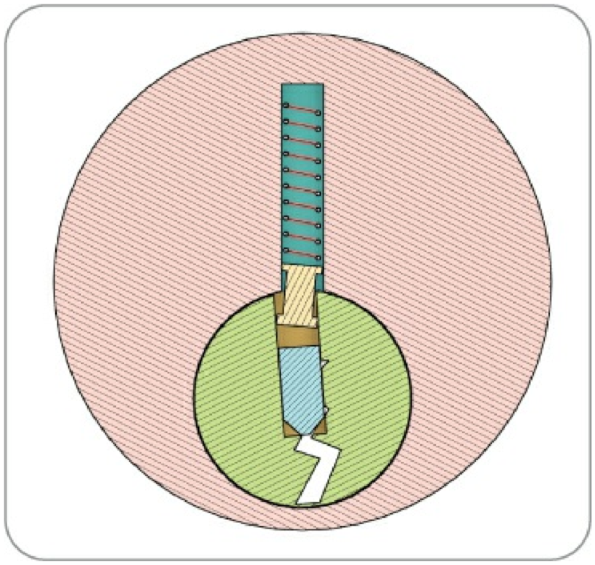


Figure 4-7: A spool pin in a false set

A beginning picker might mistake this slight rotation as having properly set the pin stack, but the plug rotation that occurs from a false set is much greater than when a pin stack is set properly. To overcome a spool pin in this blocking position, you must decrease tension and allow the plug to *counter-rotate*—to turn slightly back toward the locked position—while continuing to lift the spool pin and release it from the bind. This is tricky, as too much counter-rotation will reset all the pin stacks, meaning you have to start all over. We'll explain this technique further in Chapter 7.

A lock should never contain all spool pins. If it did, the plug could rotate several degrees in either direction (as much rotation as a spool allows), which could interfere with using the key. For this reason, locks that rely on spools usually have a standard driver pin in at least one of the pin stacks. In high-security locks, this standard driver pin is often made of hardened steel, instead of the typical brass, to add drill resistance to the lock.

Serrated Pins

Almost as common as the spool pin is the *serrated pin*, which has several very small grooves cut into it, much shallower than a spool pin's central groove (Figure 4-8).

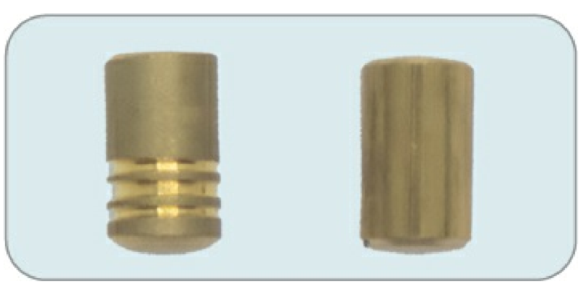


Figure 4-8: A serrated driver pin (left) next to a standard plain driver pin (right)

Rather than bind like a spool pin, serrated pins will repeatedly snag on the bible while being lifted, producing small clicks on your tension tool that can give the impression that the pin is set when it isn't. This snagging makes it feel like there's dirt or grit in the lock, even if it's new.

Although serrations are most often used on driver pins, some American-brand padlocks and some newer ABUS locks use them in key pins as well. Some manufacturers combine serrations and spools, making lockpicking a bigger challenge.

Some lock builders also *countermill* (cut threads into) the pin chambers in the bible, although this feature is uncommon in commercial locks. These threads snag on the serrations, making the pin even more difficult to lift.

Chisel-Tipped Pins

One of the more interesting security pins is the *chisel-tipped pin*, found inside most Medeco locks like the Biaxial and M3. Typical key pins come to a dull or fine point, like a ballpoint pen or pencil, to ride along the surface of the key's bitting. In most Medeco locks, the key pins have angled tips, like that of a chisel, as shown in Figure 4-9.

Figure 4-9: Medeco Biaxial pin

The purpose is right in the name *Biaxial*: these locks check two dimensions of their keys rather than one. Chisel-tipped pins have to be not only lifted to the correct height, but also rotated within the lock to the correct orientation. Accordingly, the cuts on the key aren't made perpendicular to the blade, but at various angles, into which the chisel tip of the pins will drop. Figure 4-10 shows the side of a Medeco key, which looks similar to many keys from this perspective.

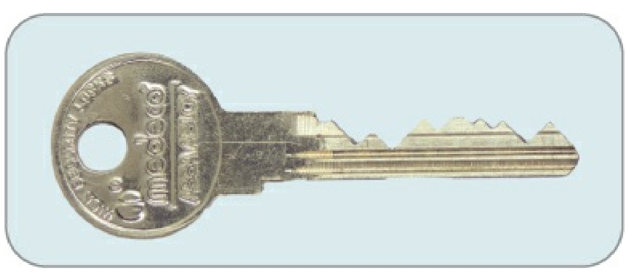


Figure 4-10: Side view of the Medeco Biaxial key

However, when you view the key from above, as in Figure 4-11, you can see the varying angles of some of the cuts.

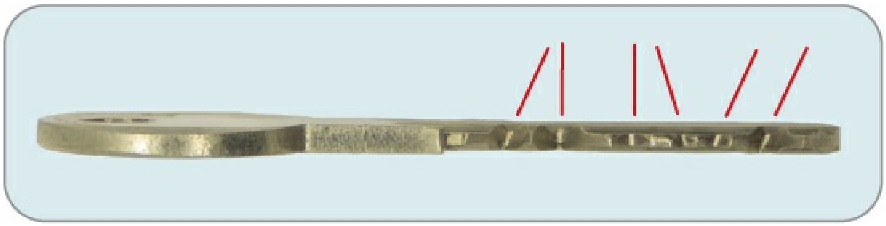


Figure 4-11: Top view of the Medeco Biaxial key

The pins have corresponding grooves cut vertically into them to check the rotation. The plug contains a sidebar that drops into these grooves when they're all aligned. We'll discuss sidebars more later in this chapter.

Pin-in-Pins

The final security pin design to cover is the *pin-in-pin*, or *telescoping pin*. These pins, which can replace a typical driver or key pin (or both), consist of a hollow tube or pipe-shaped pin surrounding a second, thinner pin. Figure 4-12 shows a set of telescoping driver and key pins.

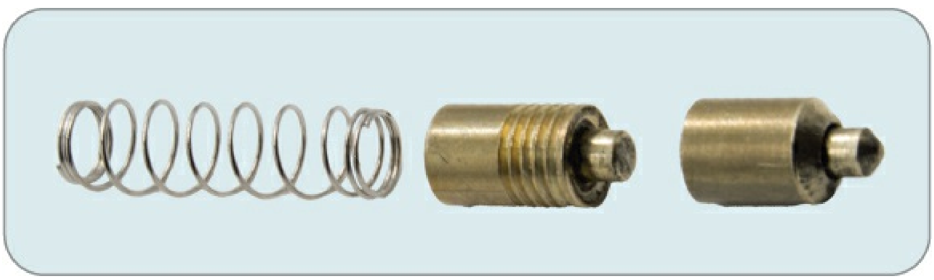


Figure 4-12: One pin-in-pin stack from a Mul-T-Lock; from left to right: the spring, inner and outer driver pins, and inner and outer key pins

To set this pin stack, you must lift both the inner and outer pins to the correct height. The pin-in-pin is seen almost exclusively on dimple locks, like the high-end Mul-T-Lock and KESO locks, where a second cut can be drilled in the center of a larger dimple. You can see the concentric circle cuts indicative of pin-in-pins on the Mul-T-Lock key in Figure 4-13.

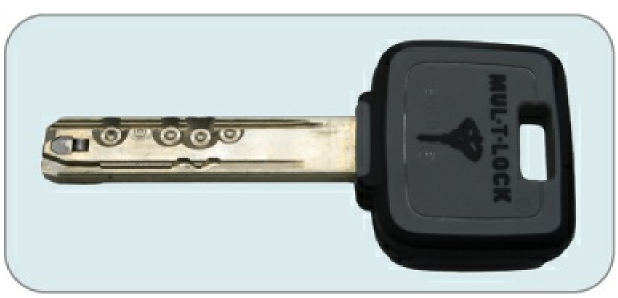


Figure 4-13: A Mul-T-Lock dimple key with donut-shaped pin-in-pin cuts

In Figure 4-14, this key is inserted into its cutaway lock and turned, showing the nested pins in both the bible and the plug.

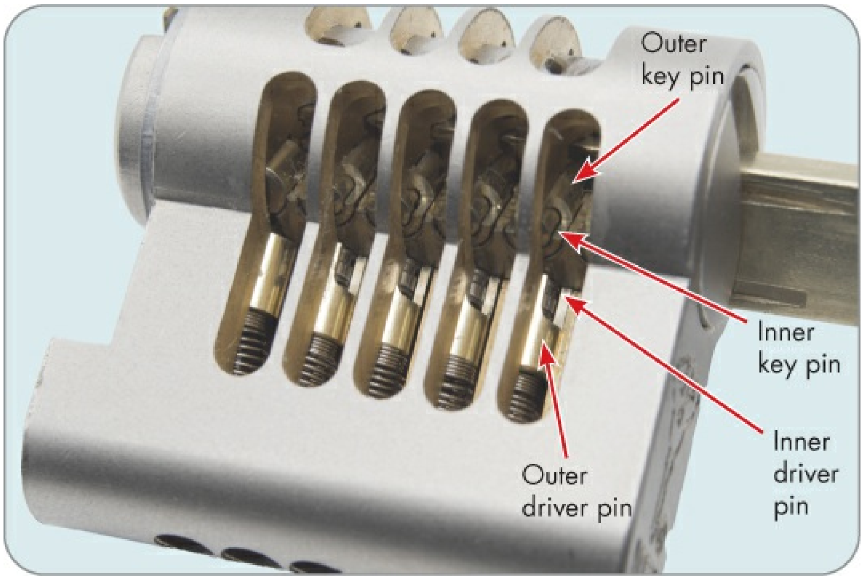


Figure 4-14: A Mul-T-Lock cutaway showing pin-in-pins

Other Pin Shapes

What do mushrooms, bombs, bullets, barrels, and bottles of booze all have in common? Their shapes have inspired various security pin designs. Any shape that provides unusual or inconsistent feedback during picking but still behaves well when operated with a key has the potential to increase a lock's pick resistance.

Those who like a bit of whimsy in their locks can find novelty pin shapes on the market. SPARROWS Lock Picks sells driver pins shaped like chess pieces, ammunition, and even Christmas trees and snowmen, all designed by noted UK locksporter Lock Noob. While perhaps not practical for widespread use, these pins do meet the objective of providing unusual feedback during picking! Several of these pins are shown in Figure 4-15.

Figure 4-15: A variety of specialty pins

Sidebars

In a typical pin tumbler lock, the driver and key pins collectively prevent the plug from rotating, and thus the lock from opening. Many high-end locks go a step further and add a sidebar. As Chapter 3 explained, a *sidebar* is a piece of metal that runs the length of the plug and rests in a notch in the housing. The plug has a corresponding slot that the sidebar can drop into when the proper key is inserted, allowing the plug to turn. Figure 4-16 shows an engaged sidebar inside a cutaway lock.

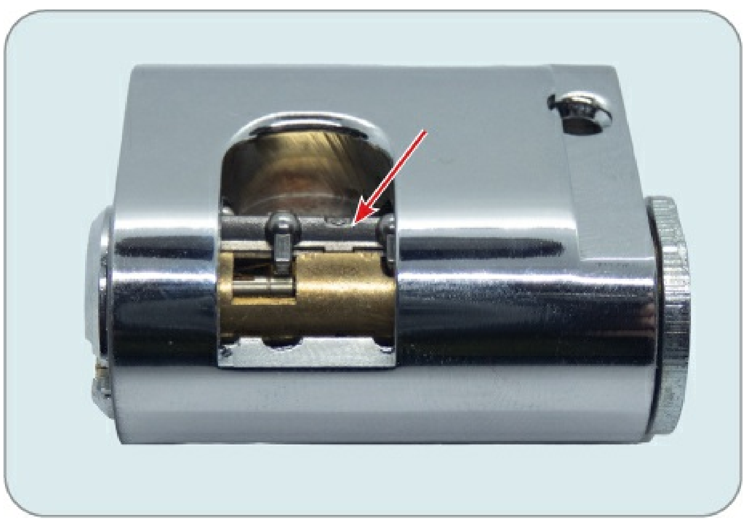


Figure 4-16: A BiLock cutaway lock, revealing a locked sidebar

Figure 4-17 shows the same lock with the key inserted to release the sidebar.

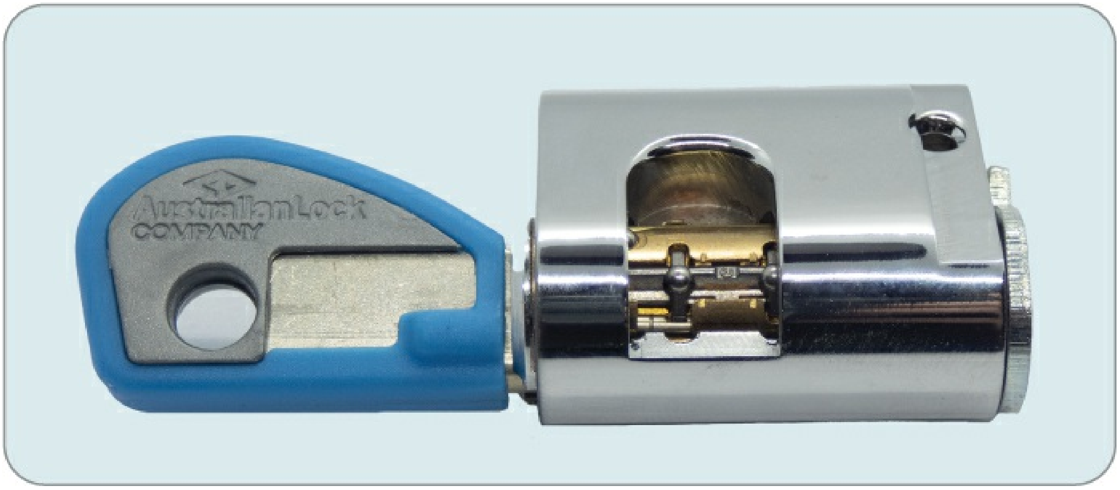


Figure 4-17: The same lock as Figure 4-16, with its key inserted, releasing the sidebar into the plug

The mechanism that prevents the sidebar from dropping into the plug depends on the lock. Locks with side pins, such as the Schlage Primus shown earlier, often have those pins block the sidebar until they're properly set. In the disassembled Primus shown in Figure 4-4, the sidebar is the notched metal bar on the left of the pinning tray. These notches interact with the grooves on the side pins, shown in Figure 4-1. The sidebar rests in the long black slit just visible on the plug near the top in Figure 4-4.

Many other locks also have sidebars. On the Medeco Biaxial, the sidebar is freed when all the pins are rotated to the proper angle. Some locks, like BiLock and Medeco brand cam locks, don't use driver pins at all. Instead, the key pins and springs are contained entirely inside the plug, and notches on the side of the key pins interface with a sidebar (or two, in the case of BiLock) as the primary locking mechanism.

Another common sidebar mechanism is the *slider*. A track on the key operates what's essentially a tiny wafer lock that blocks the sidebar until the cuts are aligned. The Mul-T-Lock MT5, M&C Condor, and Yale Superior are all dimple-style locks with a slider and sidebar, and the M&C Matrix is a pin tumbler with five pins and five sliders. Figure 4-18 shows a key with a slider track.

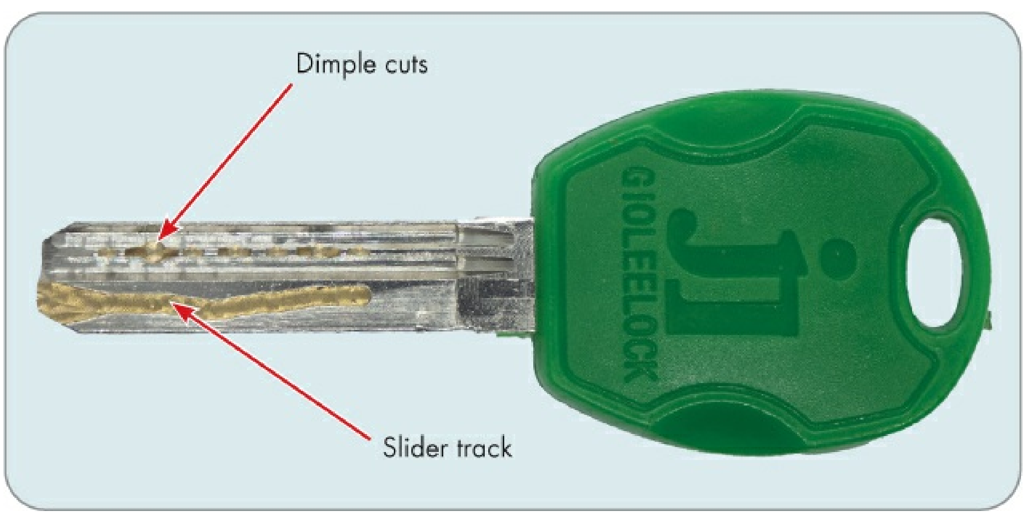


Figure 4-18: A dimple lock key with a slider track

We'll talk more about sliders in Chapter 7.

Wards and Paracentric Keyways

Adding more parts to a lock is a good way to increase pick resistance, but it also adds complexity and cost to both manufacturing and servicing. A simpler approach is to make it harder to reach the pins with a picking tool. To do this, manufacturers add wards to their plugs or create oddly shaped keyways.

As discussed in Chapter 3, *wards* are metal protrusions designed to prevent things other than the properly shaped key from being able to fit or rotate in the lock. Warding can limit the space available for picking tools. In particularly unlucky cases, a picking tool might even get wedged in the wards and be difficult to remove without breaking.

Nonuniform—or paracentric—keyways have wards that cross their centerline, giving them a zigzag appearance. While many keyways are technically paracentric, the paracentric keyways in high-security locks are often extreme, with narrow spacing between wards and severe angles. Picking a lock with such a keyway requires very thin picking tools (which give less feedback, cost more, and are more prone to breaking) and a variety of tension tools to find one that can fit well without popping out or filling the limited available space.

Many notable locks have paracentric keyways. Medeco KeyMark locks rely principally on their keyways for additional security beyond the standard pin tumblers inside. Their keyways, one of which is shown in Figure 4-19, are so oddly shaped that at first glance the lock looks like someone attacked it with hand tools.

Figure 4-19: A paracentric keyway in a KeyMark lock

ABUS also makes complex keyways, including one that appears to spell out *ABUS* (Figure 4-20). Many major brands offer at least one paracentric keyway, including ASSA, BEST, CISA, and Lockwood.

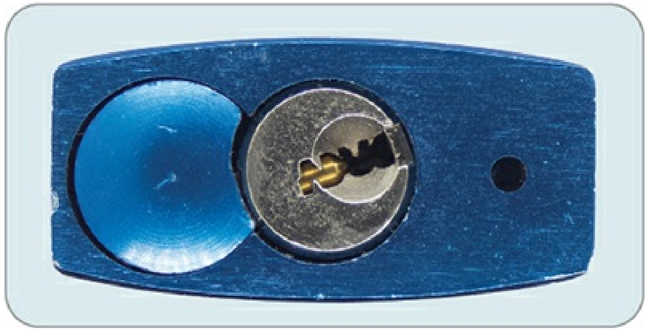


Figure 4-20: An ABUS 72 padlock with the ABUS keyway

Paracentric keyways cost more to make because the plug requires more passes through machining tools. Additionally, key blanks cost more and may be a bit sharper or more fragile because of the grooves milled into the key blank. As a result, paracentric keyways are often reserved for higher-end locks.

Interactive Key Elements

A lock's inner mechanisms aren't the only factor manufacturers can refine to improve security. Some brands have started building interactive, or movable, elements into their keys, which are checked by the lock during operation. These interactive features serve several purposes.

First, they make illicit key duplication difficult. If you've watched enough spy films, you've probably seen a special agent press a key into clay and later make a duplicate by pouring a low-melting-point metal into the mold. That's not possible with these interactive elements. Even 3D printers can have a hard time re-creating them.

Second, these elements can make picking harder. Depending on the design, picking a lock that uses interactive keys might be as simple as lifting one additional pin inside the lock with your picking tool, or it might require making several moves during picking.

Finally, lock manufacturers often want to extend the life of an existing line of products. Adding a new interactive element can justify new patents, allowing the manufacturer to continue restricting the supply of key blanks and thus continue selling the lock as a high-security product.

Many high-end brands use interactive elements, especially those owned by ASSA ABLOY. Its Mul-T-Lock brand introduced a moving dimple key element on its Interactive product in 1994, which raises one pin stack higher than otherwise possible. ABLOY's current top-of-the-line Protec^2 features a ball bearing located next to the bow of the key that shifts as the key is turned (Figure 4-21).

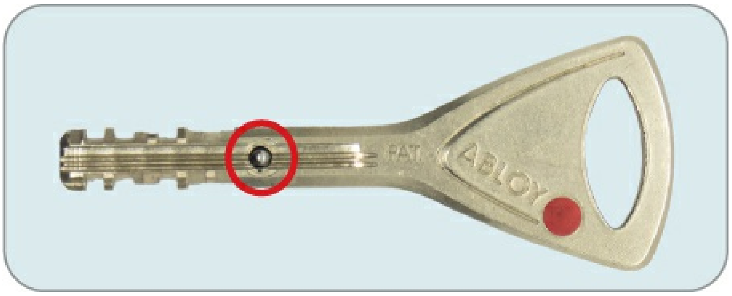


Figure 4-21: An Abloy Protec^2 key with a movable ball bearing

ASSA ABLOY's KESO brand has spring-loaded pins inside the key of its $8000\Omega^2$ system (see Figure 4-22). These pins protrude slightly from either side of key's tip and are patented until 2034.

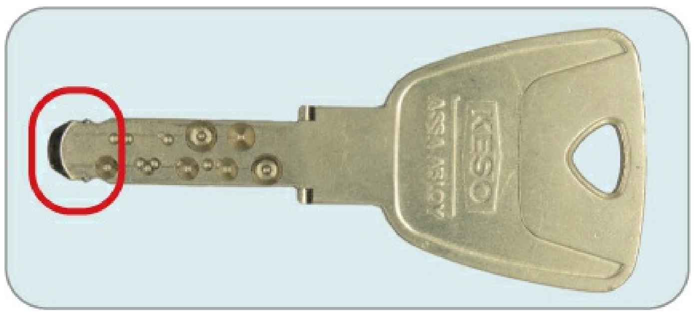


Figure 4-22: A KESO $8000\Omega^2$ key with active pins at the tip

Aside from ASSA ABLOY, the BiLock brand also includes interactive elements in some products. Its NG and QC lines include a pivoting bar within the key near the bow. This part releases either the sidebar or the plug retention mechanism, depending on the model.

Magnets

Magnets are used across several lock brands, from the Avocet ABS, which uses a single simple magnet to pull a pin rather than depress one, to the EVVA MCS, which uses eight magnetic rotors and is one of the highest-security locks available. (Imagine almost every interactive element you've read about thus far, plus a magnet!)

On the MCS, each magnet "pill" on the key (Figure 4-23) rotates the rotors as the key is inserted. Each rotor has a gate, and once all the gates are aligned, two sidebars retract, allowing the plug to turn.

Figure 4-23: An EVVA MCS key with four circular magnet pills on the blade of the key

Figure 4-24 shows a cutaway EVVA MCS lock.

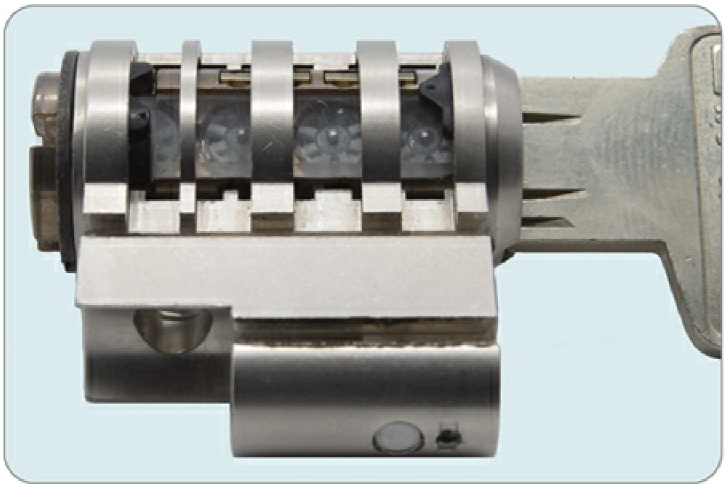


Figure 4-24: A cutaway EVVA MCS lock with key inserted. The rotors are the spoked wheels.

Fortunately, locks with magnet-based mechanisms are beyond what you'll typically find in competitions.

Summary

In this chapter, we reviewed enhancements that lock manufacturers can add to their locks to make them more difficult to pick. These include curiously shaped pins, sidebars, paracentric keyways, and keys with interactive elements. In the next chapter, you'll start to get your hands dirty as we discuss basic lock maintenance procedures—including disassembly, reassembly, and repinning—that all locksporters should know.

5
LOCK MAINTENANCE FOR LOCKSPORTERS

Although locksporters have a good understanding of how locks work, there's a big difference between what we do and what locksmiths do. Locksmiths need to worry about properly installing lock hardware, repairing broken mechanisms, calculating master-key systems, duplicating keys, assisting during lockouts, and maintaining locks.

We should leave locksmithing to the professionals. However, certain aspects of lock maintenance are valuable for locksporters to know, such as disassembling locks to better understand their mechanics, repinning locks to make them easier or harder to pick, reassembling locks after they come apart, and lubricating locks when they become hard to operate. Locksporters eventually amass quite a collection of locks, and it wouldn't be practical to have these serviced professionally every time we wanted to try picking a different bitting or swapping in some high-security pins.

WARNING

Just as we advise you not to pick locks you own that are still in service (like the one for your front door), we also recommend not servicing your own locks that are in use. You don't want to risk damaging anything important. A professional locksmith can ensure that not just your lock, but also whatever it's attached to, is in good working order.

This chapter focuses on pin tumbler locks, as they're the most common and often can be serviced by the user.

Disassembling Locks

Taking apart a lock has several uses in locksport. You may want to examine the types of pins used in the lock, replace parts if it is malfunctioning, or repin it (covered in the following section). Many locksporters on YouTube and other video platforms will disassemble a lock immediately after picking it to prove to viewers that the lock hasn't been modified.

Locks tend to have a lot of small parts that are often under pressure from springs. The first lock you disassemble should be an inexpensive one with readily available spare parts, just in case you lose any pieces in the process.

Useful Tools

You'll need a few tools on hand before you disassemble a lock. Some can be found at hardware stores, and all can be purchased on locksmith-focused websites—though some sites won't sell to nonprofessionals. See Appendix B for a list of vendors that sell lockpicking tools to hobbyists.

Screwdrivers

Locks often have components, such as cams, that are held on with screws. You'll need a good set of flathead and Phillips screwdrivers of various sizes to remove these parts. Purchase a set of hex wrenches as well, since some manufacturers prefer these over standard screws.

Tweezers

Having a decent pair of tweezers is great for picking up and placing small parts. We suggest investing in a pair of *pinning tweezers*, shown in Figure 5-1, which have a groove or bend in the tips to grip cylindrical objects like pins and springs.

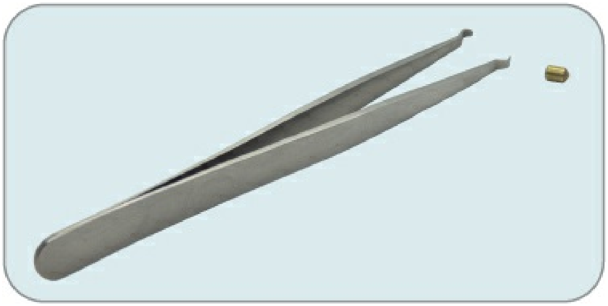


Figure 5-1: Pinning tweezers

Plug Follower

Since parts in the lock are under spring tension, quickly pulling the plug out of the housing risks sending springs and pins flying everywhere. To avoid this, use a *plug follower* (Figure 5-2), a small plastic or metal tube you slide in behind a plug to keep everything in place until you're ready to remove the pin stacks one by one. The plug follower should be the same size as the plug you're removing, so find a set that includes several sizes. If you have access to a 3D printer, you can find a variety of plug follower designs online, such as the one from Harley Ross (WestCoastPicks) at *https://www.thingiverse.com/thing:2981544*.

Figure 5-2: Plug followers in a variety of sizes and materials

Pinning Shoe

For a double-sided Euro profile cylinder, you can't use a plug follower because the other half of the lock is in the way. Instead, you can use a pin retainer tool—often called a *pinning shoe*—to hold the driver pins in place as you remove the plug. A pinning shoe is a long, thin strip of metal with a spring-loaded base that fits around the bottom of the lock's housing. This tool can be hard to find in the US, but you can make one with rigid metal wire, like a section of an old windshield-wiper blade. Figure 5-3 shows a commercial pinning shoe, as well as a 3D-printed version by Thomas Wenzel at redcatimaging (*https://www.thingiverse.com/thing:2457469*).

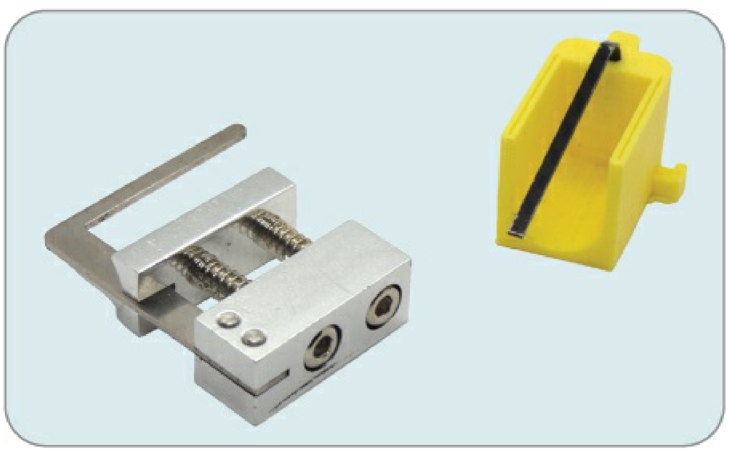


Figure 5-3: A commercial pinning shoe (left) and a 3D-printed pinning shoe (right)

Pinning Tray or Mat

As you're taking the lock apart, you'll want to organize the parts so you can remember where they go. You can set each piece on a *pinning tray* or mat, which usually has numbered slots to help you keep track of which pin stack each pin and spring came from. Plenty of small pinning tray designs are available online to 3D print or laser cut. Figure 5-4 shows a laser-etched tray designed by noted locksporter Datagram that doubled as a LockCon conference badge in 2019.

Figure 5-4: A laser-etched pinning tray holding a disassembled KIK cylinder

You can also peel the top layer off a piece of corrugated cardboard and use the channels to hold pins, as shown in Figure 5-5.

Figure 5-5: Corrugated cardboard: the world's most readily available pinning tray

However, if you have the space on your workbench, consider purchasing a large, commercial pinning mat, which will allow you to work on multiple locks at once. Locksmithing and lockpick manufacturer websites often sell them for $15 or less.

Curved Shim

A *curved shim* is a thin slice of steel foil that you can slip between the plug and the bible from the rear of a cylinder to keep key pins in the plug and keep driver pins in the bible. This tool helps with opening locks you can't yet pick, as you can set the pins one at a time. It also ensures that nothing gets jammed when you're taking apart high-security locks. If you can't find professional locksmithing shims, try cutting open the small security tag found on video game cases; they contain two small pieces of foil that are a bit flimsier than locksmiths' shims (see Figure 5-6).

Figure 5-6: Two professional shims (left) and improvised shims pulled from security tags (right)

Clip Remover

Some brands of locks—mostly Euro profile cylinders—use a *circlip* or *C-clip* (a flat, C-shaped piece of metal) to hold the plug in place. Although you can pry these off with a flathead screwdriver or pair of pliers, doing so will often bend and damage the clip. Instead, we recommend using a *clip remover*, a small claw-shaped blade that can remove C-clips without distorting them (Figure 5-7, top). SPARROWS Lock Picks also sells a multipurpose lock tool called the Gut Wrench that has notches for C-clip removal and installation (Figure 5-7, bottom). Alternatively, a keycap puller—used to remove keys from computer keyboards—can also remove C-clips.

Figure 5-7: A C-clip remover (top) and the multipurpose SPARROWS Gut Wrench (bottom)

Vise

While not strictly necessary, mounting the lock in a vise can make certain steps easier to perform. A vise frees up both your hands for tools; however, since several steps require turning over the lock, you may find a vise more trouble than it's worth.

Now we'll run through the steps to disassembling locks. When you're disassembling unfamiliar locks, locksporter Peter South (@yakMedic) suggests placing the lock in a large plastic zipper-seal bag and disassembling it in there. That way, any loose parts are likely to stay in the bag and not end up lost.

Step 1: Unlock and Remove the Lock

If your lock is currently installed in a door, padlock body, or other type of mount, remove it so you have only the lock cylinder to work with. This process varies depending on the lock, but it typically requires unlocking the lock and then removing one or more screws holding the cylinder in place. If you're disassembling an interchangeable core lock (SFIC or LFIC), remove the core from the housing by using the provided control key (or by picking it, though it can be quite tricky to get each pin stack to the proper height for the control plug to be released).

NOTE

Most inexpensive padlocks can't be rekeyed or serviced by the user. However, some high-end padlocks have removable cores—often by using IC cylinders or by containing a miniature KIK-style cylinder held in place by a screw, typically in the bottom of the shackle's hole.

To remove the plug from the shell, you must unlock the lock, either by using a key or picking. Generally, the method doesn't matter, with one exception: if you're working with a double-sided Euro profile cylinder and want to *decode* the lock—see exactly which pin is in which chamber—you'll need to pick it open rather than using a key.

If you have access to the back of a cylinder for which you don't have a key, you can shim the lock open. Use a picking tool to lift all the pins fully; then slide in the shim from the rear, between the plug and the shell, just below the bible. Keep a little pressure on the shim as you lower the rearmost pin stack, and you'll find that the shim slides into the shear line—but make sure it isn't trapped in a security pin (that is, be sure the shim slides in all the way to the next pin stack). That seven-pin lock is now effectively a six-pin lock if you leave the shim there while picking. If you continue this process, you can easily make a very hard lock into a temporary five-pin lock, pick that, then advance the shim one position, pick it as a four-pin lock, and so on.

NOTE

We highly recommend always using a shim when taking apart a challenge lock or anything with special pins, like a Mul-T-Lock Interactive or a lock with trap pins. Some locks have thinner 2.3 mm diameter pins, which tend to get trapped in the C-clip recess on the back of the plug. A shim avoids these traps!

Step 2: Orient the Plug

Once you've unlocked the lock, you need to be mindful about how you rotate the plug. When the lock is unlocked (or fully picked), the key pins are held in place within the plug, while the driver pins and springs are within the bible. Therefore, if you rotate the plug with the key pins facing down and then remove it, the pins will fall out and scatter everywhere.

When disassembling a KIK, rim, or mortise cylinder, rotate the plug 90°, and then lay the cylinder on its side so the plug is oriented up, as shown in Figure 5-8.

Figure 5-8: A KIK cylinder with the plug turned 90° from the locked position

For Euro profile cylinders, rotate the plug 180° to position the bible at the bottom, as shown in Figure 5-9.

Figure 5-9: A Euro profile cylinder with the plug turned 180° from the locked position

Step 3: Remove the Plug's Retaining Mechanism

Next, you need to remove the part that keeps the plug in the housing. The retaining mechanism varies across lock formats. On mortise cylinders, it's typically a cam held on with a couple of small screws. Remove the screws to free the plug.

With KIK and rim cylinders, the rear of the plug is a bit more complicated. Their plugs are threaded at the end and have a corresponding threaded cap that acts like a bolt on a screw. But the plug's rotation while it's being locked or unlocked will loosen or overtighten the cap. To prevent this and keep the cap moving in unison with the plug, a spring-loaded pin, known as a *cap pin*, extends from the back of the plug and clips into notches on the cap, as shown in Figure 5-10.

Figure 5-10: The rear of a KIK cylinder with the cap pin highlighted

To remove the cap, depress the cap pin by using a picking tool or small screwdriver; then, while preventing the plug from rotating, unscrew the cap by turning it counterclockwise (Figure 5-11).

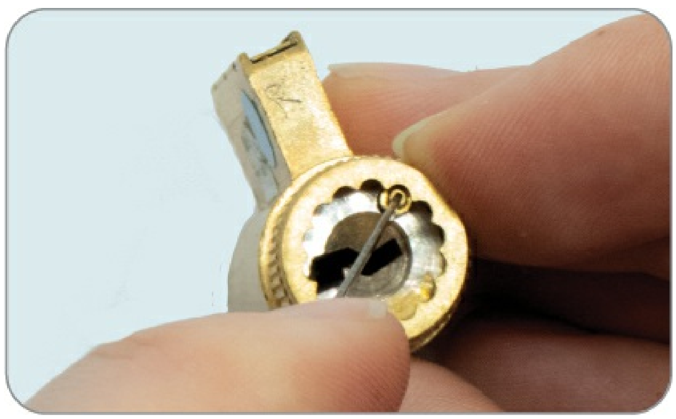


Figure 5-11: Depressing a KIK cylinder cap pin with a picking tool while rotating the cap

Be careful, as the cap pin can go flying if released too quickly. Specialty cylinder cap removal tools can make this process a bit easier, but generally aren't worth buying if you aren't disassembling these cylinders frequently. With the cap now off, use tweezers to remove the cap pin and its spring and set them aside. You may need to turn the lock upside down and tap it to get the spring out of the plug.

NOTE

The two sides of a KIK housing may look symmetrical, but they usually aren't. One outermost pin stack hole is often drilled much closer to the edge of the housing than the other. Note which side of the housing is the front to save you trouble during reassembly.

For double-sided Euro profile cylinders, remove the C-clips by carefully inserting the claw of your C-clip remover into the gap in the clip and prying until the clip partially slides off the plug, as shown in Figure 5-12.

Figure 5-12: Prying a C-clip loose with a clip remover

Then use the clip remover or a pair of pliers to grip the exposed portion of the clip and remove it completely, as shown in Figure 5-13.

Figure 5-13: Removing a loosened C-clip with pliers

Step 4: Install the Pinning Shoe (Euro Profile Cylinder Only)

As mentioned earlier, you'll want a pinning shoe to hold the driver pins in place while removing the plug from a double-sided Euro profile cylinder. You won't be able to get the shoe into the lock if a key is in the plug, however, so if that's the case, leave in the key and skip to step 5. Otherwise, insert the shoe's blade along the bottom of the keyway, depressing all the driver pins into the bible. Slide the bottom part of the shoe onto the bottom of the lock's housing so that the shoe is held snugly in place (see Figure 5-14).

Figure 5-14: A double-sided Euro profile cylinder with a pinning shoe inserted to retain the driver pins

Step 5: Remove the Plug

You're ready to remove the plug and its key pins; this process varies depending on the lock format. Let's start with Euro profile cylinders.

For a Euro Profile Cylinder

If you used a key to unlock the Euro profile cylinder, orient the lock so the bible is down and then slowly pull the key away from the lock—the plug will come with it. The driver pins and springs will pop out of the bible and into the plug's chamber, since no shoe is holding in the pins. Once you have the plug about halfway out of the housing, switch to pulling it directly with your fingers, rather than with the key. Be careful as the plug nears the end of the housing, since the driver and key pins will spill out. For a double-sided Euro profile cylinder, you'll use a plug follower to remove the second plug, as described shortly.

For a picked double-sided Euro profile cylinder with a pinning shoe installed, the process is a bit different. On the first side, use a picking tool to snag one of the key pins, or wedge the tool between the plug and the cam, where the C-clip was. The goal is to extract the plug from the housing enough to grab it and pull it out (as shown in Figure 5-15).

Figure 5-15: Top-down photo of pulling a plug from one side of a Euro profile cylinder

When you pull out the plug, make sure to position it with the key pins facing up so they don't fall out. Followers that are included with pinning shoes have a notch so that you can insert the follower with the shoe still in place and then remove the shoe. A follower is more secure than a shoe and less likely to be accidentally knocked out of place.

Once you've totally removed the plug from one side of the Euro profile cylinder, you'll use a follower to disassemble the second side, regardless of how it was unlocked. Slide out the cam from the center of the lock and remove the C-clip from the second plug. Pass the follower through the empty side of the lock, and then use the directions in "For Other Cylinders," next. You can also follow those instructions if you're working on a *snapped* Euro profile cylinder (one that's been broken in two at the cam joint).

NOTE

Snapped cylinders are common in some locksporters' collections because locksmiths often have scrap-metal buckets filled with them from replacing old locks and are generally happy to sell them to locksporters for the same price they'd get for the scrap metal. It's a cheap way to get practice locks and saves the locksmiths a trip to the recycling center.

For Other Cylinders

For KIK, rim, and mortise cylinders, you'll use a plug follower to push the plug out of the shell. The follower will trap the driver pins and springs in the bible so you can remove them individually. With the lock housing and plug oriented as described in step 2, place the follower on the back of the plug. If your follower has a notch cut in it, be sure that the notch isn't facing the bible. Keeping pressure on the front of the plug with one hand, use your other hand to push the follower until the plug emerges from the front of the housing (Figure 5-16).

Figure 5-16: A plug follower pushing a plug out of its housing

Continue until the plug is completely out of the lock and the follower is slightly protruding from the front of the lock housing, as shown in Figure 5-17. Don't remove the follower yet!

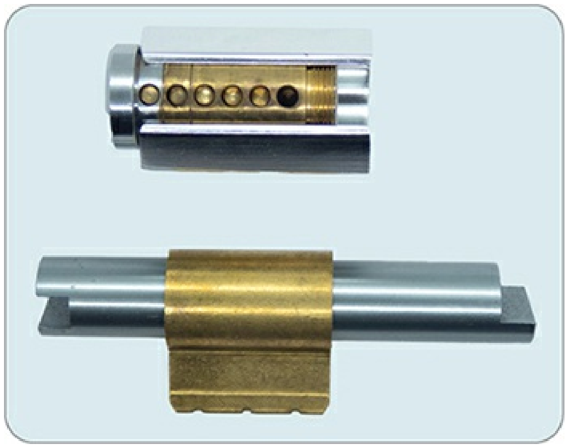


Figure 5-17: A plug follower in a lock's housing (bottom) and the plug with its key pins in a stand (top). This plug has only five out of six chambers filled, which is quite normal on lower-security locks that use the same housings as higher-security models.

Step 6: Dump the Key Pins

Now that you've removed the plug, you have access to the key pins. The easiest way to dump them in an orderly fashion is to place your thumb over the pin chambers, excluding the last chamber, farthest from the face of the plug. Over a pinning tray, turn the plug upside down and, if needed, give it a gentle tap (an older lock might require a bit more force). The pin should fall into the tray. Using tweezers, place the pin into the tray's last pin space.

Slide your thumb back, exposing the second pin hole on the plug, and repeat the process. Do this for each pin in the plug, as shown in Figure 5-18.

Figure 5-18: Dumping the key pins from the plug

Step 7: Release the Driver Pins and Springs

If you intend to rekey this lock, you can stop the disassembly process here, since the key pins are what must match up with the key's bitting, and many locks use the same driver pin length for each pin stack. However, if you want to see what the driver pins look like (curious what kind of security pin the manufacturer put in that pin stack that gave you trouble?) or need to replace the springs, continue with this step.

BALANCED PIN STACKS

While many brands have consistent-length driver pins, not all do. Some locks use a *balanced pin stack*, which means a correlation exists between the driver pin and the key pin lengths: long key pins are paired with short driver pins, and vice versa. Rekeying these locks requires replacing the driver pins as well.

Balanced pin stacks help reduce the pressure on the springs of pin stacks with long key pins. Imagine a key with a very shallow cut near the tip and a very deep cut near the bow. The corresponding lock would have a long pin near the front that would need to be pushed up well into the bible to allow the shallower cuts to pass deeper into the plug. This not only wears out the front stack's spring faster, but also might make the key hard to insert. Balanced pin stacks also stop some advanced attacks, such as decoding the lock by carefully measuring the pin stack when it's pushed all the way to the top of the bible. With uniform driver lengths in nonbalanced stacks, any differences in the height of the pin stacks hint at the relative length of the key pin. The varied driver lengths in a balanced stack don't give you the same clues.

Balanced pin-stack locks don't always have as many possible lengths of driver pins as they do key pins; often they'll have a short, medium, and long driver, each of which is used with two or three key-pin lengths. This makes lock-pinning kits a little less expensive and bulky.

To release the driver pins and springs, orient the lock so the bible is on the bottom. With pinning tweezers in your dominant hand, use your nondominant hand to slowly begin to pull the plug follower or pinning shoe out of the lock and begin to expose the first hole in the bible where a driver pin and spring are held. When the hole is almost entirely exposed, use the tweezers to hold down the pin and gradually release it, as shown in Figure 5-19.

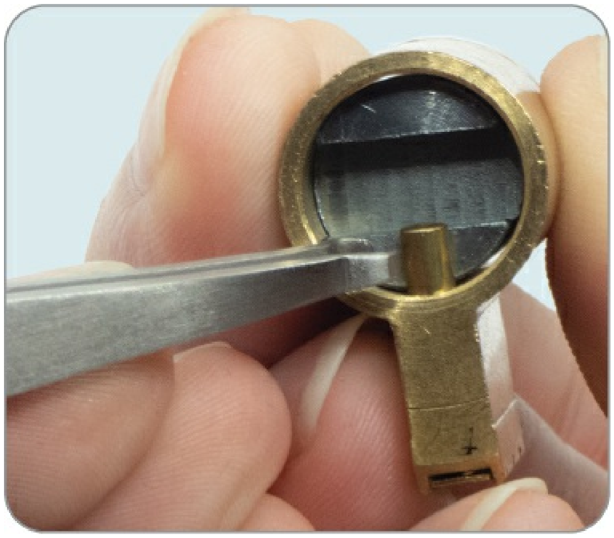


Figure 5-19: Releasing a driver pin

Once the first driver pin is released, use the tweezers to place it on your pinning tray. If the spring is poking out of the hole, gently grasp it with the tweezers and remove it as well. If not, carefully turn the lock over and tap it on the table to dislodge the spring.

Repeat this process until all the pin stacks have been emptied and the follower or shoe is out of the lock. Congratulations! You've completely disassembled a lock.

Repinning Locks

Repinning, or *rekeying*, is the process of reordering or replacing pins to allow a different key to operate the lock. While locksmiths might repin a lock because of a lost key, locksporters do it for other reasons.

One reason might be to build a *progressive lock set*, which includes several locks of the same model that are increasingly difficult to pick. For example, you could buy five KIK cylinders that each have five pin stacks, and then remove four pins from the first, three pins from the second, and so on. This way, you can practice picking locks with only one or two pins before working your way up to the five-pin lock.

Another reason is to change the lock's bitting. Altering the pin pattern can greatly change the lock's difficulty. For example, an alternating high-low bitting such as 1-5-1-5-1 can be more of a challenge than a gradual bitting like 3-2-4-3-2. Even if you don't have spare pins for the type of lock you're repinning, you can rearrange the existing pins.

You might want to repin a lock to make it a *challenge lock*: a lock intentionally modified by a lockpicker to make picking it more difficult. Challenge locks might include custom pins, nonstandard springs, or countermilling. They aren't expected to stand up to regular use, so they might contain unusual pin materials such as wood or glass.

Repinning comes in handy when a lock's current pins or springs are damaged. Locks can become more difficult to pick as some of their parts wear down. While most locks are built to handle thousands of opens, lock designers don't build locks to take the repetitive force encountered in lockpicking.

Before repinning a lock, ask yourself the following questions:

- Do I have spare pins for this lock? (If not, you're limited to rearranging the old pins, but this is still good practice.)
- Do I want to pin this lock so that it can open with an existing key?
- Do I want to add security pins?
- How many pin stacks do I want in use?
- Do I want a particular style of bitting (such as high to low, low to high, or alternating)?

NOTE

An easy-to-pick lock should include standard pins, use few pin stacks, and avoid very long or short key pins. On the other hand, a challenging lock should have various types of security pins, use every pin stack, and alternate key pins in a high-low-high-low pattern.

Once you've answered those questions, select your pins and lay them out in a pinning tray in the order in which you'll place them inside the lock. If you're working with an existing key, set it on your mat to visualize what pins are needed. You can also use calipers or a *key gauge* (a piece of metal with notches and labels to quickly identify the cuts on a key) to determine the correct pin size, which you'll confirm in step 3 of reassembly.

If you're replacing the driver pins, arrange the new ones on the pinning tray above each key pin. If the lock you're assembling uses balanced pin stacks, be sure to use the proper driver pin length by checking the lock manufacturer's specification sheet for that series of lock. One especially useful reference site is the Locksmith Security Association of Michigan's tech manual library (*https://lsamichigan.org/tech_manuals.xhtml*).

If using spool driver pins, be sure that at least one is standard; otherwise, the plug will drift a few degrees and can make the lock bind when a key is inserted. Finally, if you're removing pin stacks to make a progressive lockset, remove any driver pins and springs corresponding to removed key pins, or else the drivers will shoot down into the plug when you reinsert it. Figure 5-20 shows a pinning tray with key and driver pins chosen to match an existing key.

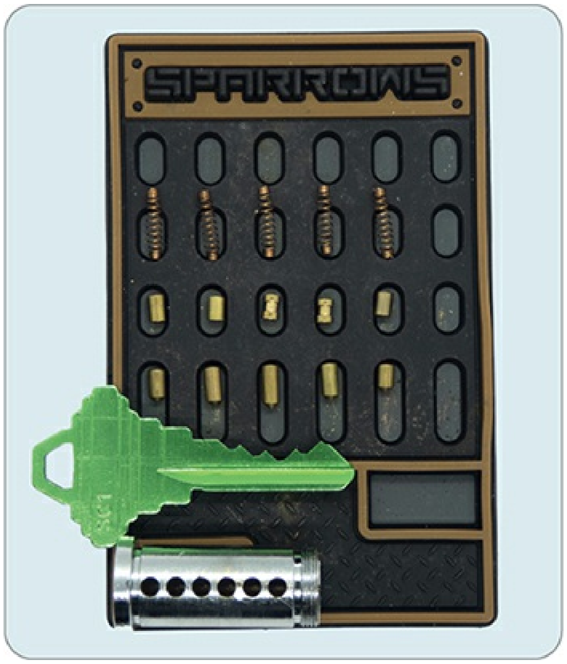


Figure 5-20: A pinning tray with key and driver pins selected to match a key

MACS

The *maximum adjacent cut specification (MACS)* refers to a manufacturer's rules for permissible cuts for a given model of lock and key. These rules state how big the difference can be between the cuts at two adjacent positions on a key. MACS prevents potential problems with making or using certain keys. An especially deep cut may remove so much material from the key that the cuts on either side can't be very shallow. All pin tumbler key cuts are V-shaped, so the pin has to ride up a slope that can be only so steep before the key can't be inserted—or worse, removed.

If you're repinning a lock just for picking, MACS doesn't matter much. However, if you want a working key for that lock, confirm the MACS for that brand before repinning it. Not all lock manufacturers have MACS, so some brands of locks allow any bitting.

Reassembling Locks

To put a lock back together, you essentially follow the steps for disassembly in reverse. Luckily, most of the steps are easier than their disassembly equivalent. Make sure you have the same tools available as when taking the lock apart.

Step 1: Insert the Springs and Driver Pins

To insert the springs and driver pins back into the lock's bible, you need the housing, the springs, and the driver pins, as well as a plug follower and pinning tweezers. A good light source, like a desk lamp, will help you see into the housing.

Start with the pin stack closest to the rear of the lock, which corresponds with the tip of the key. (If you're leaving out pin stacks when building this lock, you'll want to skip as many chambers as pin stacks you're omitting, pushing the plug follower past those holes.)

NOTE

The front and rear sides of the housing on a KIK lock aren't interchangeable; if in doubt, make sure that the bore holes on the plug line up with the position of the chambers in the bible.

Insert the plug follower into the rear of the housing and slide it in just far enough to stop right before the chamber for the rearmost pin stack you're filling. Using your tweezers, place a spring into the chamber, as shown in Figure 5-21.

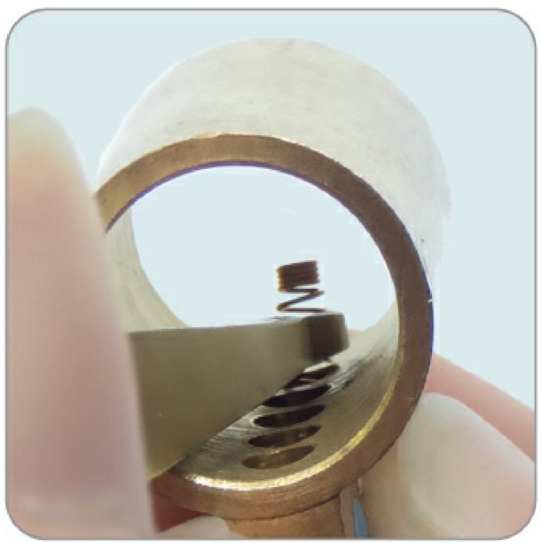


Figure 5-21: Inserting a spring into the bible

Pick up one end of the driver pin with the tweezers; don't grasp it in the middle. Put it into the chamber, depressing the spring, but don't release the tweezers or the pin will shoot out of the chamber. Instead, push the plug follower forward, putting pressure on the back side of the pin to wedge it in place. Once it's wedged, release the tweezers and use the tip to push on the top of the pin, allowing the plug follower to slide over the pin and trap it in the housing, as shown in Figure 5-22.

Figure 5-22: Installing a driver pin in the bible

Take a breath! This step is the hardest part of the reassembly. It's okay if you don't get it the first time; we've all had to chase down an escaped pin at some point. Once the first driver pin is in place, repeat the process for the remaining drivers until you've filled the frontmost chamber.

Step 2: Populate the Plug

Grab the plug, key pins, and your tweezers. In each chamber you plan to use, place one key pin (see Figure 5-23). Unlike most driver pins, key pins have a top and bottom, so be sure to put the pointed or rounded side down into the plug—that's what helps the pin ride along the key's bitting. The flat side of the key pin should be at the top so that the plug is smooth when the proper key is inserted.

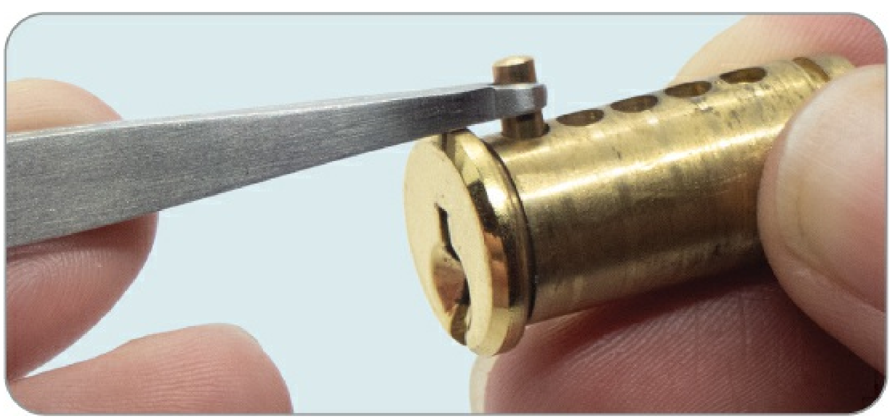


Figure 5-23: Placing a key pin back in a plug

If you aren't using every pin stack, make sure you're filling in the same chambers that you put drivers into in step 1. Having a driver pin with no corresponding key pin almost certainly renders the lock inoperable.

Step 3: Check the Key

If you have a key that you want to work in this lock, now's the time to check your work; if not, skip this step. Carefully insert the key into the plug, making sure not to spill any of the pins. The pins will move up and down, but they shouldn't fall out if you hold the plug with the pin holes up and slowly insert the key. To ensure that the pins stay in place, you can place a finger gently over the top of them as you insert the key.

If you've properly matched the key pins to the key, the top of each pin should be flush with the plug's surface when the key is fully inserted (see Figure 5-24). Any pin sticking up above the top of the plug is too long for that chamber. Any pin sitting below the surface is too short, and you need to move up a size. Once all the pins look right, continue to step 4.

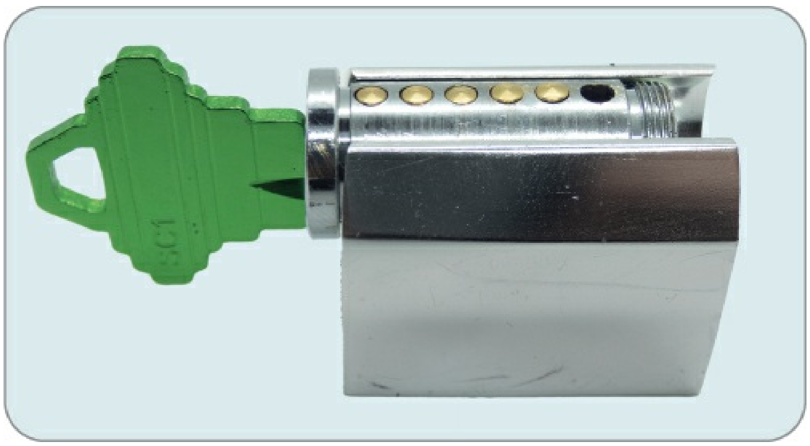


Figure 5-24: Key pins in a plug with a matching key. The cuts on this key aren't perfect—the middle pin is sitting a bit low and the pins near the tip of the key are a little high—but they're within the lock's tolerance, so the lock and key will work.

Step 4: Insert the Plug

Just as you used the plug follower to push out the plug during disassembly, now you'll use the plug to push out the plug follower. Carefully turn the lock housing on its side so the pins in the bible are rotated 90° from the key pins in the plug. If your plug follower has a notch at the end, make sure it's rotated so the gap isn't in the same spot as the bible; otherwise, a driver pin could escape.

Slowly use the rear end of the plug to push the plug follower out of the lock until the front of the plug is resting on the front of the housing. Don't allow any space between the plug and the follower, or a driver pin might pop out. You might feel several clicks as the driver pins transition from riding on the follower to riding on the plug, but they shouldn't get stuck. If necessary, you can use a shim to smoothly guide in the plug. This is especially helpful for T-shaped driver pins or thinner 2.3 mm standard pins.

If you're using a double-sided Euro profile cylinder, replace the cam in the middle of the lock, between the two plugs. The cam has two pieces: the cam itself and the clutch that fits into the back of both plugs and interfaces with the cam. Slip the clutch into one of the plugs; then slide the cam into the cutout in the middle of the lock and rotate the cam until it aligns with the clutch and the two parts fit together, as shown in Figure 5-25. (Double-check that the cam isn't 180° out before locking it—see the next section.)

Figure 5-25: Reinserting a plug and cam into a Euro profile cylinder

Step 5: Lock the Lock

If the previous steps went well, you can lock the lock, making it easier to install the plug-retaining mechanism. Insert a turning tool (included with any lockpick set) or any small, flat piece of metal into the front of the plug and rotate it so that the key and driver pins align. You should feel a click as the plug locks into place.

For double-sided Euro profile cylinders, make sure the cam is rotated to the correct position—with the cam's bar down near the bible, off-center by just a couple of degrees—before locking both plugs. Otherwise, the cam can get locked in a position at the top of the lock, 180° from where it should be; this is known as a *slipped cam*. While not a big deal for a lock used for locksport, a slipped cam prevents the lock from being used in a door.

Step 6: Install the Plug-Retaining Mechanism

Now that the main parts of the lock are assembled, you can reinstall the plug-retaining mechanism in the housing. At this point, the plug is being held in by the driver pins, but if the lock were opened with a key or picking tool, the plug would slide right out. Mortise cylinders are the easiest: simply reattach the rear cam, using the screws that hold it in place.

For KIK or rim cylinders, you need to reinstall the cap. Make sure the spring and cap pin are in the back of the plug. Place the cap over the back of the plug, and with a picking tool or flathead screwdriver, reach into the cap's center hole and depress the cap pin. With the pin depressed, thread the cap onto the plug. Once the cap feels snug, release the cap pin and rotate the cap until the pin locks in place. It's possible to over- or under-tighten the cap: too tight, and the lock won't turn smoothly even with the proper key; too loose, and the plug will shift forward and backward within the housing. Press down the cap pin and adjust the cap as needed.

On Euro profile cylinders, you need to reinstall the C-clips (Figure 5-26). Make sure they're still flat and weren't bent out of shape during removal. If they were damaged, you can either reshape them with pliers or purchase replacements. Find the groove on the back of the lock where the clips attach and push them back onto the plug until they snap into place.

Figure 5-26: Reinstalling a C-clip using the SPARROWS Gut Wrench

Step 7: Test It Out

With all the parts reassembled, perform a few final checks. If you have a key, does it work? If the lock is double-sided, does the key work on both sides? If you put a picking tool in the lock, can you feel the pin stacks you installed moving properly and feeling springy? If so, excellent.

If the lock is feeling a bit stiff, check that the plug-retaining mechanism is installed properly. If everything seems correct but you're still getting resistance from some of the pins or when turning the plug, you might need to add a lubricant.

Applying Lubrication

Lubrication is an important part of lock maintenance. Locks have a lot of parts that should move freely without binding up. Since locks are often exposed to the elements and to dirt and grime introduced by keys, they need a bit of lubrication every now and then.

Add lubricant anytime a lock is hard to operate with a key, a pin stack is hard to lift or feels gritty during picking, or the shackle is stuck even after you've picked the lock. Lubricating any used locks when you first add them to your collection is also a good idea, especially if they've been used outside.

A lot of debate occurs about the best kind of lubricant for locks. Keep the following in mind when choosing one:

- Try to use lubricants that are advertised for use in locks.
- Lubricants can be wet or dry. Both work but shouldn't be mixed. Once you've chosen one for a lock, don't switch back and forth (unless you completely disassemble the lock and soak it in a solvent to remove existing lubricant).
- Petroleum-based, water-displacement-type lubricants, such as WD-40, are never a good option for locks. They can attract and trap dirt and can leave a gummy residue, necessitating repeated applications that further hinder the lock's function.
- Organic/cooking lubricants like coconut oil or cooking spray degrade quickly and should never be used on locks.
- Graphite isn't an ideal lubricant, as it's messy. Use it only if recommended (and previously applied) by the lock manufacturer, such as for BiLocks.
- Never mix graphite and oil-based lubricants; they form a solid that will jam a lock.

For wet lubricants, we recommend Houdini Lock Lube, GT85, and Tri-Flow Superior Lubricant. For dry lubricants, a great option is PTFE powder, the compound used to make Teflon coatings. It has great lubricating properties and doesn't gum up locks. It is also a principal ingredient in Tri-Flow and GT85.

You can lubricate most locks by holding them bible side down, spraying or squeezing the lubricant into the keyway, and inserting a key or rake-style picking tool several times to work the solution into the lock's mechanism. For particularly stiff locks, some disassembly may be needed to thoroughly clean and lubricate hard-to-reach places.

For safe locks, a small amount of grease-like lubricant is often preferred to keep all the moving parts happy. S&G uses and recommends a very thin coating of Shell AeroShell Grease 22 on the internal parts and bolt of its mechanical safe locks. If you're using a different grease, make sure it's compatible with all the materials used in the lock (often a mix of brass, zinc, steel, and even a few plastics). If the grease is obvious after you apply it, you've probably used too much.

Summary

In this chapter, we discussed the basics of lock maintenance that every locksporter should know: disassembling, repinning, reassembling, and properly lubricating locks. Next we turn to Part II. To introduce you to lockpicking, we'll discuss *why* locks can be picked, as well as the fundamentals of the lockpicking process.

PART II

PIN TUMBLER LOCKPICKING

To learn how to pick locks, first you need to understand how locks work and what makes it possible to pick them. We covered how locks work in Part I, so now we'll address the second piece: the vulnerabilities in lock mechanisms that allow them to be picked. What exactly makes lockpicking possible?

As you've seen, pin tumbler lockpicking involves aligning each pin stack with the shear line so the plug can rotate and the lock will open. But how can you tell when the pin stack is aligned at the shear line, and how do you keep it there as you move on to the other pin stacks? We'll answer these questions in this introduction to Part II so you can apply that knowledge in Chapters 6 through 8.

The Element Binding Order Principle

Every lock has tiny, unintentional manufacturing imperfections. For example, consider the following image, which shows how pins are cut from their original state, known as the *wire*.

The wire might vary slightly in thickness from top to bottom, or the holes drilled in the lock's housing and plug might not be exactly straight. Regardless of the exact manufacturing defect, one pin is always a bit thicker or is situated a bit off-center, so that it makes contact with the housing first and keeps the plug from turning. That pin is referred to as the *binding*, or *blocking*, *pin*. Lockpicking requires finding out which pin is currently binding and *setting* it, or aligning it with the shear line. Setting that first pin causes a second pin to bind, setting the second causes a third pin to bind, and so on until you've set all the pins and opened the lock. This is known as the *element binding order principle*, and it's what makes lockpicking possible.

NOTE

The element binding order principle holds true for almost any mechanical lock, including dimple *locks and lever locks. The elements might be pins, sliders, levers, or discs. It might seem impossible that these imperfections exist in every lock, but it's true. Tolerances vary greatly among manufacturers, but even in the most expensive locks, subtle differences exist in pin thickness and position that will cause one of the pins to bind when you apply tension.*

The order in which the pins must be set depends on the locations of the imperfections. Since the defects weren't manufactured in, they'll be different in every lock, and you won't know this order beforehand. Unless you set the pins in that specific order, the lock won't open. You need to learn to feel which pin is the first to bind.

Feeling for a Binding Pin

To experience what a binding pin feels like, gather a lock, a tension tool (shown at the top of this photo), and a picking tool (bottom of photo).

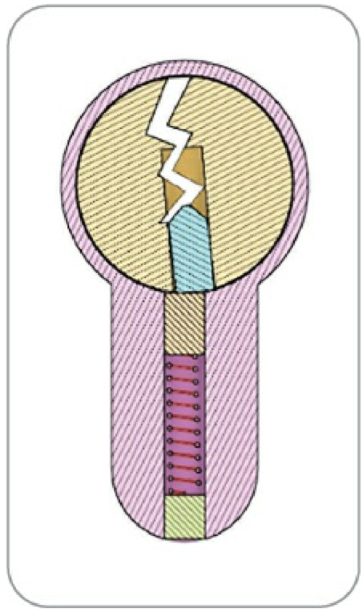
We'll explain in detail how to use these tools in Chapter 6, but for now, simply insert the tension tool in the keyway and apply a small amount of tension on the cylinder, trying to gently rotate the plug. Because of the element binding order principle, one pin stack will start to bind, but you don't know which one yet.

Use your picking tool to push on the first pin stack and feel the spring tension. Do you feel the stack push back with the force of the spring? Or do you need to push harder to move the pin? If you answered yes to the second question, this additional friction is the pin scraping against the housing, indicating that you're moving the binding pin. If you feel only spring tension, move to the next pin stack until you reach the one that has more friction.

Keeping the Set Pin in Place

When actually picking a lock, once you find the first binding pin and push it until it's aligned with the shear line, you must keep tension on the plug to hold the set pin in place against the housing. If you release that tension, the spring will make the pin pop back to its default position, and the lock will reset.

The following illustration shows a pin stack set in the correct position; you can see that the driver pin is no longer able to pop back into the plug. The plug isn't rotating to open yet, since more pin stacks are still binding, but as long as you maintain tension on the plug, the pin will stay in place at the shear line.



For demonstration purposes, this illustration intentionally exaggerates the amount of plug rotation you'll get when picking. In reality, the rotation is so minute that you probably won't see it, but you'll feel a kind of click in your tools when the pin pops into place.

Chapter 7 goes into far more detail on the lockpicking process and the feedback you'll feel when you've properly set a pin. Then, to wrap up Part II of the book, we'll walk you through preparing for a lockpicking competition in Chapter 8. First, though, it's time to familiarize yourself with the various lockpicking tools and how to use them.

6
PIN TUMBLER LOCKPICKING TOOLS

In this chapter, you'll learn about basic lockpicking tools as well as more specialized tools for nonstandard locks. We'll also briefly discuss pick guns. You'll need at least one pin tumbler lock to practice on; any lock will do, as long as it's not actually in use (in case of damage). You'll also want a basic lockpicking set that includes a few tension wrenches, hooks, and rakes. Most beginner sets include these tools.

Tension Wrenches

A *tension wrench* is typically a strip of metal with one end bent at a 90° angle. You insert the bent end into the plug and, with your finger on the long end, apply a little bit of force to rotate the plug slightly in order to keep the set pins in place while you tackle the other pins. Once all the pins are in place, you use the tension wrench to fully open the lock.

Tension wrenches come in a variety of forms, sizes, and materials. Stainless steel is the most common material, but some are made of spring steel, which allows them to bend more easily. Spring steel wrenches can be useful for locks that require little tension to pick, but they may not be suitable for stiffer or heavier-duty locks.

Figure 6-1 shows two typical tension wrenches, both made of stainless steel.

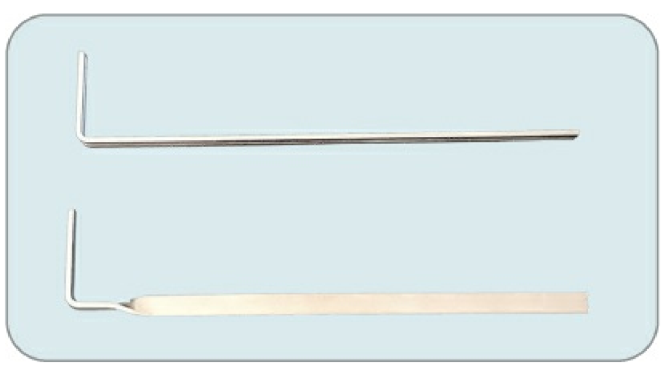


Figure 6-1: Basic tension wrenches

One factor to consider when choosing a wrench is the amount of feedback it gives. For example, the bottom wrench in Figure 6-1 has a twist, which allows the long end to bend a little when you apply pressure to it. This gives you good feedback on the amount of force you're using, making it useful for more delicate locks. The straight wrench is rigid, which gives less feedback but can be useful for stiff locks or those that require a lot of tension. Your choice of tension wrench will generally depend on what you feel comfortable with, so trying both types to see which works better for you is worthwhile.

Tension wrenches also come in different lengths, widths, and thicknesses to fit keyways of various shapes. For example, European locks often have a smaller keyway than those found in the US, so they require a thinner, smaller tension wrench. Figure 6-2 shows two tension wrenches of drastically different sizes.

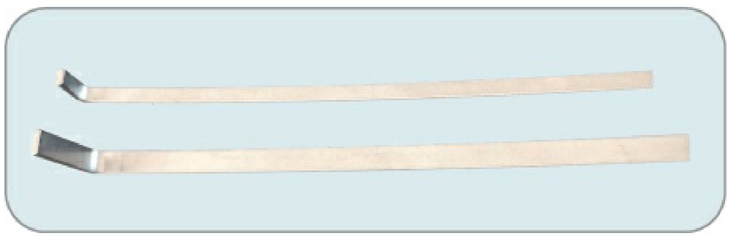


Figure 6-2: Tension wrenches of different sizes

Dimple locks usually require a thick, square tension wrench because the keyway is so wide. Figure 6-3 shows a wrench made specifically for dimple locks, next to a regular wrench.

Figure 6-3: A tension wrench for dimple locks (top)

A *flat tension wrench* is a flat piece of metal with an end that's curved rather than bent at a 90° angle from the handle. The thickness of a flat tension wrench determines its stiffness. Some plugs require more force than others to turn and might need a stiffer tension wrench.

The flat tension wrench in Figure 6-4 has a curve on both ends, effectively providing two tension wrenches in one. The ends are also serrated to give the wrench a better grip on the plug.

Figure 6-4: A flat, serrated tension wrench

While most tension wrenches are simple, more specialized versions are available, such as the ones shown in Figure 6-5. The one on the left is specifically designed for use in tubular locks, often found in vending machines. The wrench on the right is used on wafer locks, such as those found in cars; it grabs both ends of the keyway, leaving room in the middle for picking tools.

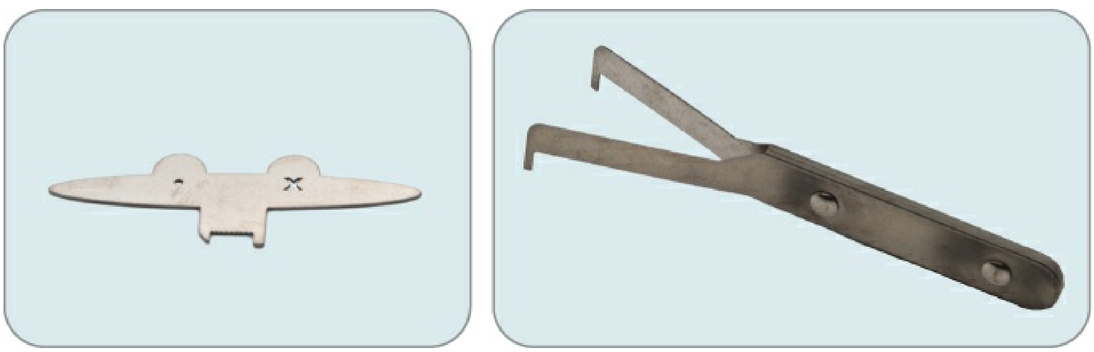


Figure 6-5: Tension wrenches for tubular locks (left) and wafer locks (right)

NOTE

At the time of writing, tubular and wafer locks are not included in any competitions, though they can be a fun personal challenge.

It pays to have a variety of tension wrenches with you in a competition. Changing wrenches is common when you move from one lock to another, even if the other tools you use remain the same.

DIY TENSION WRENCHES

You can create your own tension wrench from a piece of flat metal. Lockpickers have found that the long steel insert from car windshield-wiper blades works well; you might try asking nicely for discarded wiper blades at auto parts stores or car service centers. Cut the metal to the desired length and use two pairs of pliers to make a 90°

bend toward the end. Twist the long end if you prefer. If the metal is too stiff to bend, try heating it up with a torch to soften it. Once you're happy with the shape, use some fine-grit sandpaper to smooth the edges of the metal.

You can use other sources of scrap metal to make tension wrenches in various shapes and thicknesses. For example, broken street-sweeper bristles found on the side of the road are another favorite of lockpickers.

Raking Tools

Raking tools rapidly slide over pins in a back-and-forth motion to push them to the correct position; sometimes you can even set multiple pins in a single rake. Rakes broadly come in two types: *mountain rakes*, which have jagged peaks, and *snake rakes*, which have rounded waves. Figure 6-6 shows two mountain rakes on the left and four snake rakes on the right. The shapes are intended to resemble a key's bitting.

Figure 6-6: Rakes from various vendors

NOTE

For competition purposes, we recommend you focus on mastering single-pin picking instead of raking (see "Picking Tools" on page 92). Single-pin picking works in a repeatable way, whereas with raking, a certain amount of luck is always involved. That said, mastering raking means sometimes you'll be able to open locks very fast, which can be an advantage.

Like tension wrenches, rakes come in a variety of materials. The stiffness and thickness influence the cost as well as how you use the tool. Thinner rakes are more expensive and can be prone to bending, but they work well in locks with narrow or curved keyways. Thicker rakes are cheaper and sturdier but might break in half if you apply too much force. If your budget allows it, go for the thinner ones, as they fit in more locks.

A rake should have some kind of handle so the bare metal doesn't cut into your hand when you're using it. Figure 6-7 shows several kinds of handles.

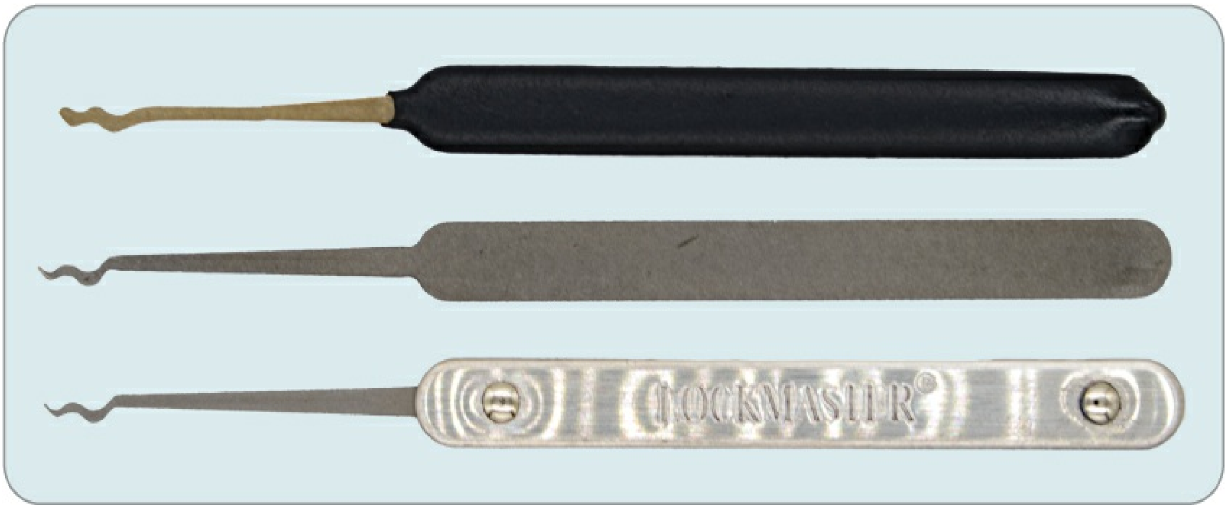


Figure 6-7: Rake handles

Cutting the rake teeth and handle from one piece of metal, as in the middle rake in Figure 6-7, was once common. However, this kind of rake is uncomfortable to use and pretty rare these days. To improve the comfort, you could wrap the handle in tape or rubber tubing, such as heat shrink tubing used in electronics, but just buying a rake with a proper handle is easier.

Finally, we'll briefly mention two tools you likely won't use often: the Bogotá pick and rake, invented by a lockpicker by the name of Raimundo. The original versions come with either a curled handle, as shown at the top of Figure 6-8, or a straight handle that doubles as a tension wrench, and are available in steel and titanium. The Bogotá pick has one peak, and the rake has three sharp peaks. Several manufacturers now also offer rakes in a similar style, such as the Multipick rake at the bottom of Figure 6-8, which has two peaks and is used by some lockpickers as a tool of last resort when a lock won't open and time is running out.

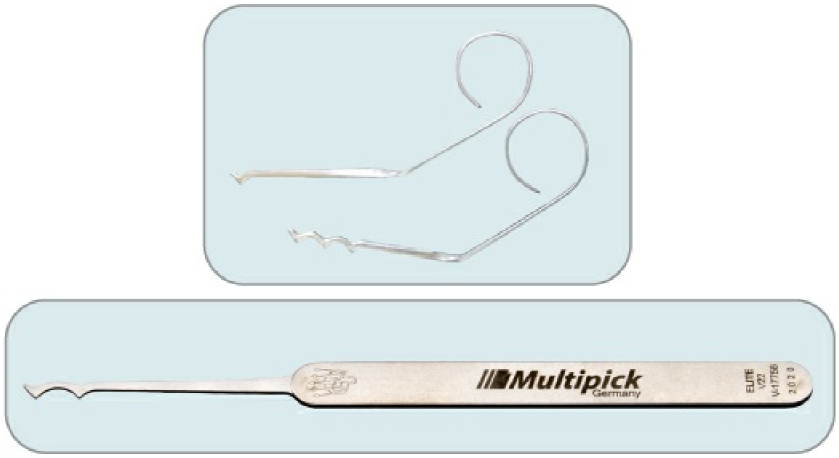


Figure 6-8: The original Bogotá pick and rake (top and center, respectively) and a Bogotá-style pick from Multipick (bottom)

Picking Tools

Single-pin picking, the technique of aligning a single pin at a time, is generally thought to exemplify the true art of lockpicking. For this, you use picking tools like those shown in Figure 6-9; most of these are *hooks*, a straight length of metal with a curve or bend at the end. You insert the tool inside the keyway and push each pin deep enough to align it with the shear line. When all the pins are set to the correct position, the lock opens. Picking tools vary in material, thickness, and size to match different kinds of locks.

Figure 6-9: Various shapes of single-pin picking tools

The thickness of the tool impacts its flexibility as well as its ability to pick locks with narrow keyways. Common thicknesses are 0.6 mm and 0.4 mm in Europe, and 0.025 inches and 0.018 inches in the US. Thinner picking tools are often called *European picks*, as narrow keyways are more common in Europe. Figure 6-10 shows a wide and narrow keyway, respectively.

Figure 6-10: Wide (left) and narrow (right) keyways

While the keys for these locks may be about the same thickness, the keyway on the right has multiple protrusions that a tool has to maneuver past to push down the pins. In this case, a thin picking tool would suit the narrow keyway, while the wide keyway could be opened with any type.

Picking tools also come in various sizes to accommodate pins at different depths. The hook size you choose depends on a few factors. For a given range of locks, you have only a few possibilities for pin lengths that correspond to the cuts in the key. The longest possible pin matches the deepest cut in the key.

A long key pin needs to be moved only a tiny bit, so a small hook will do. A short key pin, on the other hand, needs to be moved much farther for the corresponding driver pin to clear the shear line, and might require a larger hook to reach deeper into the pin stack. Larger hooks can also push pins behind other pins, whereas a pick with just a slight bend might not. However, large hooks also take up a lot of space in the keyway, making it tricky to navigate through narrow keyways or reach around longer pins.

The largest hook available is sometimes called a *gonzo hook*, a reference to the beak of the Muppet Gonzo the Great (Figure 6-11).

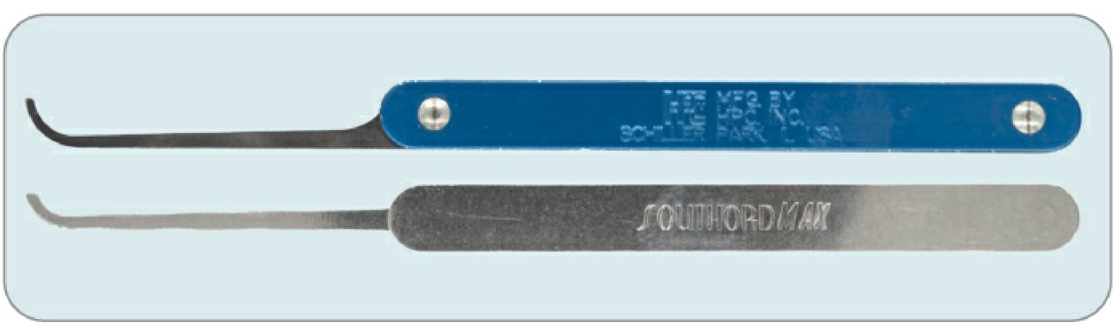


Figure 6-11: A gonzo hook (top) next to a regular hook (bottom)

Gonzo hooks are so large that they come in handy on rare occasions when a pin that needs to be pushed deep is right behind a pin that does not; Figure 6-12 shows one in action.

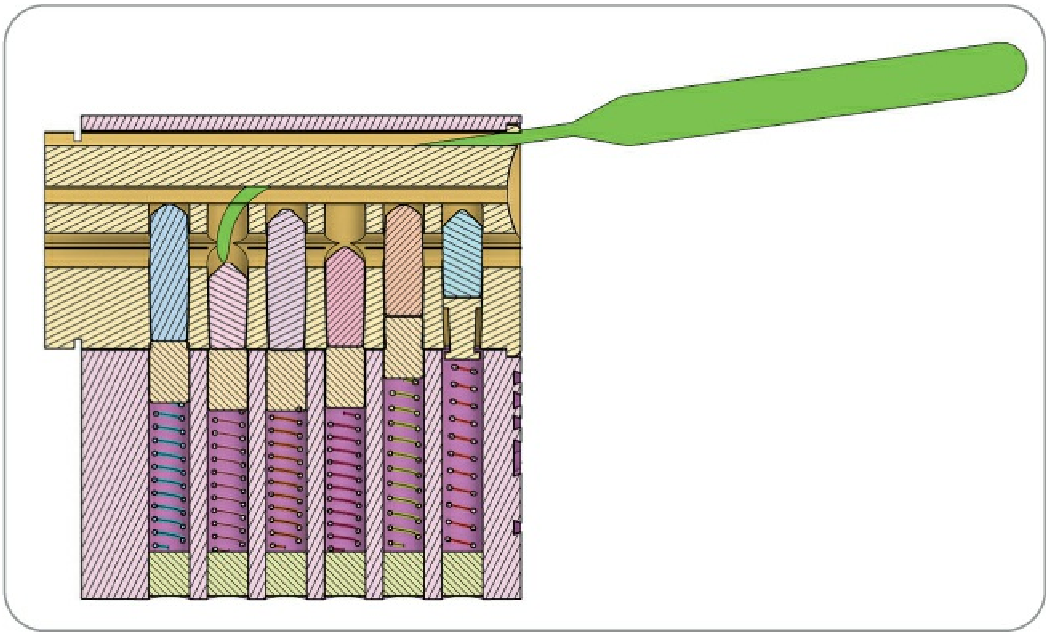


Figure 6-12: A gonzo hook being used to move a short key pin

Some picking tools are curved the whole length of the pick, like the rightmost two picks in Figure 6-9. This idea was made popular by Falle-Safe. Because of the shape, these tools don't fit well in narrow keyways. They are expensive and not used much.

Half-diamond picks (the third, fourth, and fifth picks from the right in Figure 6-9) can act as both a rake and hook because of their unique shape. You can use the half-diamond to rake when removing it from the keyway, which is a useful technique you'll see in Chapter 7, but not when inserting it. Most lockpickers rarely use the half-diamond, however, as it's not as good as a rake for raking and not as good as a hook for picking. A half-diamond is included in most pick sets, so you can try it and see if it works for you, but don't bother buying one separately.

> I always bring a mix of picks to competitions. For example, the HPC 2000 series is thin and a bit flexible, whereas the SouthOrd MAX with ABS handle is very sturdy. I also own picks made by Storm, SPARROWS, Multipick, Peterson, Lockmasters, and others; for beginning or intermediate lockpickers, any tool by these major brands will usually do the job.
>
> —WALTER

Dimple Picks

Dimple picks are specifically designed for dimple locks and are used in almost the same way as regular picking tools: you insert them and push on the pins while gently rotating the tension wrench. The only difference is the motion you use: you rotate the dimple pick to push on the pin, whereas you push a regular picking tool down or up on the pin. Figure 6-13 shows various dimple picks.

Figure 6-13: A variety of dimple picks

As you saw in Chapter 3, dimple locks are similar to regular pin tumbler locks but with the keyway rotated 90° to accommodate the "dimples" on the flat side of the dimple key. The keyways of these locks tend to be wide, so we recommend using a wide tension wrench.

While the handle shape for a dimple pick is mostly a personal preference, the shape and thickness of the tip affect the way you use the tool. The tip is normally a small square that can be flat or curved, and the size you choose depends on the size and spacing of the pins. A larger tip is suited for larger pins spaced farther apart, whereas a smaller tip is better for smaller pins spaced closer together. Some cheap dimple picks have a very thick or even square shaft, which makes them hard to maneuver, but you can file off a bit of material to make them thinner.

Dimple locks have some pins that need to be set deeper than others, so the tip on a dimple pick can range from flat (for pins that need to be pushed only a little bit) to curved (for those that need to go deeper). For this reason, dimple pick sets typically contain flat picks and at least one curved pick in left and right variants. Figure 6-14 shows three dimple picks, varying in curvature only.

NOTE

Dimple picks come in left and right variants (see the top of Figure 6-13) because a dimple lock's *pins are positioned at either the far left or the far right of the keyway, leaving room for the pick on the opposite side. Flat dimple picks don't differentiate between left and right since the tool can simply be flipped over, but dimple picks with a curved tip differ; see Figure 6-14 for a close-up look.*

Figure 6-14: Different dimple pick tip shapes

Dimple rakes, shown in Figure 6-15, are created from a ribbed piece of sheet metal and work the same way as standard rakes. Most dimple pick sets don't include them because they don't work well; generally, only cheap dimple locks will open with them. Using a regular snake or mountain rake, held horizontally, is more effective.

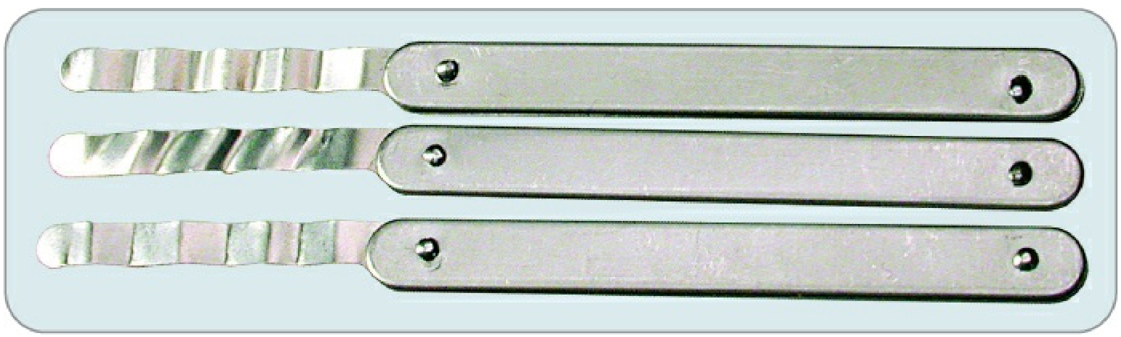


Figure 6-15: Dimple rakes

One type of dimple pick is designed specifically for use on Mul-T-Lock dimple locks, which have the pin-in-pin system discussed in Chapter 4. To pick these locks, you first set the hollow outer pins, then the solid inner pins. Figure 6-16 shows a pick set that includes a dimple pick that can push down the outer pin without touching the inner pin. In most cases, you can pick pin-in-pin locks with regular dimple picks just as well.

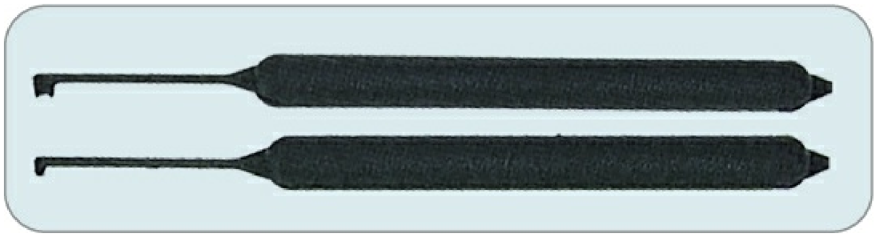


Figure 6-16: Dimple picks for a pin-in-pin Mul-T-Lock; the top pick is for the outer pins, and the bottom is for the inner pins

Regular hooks and rakes can also be used to pick a dimple lock. However, they can be tricky because the keyway is perpendicular to the pins, leaving little space above the pins for the hook to fit, as shown on the left in Figure 6-17. If you rotate the hook 90°, you usually have enough room to insert the pick all the way to the back. You can then push the pins by rotating the pick, rather than pushing on it, as shown on the right in Figure 6-17.

Figure 6-17: Using a hook to pick a dimple lock

Buying an additional cheap set of dimple picks gives you the option of filing the picks into shapes that better suit you. If you're adventurous, stick with your standard lockpicking gear and use those for dimple locks as well.

Pick Guns

Pick guns (also known as *snap guns*) are considered more of a party trick than a useful tool in locksport (although for locksmiths, they can be handy). A pick gun lifts or depresses a needle in the keyway to strike all the pins in a lock simultaneously, forcing the key and driver pins apart and allowing you to turn the lock before they come back together. We'll explain this process in more detail in Chapter 7. Pick guns come in both manual and electric versions.

The manual pick gun shown in Figure 6-18 is designed for US locks, where the pins are above the keyway. To use it on locks in European orientation, you hold it upside down.

Figure 6-18: A manual pick gun that fires only upward

The needle is replaceable, and both styles of pick gun have a screw to adjust the force with which the needle strikes. The manual pick gun has a copper wheel marked *L* for low and *H* for high pressure, while the electric pick gun (Figure 6-19) has a screw at the tip to adjust the force.

Figure 6-19: An electric pick gun

The manual pick gun strikes only once or twice at a time. The electric pick gun is faster, continually striking as long as you hold down the button, but is much louder and more expensive.

Most competitions don't allow pick guns. The exception is the SSDeV freestyle championship, where participants are required to bring their own locks for others to open and therefore often bring locks that are harder to open with a pick gun.

> Pick guns aren't always faster or more effective than picking. I once competed in the freestyle competition and forgot to bring my pick gun, but using standard tools I was able to open locks faster than others who used a pick gun.
>
> —WALTER

Comb Picks

Some locks have a defect whereby they open when all the pin stacks (both key and driver pins) are pushed out of the plug and into the bible. Lockpickers can take advantage of this by using an *overlift attack*. The East German secret police used this trick to get quick access to houses with state-supplied locks that purposely had this defect. Some cheaper padlocks today still have it.

To pick such a lock, you use a *comb pick*, so named because it looks like a small hair comb (Figure 6-20).

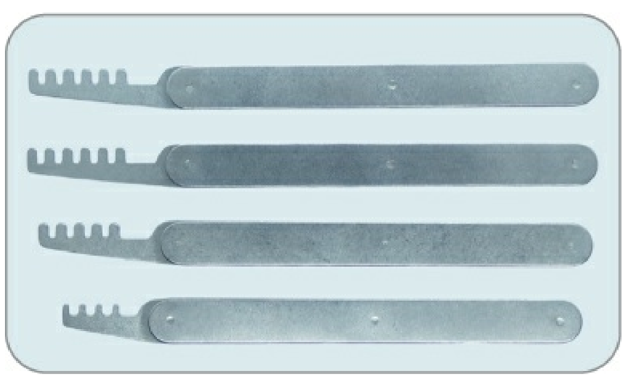


Figure 6-20: A set of comb picks

To use a comb pick, you simply insert the comb fully into the keyway and then lift the entire pick straight up. The teeth on the comb align with the pin stacks, pushing them into the bible. You can then turn the pick just like a key to open the lock. Because the number of pin stacks, the spacing between them, and the height of the plug vary among lock brands, comb picks are often sold in sets to accommodate these differences.

Combing is usually not used in lockpicking competitions, as it is considered a bypass rather than actual picking.

PICKING LOCKS WITH PAPER CLIPS

Chances are you've seen movies in which people manage to pick locks with all sorts of tools but no tension wrench. That won't work. You need the tension wrench to maintain pressure on the keyway, both to keep the pins from sliding back into place and to turn the lock open. Not using a tension wrench is like inserting a key and not turning it. However, people *have* successfully used a bent paper clip as a tension wrench.

A tension wrench needs to perform only one task: getting the plug to turn. If you can bend a paper clip so it fits the keyway and can apply enough pressure to turn the plug, you've made yourself a functional tension wrench. For a paper clip to work, the keyway needs to be rather wide, so this works better with locks sold in the US, padlocks, and dimple locks, which often have a wide keyway.

You'll still need a pick to manipulate the individual pins. If the keyway has enough room, you could do this with a second paper clip.

Tool-Buying Advice

The tools you need to get started depend on your budget and how regularly you plan to be lockpicking. You'll want your set to have a few hooks, rakes, and tension wrenches. The hooks should come in a few sizes, from small to large. You'll want a snake rake, one or two mountain rakes, and possibly a Bogotá rake. In terms of thicknesses, in Europe, it's best to have a set made from thin metal, whereas the thickness is less of a concern in the US.

Buying a ready-made lockpicking set is often the best way to start, as this will give you a collection of hooks and rakes as well as a carrying case. Once you become more comfortable and learn what works best for you, you'll begin adding individual tools that vary in stiffness, shape, and handle. Pick sets typically don't include a large enough variety of wrenches, so even if you buy a packaged set, getting extra tension wrenches in multiple shapes and sizes is worthwhile. Talk with other lockpickers about their experiences with specific tools as well.

After you've purchased the general tools, consider buying a pick set for dimple locks. Multiple manufacturers offer various sets, and the cheapest sets are often too crude for locks with a narrow keyway. We recommend buying a set from a renowned manufacturer, such as Multipick. The cheap dimple pick sets can still be useful if you want to create your own tools. You can file them into the shape you like best, and if they don't work, they haven't cost you much.

Make sure you have spares for these picking tools if you plan to enter competitions. Tools can break—and they tend to do so when you need them most.

NOTE

Most contests allow the use of only simple lockpicking tools, such as tension wrenches and various picking and raking tools. Only the SSDeV freestyle competition allows you to use any tools you like.

We also recommend purchasing a manual pick gun if you're planning to enter a freestyle competition; an electric pick gun is more costly and not as versatile. Finally, consider purchasing a vise if you're comfortable picking locks held in one.

Summary

In this chapter, you've learned about the various lockpicking tools available and the kinds of locks they can be used for, and you've gotten some recommendations for assembling your own lockpicking tool collection. In the next chapter, you'll see these tools in action as we walk through the lockpicking process step-by-step. Let's start opening some locks!

7
PIN TUMBLER LOCKPICKING STEP-BY-STEP

In this chapter, you'll start picking pin tumbler locks. You'll explore various ways to hold tools and locks, learn what tool to use when, and practice some techniques.

You'll need a lock to practice with; any pin tumbler lock will suffice, as long as it's not in use and you can afford to damage it. We recommend using a regular lock rather than a clear acrylic practice lock. Although clear locks allow you to see what's going on inside them, they're made differently than regular locks and don't feel the same when you're picking them, so they aren't great for real-world practice. You'll also need a set of hooks and rakes to align the pins in the lock and free the plug, as well as a set of tension wrenches to rotate the plug and move the cam.

You'll be trying out several techniques, and we'll go through each in the order in which a beginner is most likely to master them: tensioning, raking, single-pin picking, and using pick guns.

Later in the chapter, we'll look at rarer and more secure locks, some of which have dedicated tools. For now, don't worry about getting your hands on these special tools. Most locks can be picked with hooks and rakes, given enough practice and patience.

Tensioning

Tensioning a lock by using a tension wrench, as Chapter 6 explained, holds the picked pins in place and rotates the plug to open the lock when you've set all the pins, and it's a skill in and of itself. Before you practice tensioning, you must decide how you'll hold your lock: you can either place it in a vise or hold it in your hand. This decision affects the way you use your tension wrench, which in turn can affect your comfort level and stamina.

When using a vise, you insert the lock with the keyway facing you. If you have the key, test whether the lock can still turn when it's held in the vise. Tightening the vise too much can keep the plug from rotating, as can clamping a part of the lock that needs to rotate, such as the cam or tailpiece.

If you find that using a vise works best for you, be sure to practice picking locks without it for those situations when a vice isn't available. For more about vises, see "Using a Vise" on page 106.

Using the Tension Wrench

Next, you'll practice techniques for using the tension wrench. These instructions are demonstrated on a European cylinder lock but apply to any lock type. If you've opted to hold your lock instead of using a vise, you'll need to use the same hand to hold both the lock and your tension wrench so you can use your other hand to hold your picking tools (see Figure 7-1).

We'll assume that you're holding the picking tool in your right hand; if you're left-handed, just mirror our descriptions. You should begin tensioning the cylinder before starting to pick.

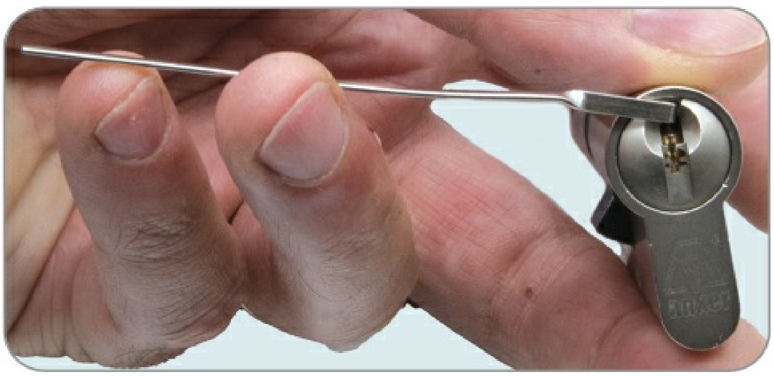


Figure 7-1: Holding a cylinder and tension wrench in one hand

Grab your lock and follow these instructions:

1. Insert the tension wrench in the keyway at the edge of the plug so the wrench is farthest away from the pins. This gives you good leverage and space for your picking tool. It's also the position that enables you to best feel the feedback from your minute variations in tension. Make sure the tension wrench isn't scraping against the housing when the plug rotates, or the additional friction will make it harder to feel what's going on in the lock. It's best to position the tension wrench such that it doesn't touch the housing.
2. Using your pinky and ring fingers, put a small amount of pressure on the end of the tension wrench handle in the clockwise direction. While some locks allow you to push counterclockwise, we recommend becoming comfortable using clockwise pressure, as padlocks usually open clockwise.
3. As you're picking, vary the amount of pressure just slightly to find the level that enables you to feel the most feedback in the tension wrench.

NOTE

When describing the keyway, we'll use the terms center *and* edge *rather than* top *and* bottom, *respectively, to prevent confusion for locks with horizontal keyways. Using the tension wrench at the edge is referred to as* bottom-of-the-keyway (BOK) *tensioning, and using it at the center is known as* top-of-the-keyway (TOK) *tensioning. In the images in this chapter, the locks are in the European orientation, so using BOK tensioning, the tension wrench is actually at the top of the lock.*

The angle at which the handle of the tension wrench comes out of the lock depends on the shape of the keyway and of the tension wrench, and can affect your comfort level.

Figure 7-2 shows an alternate technique that uses the thumb to apply pressure. When holding the lock like this, you use basically the same procedure: insert the tension wrench at the edge and apply a little tension to the end of the handle with, in this case, your thumb. The thumb is typically less sensitive than the fingertips, so this approach might provide less tangible feedback, but it's worth trying out the position to see what works best for you.

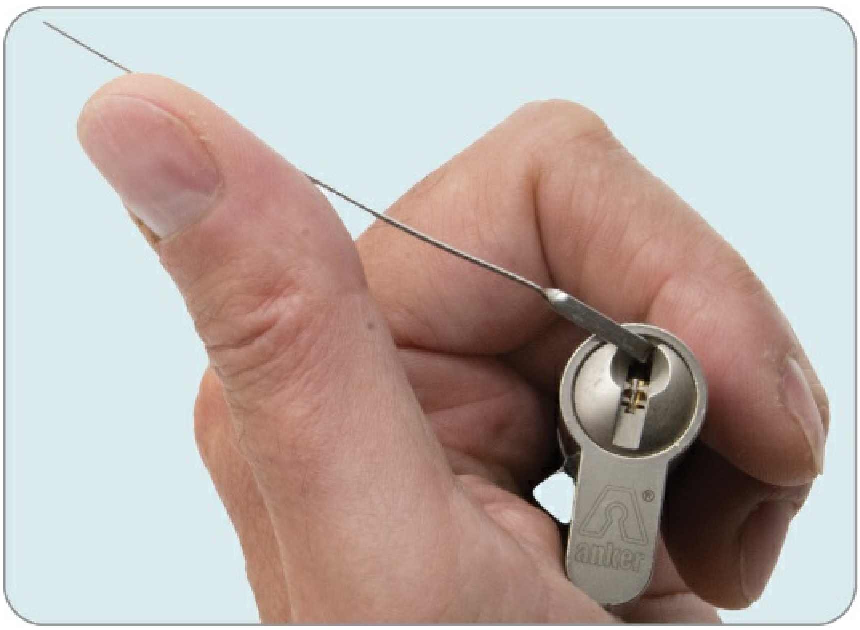


Figure 7-2: Another way of holding a cylinder and tension wrench

Now you'll try tensioning at the center instead of the edge. Insert the tension wrench in the keyway at the center and use your index finger to apply pressure, as shown in Figure 7-3. This method allows you to apply tension to either the center or the edge of the plug.

Figure 7-3: Tensioning at the center of the plug

The locksport world continues to debate whether it's best to tension at the center or the edge of the plug. Applying tension at the center has advantages and disadvantages. An advantage is that it leaves more space to insert a picking tool. A disadvantage is that your picking tool can, when you pull it backward, take the tension wrench out with it, resetting the lock. When tensioning at the center, make sure not to touch the first pin with the tension wrench; if you do, the added friction on that pin will require extra force to push it into place, making it harder to feel which pin to pick next.

Whether at the edge or center, push on the part of the tension wrench that's as far away from the cylinder as possible. The minute forces of tension are amplified the farther you get from the cylinder, giving you more accurate feedback. (In physics, this is known as increasing the *moment arm*.)

NOTE

*Some cylinders, such as the KIK cylinder, are hard to hold comfortably because of their size and shape. If you want to pick KIK cylinders but prefer holding a cylinder in your hand over using a vise, you can find 3D-printed holders on Thingiverse (*https://www.thingiverse.com*). The KIK cylinder fits tightly in the holder, which you can then hold comfortably in your hand. The holder also makes it easier to hold the KIK cylinder in a vise.*

Applying the correct amount of tension to your wrench is a tricky but crucial skill. Not every lock requires the same amount of tension, and the tension you need to apply will vary through the picking process. The best advice for beginners is to *use less tension than you expect to need*. Start by using the smallest amount of tension required; you can always apply a bit more later if needed. Applying a lot of tension can strain your hands and bend your tools, and puts too much friction on the pins, making the lock harder to pick.

More force is necessary in a few distinct situations, such as when a cylinder is mounted in a door and the wrench also needs to move mechanical parts outside the cylinder. This also occurs in some padlocks that have a spring to rotate the core back to its locked position; these locks usually need more force to overcome that spring pressure and get the core to rotate or even get the pin to set. The ABUS Diskus lock, shown in Figure 7-4, requires much more force to open than most locks (even when using a key) because the plug needs to move a large shackle. Finally, you'll likely need more force if the lock is filled with dirt, grease, or rust, or has had a rough life in general. Such locks are typically not used in competitions, luckily.

Figure 7-4: ABUS Diskus lock

In most cases, however, a light touch is all that's required. You can practice applying the least amount of tension necessary by listening to the pins drop back into place. Try picking or raking a lock and then releasing all the tension with the lock held next to your ear. If you don't hear any pops or clicks, you were using too little tension, and no pins were set (though it's hard to apply too little tension). If, on the other hand, you do hear clicks, you've applied enough tension, and you might be able to use even less. Reduce the tension, try to pick the lock again, and release the tension. If you still hear clicks the second time, the new (lower) amount of tension is still enough.

Repeat this process until you hear no clicks, at which point you've crossed the lowest limit of tension needed. This useful exercise not only exemplifies how little tension is needed but also helps preserve your tools and hand strength.

Tensioning the Cam

With some Euro profile cylinders, you can apply tension by simply pushing on the cam with your fingers, without using any tools. Most padlocks and US cylinders don't have a cam, although they might have a tailpiece that you can apply this technique to instead. Picking a lock by pressing the cam is more difficult than using a tension wrench, as the cam is close to the cylinder and so provides less feedback. Still, tensioning the cam can be helpful in certain situations, such as when you have a narrow keyway that obstructs using a tension wrench.

Euro profile cylinders come in varying lengths and usually consist of two identical locks in a single block, back to back. Figure 7-5 shows two cylinders: a regular two-sided cylinder (left) and a half cylinder (right), which has only one side. In both locks, the large cam sticks out.

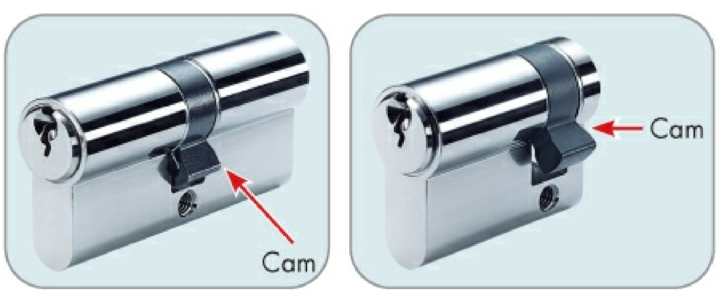


Figure 7-5: Euro profile cylinders

To try this technique, hold a Euro profile cylinder in your hand and use a finger on the same hand to push on the cam, as shown in Figure 7-6.

Figure 7-6: Tensioning the cam on a Euro profile cylinder

For some Euro profile cylinders, the cam is connected to only one of the two plugs; for others, it's connected to both. Between the two plugs is a mechanism that makes sure that the plug in which the key is inserted operates the cam. This central mechanism is activated when it's touched by the tip of a fully inserted key. Pushing the cam, therefore, will work only if you're picking the side that's connected to it via the central mechanism. To tell which side is connected to the cam, wiggle the cam and see which plug wiggles with it.

We don't recommend tensioning on the cam for beginners. Because the moment arm is short, feeling the feedback and pressure level is much harder than when using a tension wrench.

If you master this technique and want to use it in a competition, make sure that the cam is working and connected to the side you're picking and that cam tensioning is allowed. Tensioning the cam is sometimes seen as cheating, because you can't do it if the lock is mounted in a door. Picking locks in doors is for professional locksmiths, however, not people practicing locksport.

Using a Vise

As mentioned earlier in the chapter, a vise can hold the lock you're picking, freeing up your hands and giving you more space to hold the tension wrench and picking tools. A vise can be especially helpful when you're using a pick gun. Since the lock can't move in the vise, you'll feel every movement from the core in the tension wrench, providing better feedback.

Using a vise has downsides, however. For one, it's heavy, bulky, and difficult to transport. Not all vises fit all tables, so securing your vise to a competition table can be tricky. And once you have secured the vise, changing the position of the lock can be laborious.

You'll need a vise for impressioning (Chapter 9), so if you intend to try other areas of lockpicking, getting a vise and trying it out for regular picking might be worthwhile.

You can usually mount a vise on a table by using a clamp or a suction cup, though suction cups can be unreliable. For lockpicking, the vise needs to clamp the lock tight to restrict its movement. Make sure the lock's cam can freely rotate, or the lock won't open even after you've picked it. Figure 7-7 shows a lock in a vise; notice that the cam isn't clamped and has enough room to turn.

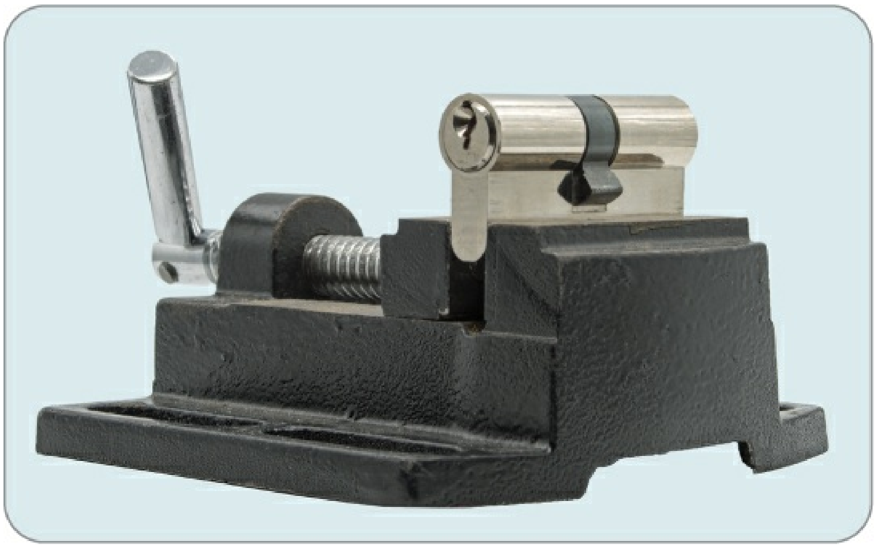


Figure 7-7: A lock clamped in a vise

A generic vise like the PanaVise 350 is a popular choice for most pickers. It can be used on any table, and the large base provides sturdiness. Another popular choice is the Bernstein Spannfix, which uses a clamp and can move around to allow optimal positioning for picking.

> I've also used a cheap machine vise I took from a column drill, as it's small and portable, though it doesn't have the movable part to position the lock. If you want a light and cheap vise, the Lishi Training Vise/Lock Holder is an option.
>
> —WALTER

Raking

Raking, as Chapter 6 explained, means rapidly moving a rake inside the lock in an in-and-out, up-and-down movement, in an attempt to knock all the pins to the shear line in one fell swoop (see Figure 7-8).

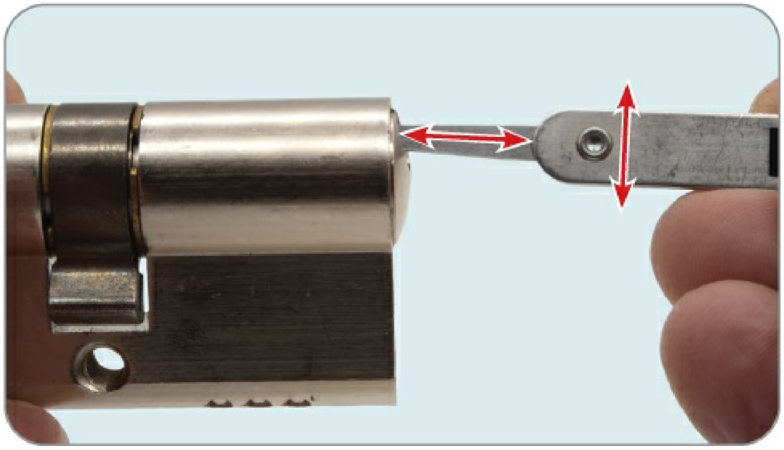


Figure 7-8: The raking movement

Considered a faster alternative to picking, raking involves quickly moving multiple pins into various positions and hoping they stay put at the shear line as you tension the plug. Because of the rake's shape, not all pins will be pushed to the same depth, which mimics a random key, so the closer the shape of your rake matches the bitting of the lock's key, the quicker and more easily the lock will open.

Since you can't know the key bitting beforehand, arriving at the correct rake to match the bitting requires a bit of luck. The best approach to raking is to change both the position of the rake and the amount of tension on the tension wrench throughout the process.

Not all locks can be raked. Generally speaking, the cheaper the lock, the easier it is to rake. With experience, you'll learn to recognize which lock brands and types can be raked open.

Using a Rake

Because several kinds of rakes exist, it's impossible to know ahead of time which will work best for a particular lock. This generally depends on the lock and the bitting of the lock's key, which, in a competition, you likely won't know. We'll give instructions here for the snake rake, mountain rake, and Bogotá.

Snake Rake

Steady your cylinder lock or padlock in either your vise or your hand. Hold the tension wrench in your preferred position. Then follow these steps:

1. Gently tension the plug with the tension wrench.
2. Insert the rake into the keyway, all the way to the end, without touching the pins.
3. Pull out the rake in one quick but gentle movement, making sure to touch all the pins. This movement should take only a quarter or half second.
4. Repeat steps 2 and 3 about 10 to 20 times or until the lock opens. During the process, vary both the amount of tension you're applying with the tension wrench and the

amount of force you're using to push the pins with the rake.

If the lock doesn't open, one or more pins may already be stuck at the shear line. You can check for this by listening to how many pins are released when you remove tension. Note that this is a tricky process; mastering it will come with practice.

Gently release the tension while keeping the lock to your ear, listening for clicks from pins popping back. If you hear as many clicks as there are pins, you know that all the pins were stuck. This happens when they're all at the shear line or when at least one pin is overset. Reduce the amount of force you're placing on the pins with the rake. Repeat from step 1 until the lock opens.

Once you've successfully raked open a lock, try opening it over and over again to learn which techniques work best and to improve your time. You have quite a few parameters to play with—tension, tools, applied force, speed, and so on—so this exercise will improve your raking skills.

OVERSETTING

You know that a pin stack needs to be aligned with the shear line for the lock to open. But what if you apply a bit too much force and push the pin stack *beyond* the shear line? In that case, known as *oversetting*, the key pin in the stack will keep the lock from opening, and you'll no longer be able to push the pin stack to align with the shear line. The only remedy is to release the tension, which causes all the pin stacks to pop back to their original places, and start over.

Mountain and Bogotá

For mountain and Bogotá rakes, only step 3 of the previous process is different. Move the mountain and Bogotá rakes back and forth continuously, touching the pins both going in and out. During this motion, vary the amount of pressure on the rake, as well as the angle at which you hold it, to alternate between pushing the front pins and pushing the back pins deeper.

Pushing the pins both going in and out is more efficient than pushing them in only one direction. Be careful to angle the rake so that its tip doesn't get stuck between pins. Although a snake rake can also be used like the mountain and Bogotá rakes, it's not designed for this and will make it harder to push into the lock while pushing on the pins.

Determining When to Rake

The major advantage of raking is that when it works, it can be quick. When you're just starting out, trying to rake a lock first can be useful, and, if that doesn't work, start single-pin picking.

Once you've become successful at single-pin picking, however, raking is generally considered a waste of time, especially in a competition environment where every second counts. If you spend 30 seconds raking and the lock doesn't open, that's 30 seconds wasted. Another disadvantage of raking is that it's difficult to know when you've pushed a pin too far and overset it, because you can't feel it as you can when single-pin picking.

Raking isn't really about finesse. It's a technique to open a lock quickly or not at all, and should be used in only certain cases:

- You're a beginning lockpicker who's not yet successful with single-pin picking.
- You have just a few seconds left to open a competition lock and know that's not enough time to set the pins individually.
- You have (virtually) unlimited time to open a lock and want to improve on an opening time you set using single-pin picking.
- You have reason to believe a lock can be raked open—for example, it's a cheap lock or you saw another competitor do it.
- You've been practicing single-pin picking for a long time without success and need to motivate yourself again.

NOTE

Dimple locks can also be raked, and a particular tool is used for the job. See "Raking Dimple Locks" on page 118 for more details.

Single-Pin Picking

Now it's time to do some single-pin picking. Single-pin picking is a more reliable means of opening locks than raking. As you've seen, many locks have security pins put there specifically to defeat raking and make single-pin picking harder. With single-pin picking, you can set security pins as well as standard pins, whereas generally raking works only on the latter.

Picking Standard Pins

Single-pin picking is a repeatable, methodical process focused on finding the one pin that's currently binding, as per the element binding order principle. To do this, you use a hook to push on all the pin stacks in the cylinder until you find the one that offers resistance, and then you push that pin just far enough to reach the shear line. You should feel in the hook and the tension wrench that the pin pops into place. You then find the next pin that's binding, push it into place, and repeat this process until the cylinder opens.

After you've picked a lock, you'll develop an image in your mind of what the pins look like inside the lock. You might learn that pin 3 needs to go very deep, and that security pins are at positions 1 and 2 and need to be set last. If you make a mistake and need to reset the lock, you can quickly get the lock back to its original state by releasing the tension.

To single-pin pick standard pins, get your pin tumbler lock or padlock, a tension wrench, and a hook, and follow these steps:

1. Insert the tension wrench and apply a little tension.
2. Find the pin that has more resistance than the other pins.
3. Maintaining light tension with the wrench, push the pin until it reaches the shear line. You'll know when you've reached the shear line because you'll feel a slight rotation in the plug, and often you'll feel (and even hear) a soft click as the pin sets. The pin stack will then be held in place. Although you probably can't see with the naked eye that the plug has rotated, you should feel it happening, as this minor movement is amplified in your hook and tension wrench.
4. Repeat steps 2 and 3 until you've set all the pins at the shear line, at which point the lock should open.

Most locks in competitions have security pins, so next let's discuss how these pins can be defeated with single-pin picking.

COUNTING PINS

It's useful to know how many pins are in a lock so that, if it doesn't open, you know whether it's stuck or you just have more pins to pick. You can determine the number of pins in several ways. Sometimes you can find the number from the brand and type of lock (either from experience or by looking up the lock's specifications). You might also see holes for the pins at the top of the bible, which will usually be plugged with a conical plug or screws. However, some manufacturers polish their locks, making it impossible to see the plugged holes (as is often the case with padlocks). It's also true that the number of plugged holes doesn't always match the number of pins.

The most reliable method is to determine the number of pins with a hook. Insert the hook in the lock at the center of the plug without using tension until the hook hits the first pin. Lift your hook and push on the first pin as far as it will go. Slide the hook farther into the lock until it hits the second pin. Push that pin out of the way, and repeat this process until you've pushed away all the pins. You now know how many pins are in the lock.

Alternatively, you can use the flat side of a half-diamond pick to count pins. Insert the tool all the way into the lock and push all the pins into the plug; then slowly slide out the pick while keeping it level. The pins will pop back one by one, allowing you to count them.

Picking Security Pins

Setting a security pin can be challenging, but it's a critical skill if you want to progress in lockpicking, since most worthwhile locks have security pins. *Security pins* have a unique shape that gives them a bit of wiggle room inside the lock, preventing them from binding like a standard pin even when you apply tension. Since we can't cover how to pick every kind of security pin, we'll focus on spool pins as an example. The guidance here should serve you well for other types of security pins too.

Recall from Chapter 4 that a *spool pin* has an indented middle section and is shaped like a spool of thread, as shown in Figure 7-9.

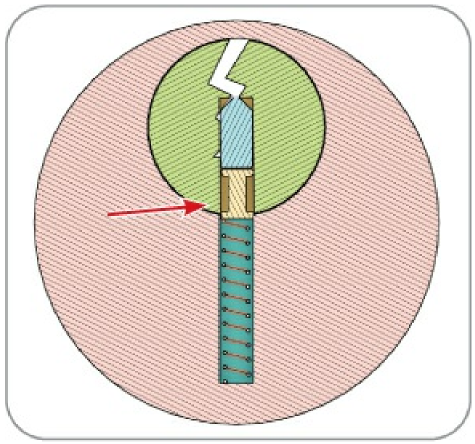


Figure 7-9: A pin stack with a spool pin

Spool pins are intended to prevent successful raking. Suppose you've raked a lock that has a single spool pin and managed to set all the standard pins to the correct height, so all that's left to set is the spool pin. When you rake while applying tension, the spool pin will rotate as its indented section meets the shear line, as shown in Figure 7-10. The spool pin is now trapped in a blocking position and can't be set to the shear line.

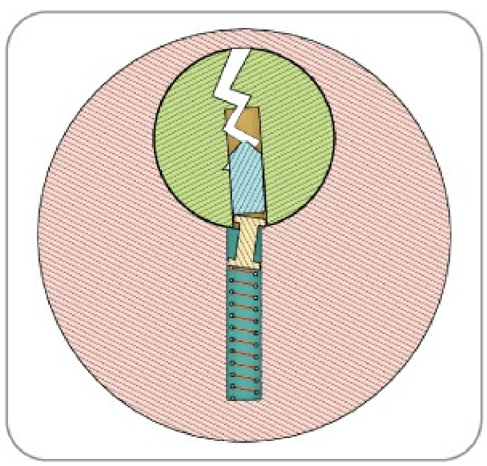


Figure 7-10: A spool pin that is blocking

You can use a hook to differentiate between a standard pin that's in its correct position at the shear line and a spool pin that's trapped in a blocking position. For a standard pin, when a pin stack is aligned at the shear line, as in Figure 7-11, pushing it farther is impossible, since the pin touches the housing and can't go any deeper. Note that you're still applying tension at this point.

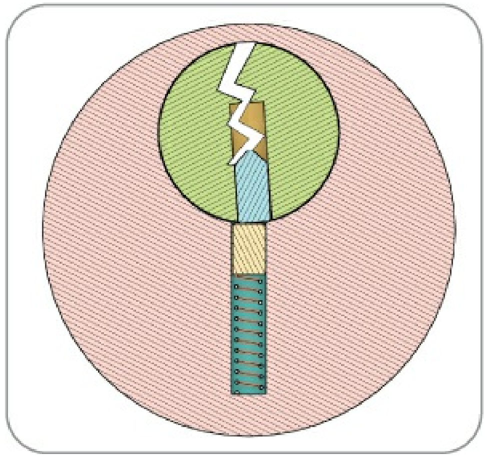


Figure 7-11: A standard pin in its correct position

With a spool pin that's blocking as shown previously in Figure 7-10, however, your hook will push the key pin against the spool pin. The spool pin then tries to straighten out to sit flush against the key pin, which causes the plug to rotate toward the *closed* position (opposite of the way you're tensioning the lock). As Chapter 4 explained, this is known as *counter-rotation*, and it's a dead giveaway that you're dealing with a security pin. It's important that you don't apply too much tension on the tension wrench here; if you do, you won't be able to feel the counteracting force.

NOTE

To summarize, when you push on a pin stack that doesn't move at all, it's at the shear line and should be left there. If, however, you feel counter-rotation in the tension wrench, you have a security pin that still needs to be set.

You can also tell that the lock has a security pin if the plug is clearly rotating but the lock is still closed. This happens only if you have all the standard pins in the correct position and the only thing keeping the lock from opening is one or more security pins. The distance that the plug can turn in this scenario differs from lock to lock. Some locks turn so much that you wonder how they can't be fully open yet; a lock in this state is considered to be in a false set. Typically, if a lock ends up in a false set when you're raking, you'll need to switch to single-pin picking to find and set the security pins.

Note that a lock will almost never have only security pins. In locks with spool pins, manufacturers always include at least one standard pin to prevent the plug from being able to wiggle with no key inserted.

Figure 7-12 shows the five stages of setting a security pin.

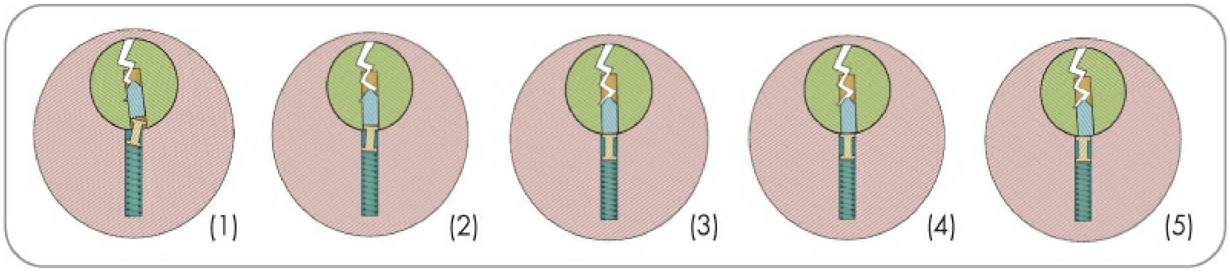


Figure 7-12: Setting a security pin

The five stages are as follows:

1. Apply tension and pick (or rake) the standard pins. The plug should rotate a little bit but not open. This indicates you're in a false set.
2. Try pushing on particular pins, and when you feel a counter-rotation in the tension wrench, you'll know that pin is a security pin.
3. Gently release a little bit of tension and push on the security pin until it's unstuck.
4. If you pushed the pin in the right distance, the pin stack will align at the shear line, the plug should again rotate in the direction in which you're applying tension, and the lock should open. If you've pushed too far, the pin will be overset and you'll have to start over.
5. If the lock has more security pins to set, or if any of the regular pins were reset because you released some tension, the lock will return to a false set, and you'll need to find the next pin to set.

Relieving tension when setting security pins is tricky. If you fully release the tension, the lock will reset and you'll have to repick the pins, so be sure to always maintain a bit of pressure. Even the counter-rotation required to set the security pin can be enough to release pins you've already set. Although that typically happens only with standard pins, security pins might also pop back. In rare cases, locks may have multiple security pins that are hard to set because as you set one, another releases.

You can practice setting security pins with special practice kits. Some are progressive sets that consist of several locks with an increasingly higher number of security pins. You can also collect various locks, keeping track of the number of security pins in each, to make your own progressive set. Another option is to take existing locks, open them up, and repin them (Chapter 5) to create a custom progressive set.

OTHER TYPES OF SECURITY PINS

In addition to spool pins (right), you might encounter other security pins including *serrated pins* (left) and *mushroom pins* (center). The spool and mushroom pins work similarly and can be picked in the same way, while the serrated pin can get stuck in multiple positions. When picking a lock with a serrated pin, you might need to click it down a few times before the pin fully aligns at the shear line.

Security pins with more exotic shapes also exist, mainly in high-security locks. Some pins are even made out of two parts that can move independently, though these are expensive to make and thus aren't found in common locks. When you have an unknown security pin, sometimes your best bet is to just keep trying until something works!

Overcoming Single-Pin-Picking Challenges

When the lock has a curved keyway, it can interfere with your ability to push on the pins straight from above. You might need to let your hook follow the curves in the lock to reach the pins, or push on the pins from the side. Try to get some locks with uncommon keyways to practice manipulating the pins.

All around the world, many keyways look like the one on the left in Figure 7-13. The mirror version shown on the right is much rarer. Picking these locks requires you to move the hook differently through the keyway to reach the pins. If you practice only on locks with the keyway shown on the left, you'll have a hard time when faced with the lock on the right in a competition. Make sure you practice both.

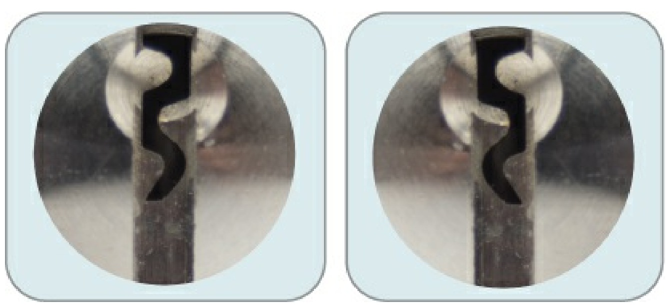


Figure 7-13: Mirrored keyways

In addition to the challenges keyways can present, you might also get frustrated by pins that need to be set very deep, especially if the previous pin needs to stay up high. The hook you use might not be able to push on the one pin while keeping clear of the pin before it. In such cases, you'll need to go through your collection of picking tools to see which one does the job.

Combining Raking and Single-Pin Picking

You can combine the speed of raking with the effectiveness of single-pin picking by using this quick technique:

1. Rake all the standard pins until the lock is in a false set.
2. Keep tension on the lock and swap the rake for a hook. Try to identify the security pins by pushing on all the pins one by one until you feel counter-rotation in the tension wrench.
3. Set that pin while you release a bit of tension on the tension wrench and let the plug turn slightly.
4. If, after the pin is set, the plug doesn't come back into a false set, this means some of the standard pins popped back. Swap your hook for a rake, and rake those pins again until the plug returns to a false set.
5. If the lock comes back into a false set and doesn't open, you know that you're facing another security pin. Again, grab your hook and find the security pin. By repeatedly setting an individual security pin and raking the standard pins in between, you'll eventually have set all the security pins, and the lock will open.

Many lockpickers start out by using this combined technique. When you get more experience in single-pin picking, you'll most likely change your technique to only single-pin picking (or to the waltering technique described next). While it's possible to get rapid results with raking, you can spend quite some time raking some locks just to find yourself in a false set. Once you master single-pin picking, using that technique to get into a false set and open the lock can be faster.

Using the Waltering Technique

You also can rake with a hook as you slide it out of the keyway.

> I've done this often enough in competitions, successfully, that friends have dubbed the technique *waltering*, though I don't claim to have invented it.
>
> —WALTER

This technique is a hybrid raking-picking process for locks with security pins:

1. Insert the hook into the lock, moving it all the way to the back of the plug, and as you take out the hook, slide the tip over the pins. You need to rake it more slowly and place more force on both the tension wrench and the hook than you usually would with raking.
2. You'll probably overset some pins, so after each rake, release a bit of tension on the tension wrench. You'll likely hear some pins popping back. This is normal with this technique.

3. Do another rake and release a bit of tension again. With many locks, a few rakes are usually enough to set the standard pins and get the plug to rotate slightly, indicating that it's in a false set with only security pins left to set. Because you're applying force on the tension wrench, you shouldn't have overset the security pins, just the standard pins.
4. When all the standard pins are set, switch to single-pin picking and set the security pins. If some standard pins pop back up, rake them using the waltering motion followed by a tiny release of tension.

Waltering differs from the standard "raking then picking" technique in that you release tension after each rake, and rake more slowly and with more force.

By combining waltering with tensioning the cam with your finger, you can open locks especially fast, which is essential in competitions. Waltering works well with certain brands of locks, such as Winkhaus, EVVA, and ABUS Pfaffenhain. Before attempting waltering, ensure that you have mastered standard lockpicking; also make sure to use a hook that doesn't bend easily, such as a SouthOrd MAX pick, as waltering requires more force than usual.

Using Pick Guns

Pick guns move a needle up and down into the keyway, aiming to set the pins all at once. They're generally not allowed in competitions, except for the freestyle competitions in Germany and the Czech Republic. Since they are a viable lockpicking tool, though, we'll offer tips on using them here.

Pick guns come with multiple needles of various lengths, but a flat needle is all you need. Use the flat side on the pins. Choose the shortest needle that can reach all the pins. To use a pick gun, follow these steps:

1. Set the pick gun to the lightest setting so it uses the least amount of force on the needle. Insert the needle into the lock so it rests on all the pins. This allows the needle to strike on all the pins at the same time. Ensure that the needle is straight. If you hold the pick gun at an angle, the needle might strike the side of the plug, which won't set all the pins and could even break the needle. You might also hit the pins in the front earlier and harder than the ones in the back, or vice versa, which won't allow the lock to open.
2. The needle should be inserted far enough to hit all pins, but not so far that it might hit the plug at the back. Check whether the needle is in far enough (hold the needle on the outside of the lock to see approximately how far it should go in), and move the needle up and down a bit to verify that it can move freely.
3. When the needle is in the correct spot, engage the pick gun:
   a. For a manual gun, shoot and almost immediately tension the lock to open. If it doesn't open, release the tension, check whether the needle is in the correct spot, and try again. Don't tension the lock too much, as this will capture the pins, making it

harder for the pick gun needle to move them. Try to turn open the lock just after the needle has hit the pins. If you're too early, the lock won't open because the pins aren't yet in the correct position; too late, and the pins will have been pushed back to their original position by the springs. The lock has a sweet spot at which it will turn open; getting the timing right takes practice.

b. For an electric pick gun, press the button to set the needle in motion and keep it pressed so the needle shoots multiple times. Vary the tension and continue until the lock opens. You can either keep your finger on the button or press it for just a few seconds at a time.

NOTE

With some paracentric keyways, you might struggle using a pick gun, as it can't make the bend; you'll notice this if the needle doesn't move freely.

If the lock won't open, try adjusting the force with which the needle strikes (usually by twisting a wheel or screw on the pick gun) and start over again.

Picking Other Types of Locks

So far, we've talked about standard pin tumbler locks, with a single row of pin stacks and a vertical keyway. Plenty of other types of locks are around, many of which can be picked using the same techniques, although some require special tools or using your tools in a different way. In this section, we'll look at dimple locks, locks with multiple rows of pins, and a few other elements and techniques.

The locks presented here are currently rare in competitions, but their popularity will likely increase as the sport of lockpicking progresses.

Dimple Locks

Dimple locks have a horizontal rather than vertical keyway, which affects the way you hold your tools. Otherwise, you pick dimple locks in much the same manner as pin tumbler locks.

Tensioning Dimple Locks

A thicker or wider tension wrench, such as the one shown on the right in Figure 7-14, is most suitable for dimple locks. You'll find that small tension wrenches—like those that work especially well in locks with narrow keyways—are too small to get a grip in a dimple lock. The tension wrench shown on the left in Figure 7-14 can be fully turned within the keyway without gripping the plug, so it's clearly too small for this lock.

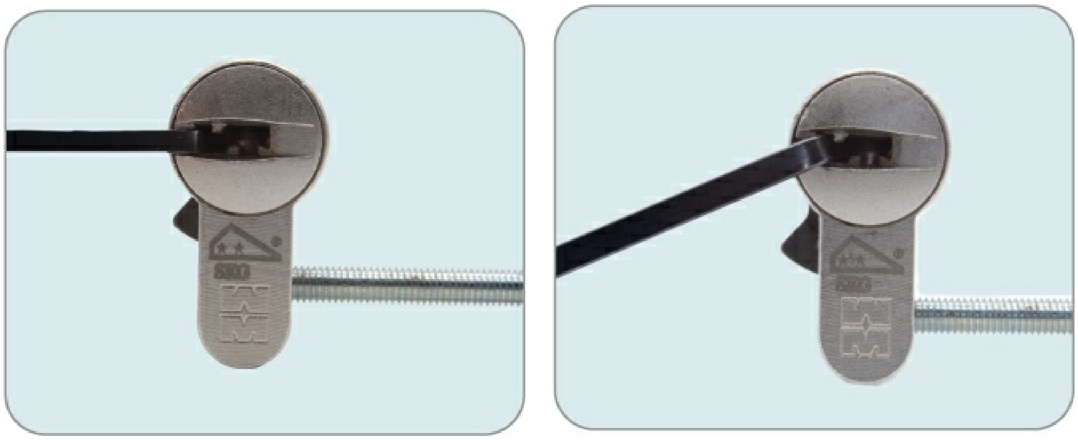


Figure 7-14: Two different sizes of tension wrenches

Take care not to scrape the tension wrench against the housing, as that creates friction, which makes picking the lock more difficult.

Raking Dimple Locks

Mountain rakes are the most effective tool for raking a dimple lock, surprisingly more so than specialized dimple rakes. The mountain rake in Figure 7-15 has a long stretch of teeth of similar lengths, making it easier to use as a sideways rake.

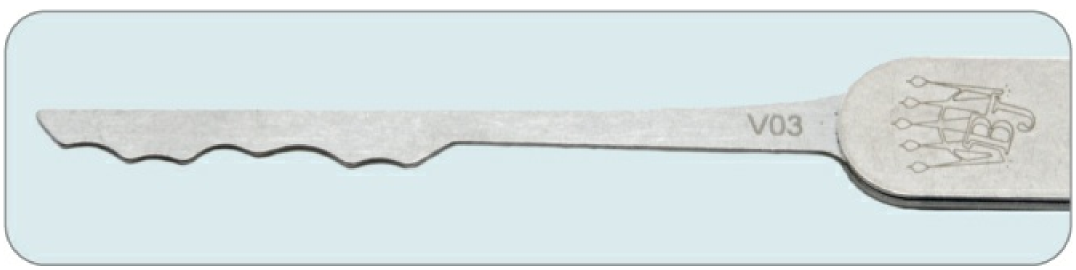


Figure 7-15: A mountain rake with teeth of similar lengths

You come in from the side and move the rake back and forth while touching the pins on the top, as shown in Figure 7-16.

Figure 7-16: Raking a dimple lock with a mountain rake

Some cheaper dimple locks have only standard pins, which means they can be raked, whereas others have security pins, requiring single-pin picking.

Single-Pin Picking Dimple Locks

To manipulate individual dimple pins, you can use a regular hook or half-diamond pick, as explained in Chapter 6. Insert the picking tool horizontally and twist it to push on the pins. With dimple locks, you can insert your picking tool from the left or the right of the pins, wherever you have room. Depending on the shape of the keyway, you might want to slide the tool against the edge of the keyway to help guide it.

Dimple locks can be frustrating, as they tend to "eat your pick": when you're trying to set a pin and maneuver the tip of a hook, the tool can get stuck. Rotating the hook back to where it was is almost impossible, so before you can do anything else, you'll need to free the tool by inserting a flat piece of metal, like another picking tool or tension wrench, to make room for the stuck tool to come out. You may need to push against all the pins as far as you can.

NOTE

Dimple pick guns, strictly speaking, are not pick guns, but rather they use foil impressioning to open dimple locks. With foil impressioning, you tension the lock to create the key bitting in a skeleton key wrapped with aluminum foil. You'll probably be quicker single-pin picking a dimple lock than using a dimple pick gun.

Locks with Multiple Rows of Pins

As we've discussed, one way to make a lock more resistant to lockpicking is to simply add more pins. The disadvantage is that locks have only a certain amount of space, so manufacturers are limited in the number of pins they can add. Most regular locks contain five pins. Figure 7-17 shows a BEST IC cylinder with seven pins in a straight line. Other examples are the ASSA ABLOY seven-pin lock and the Mul-T-Lock 7×7.

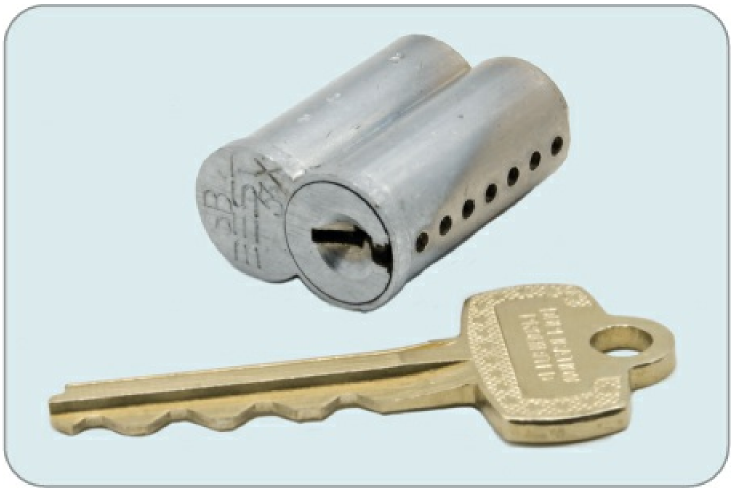


Figure 7-17: A BEST interchangeable core with seven pins

INTERCHANGEABLE CORES

Recall from Chapter 2 that ICs have two different keys. The regular key is used to open the lock, and the control key is used to rotate the plug and retract the control lug, allowing the whole core to be removed and replaced.

ICs have multiple shear lines, which complicates picking. All pins need to be set at the same shear line, either the one for opening the lock or the one for changing it out. Opening the lock at either shear line could be considered a successful open in a competition, depending on local rules.

To include more pins, manufacturers must introduce multiple rows to the lock; in turn, the key needs to have multiple rows of cuts (see Figure 7-18), which makes copying it more expensive and difficult.

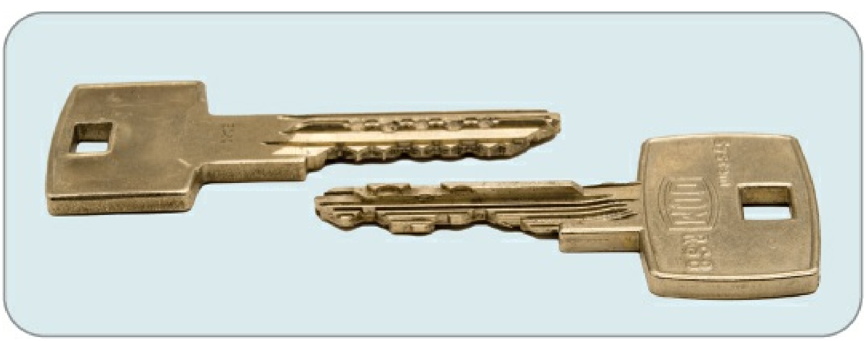


Figure 7-18: Keys to locks with multiple rows of pins: ABUS Pfaffenhain KV14 (top) and DOM RS 8 (bottom)

In locks with multiple rows, one row of pins always needs to be set completely before the pins in the other rows start to bind. As a result, when you have two rows of 6 pins each, you're basically picking a 6-pin lock in the first row and then another 6-pin lock in the second row, as opposed to picking one 12-pin lock.

The row you need to set first depends on the lock. Start picking in any row. If you feel a binding pin, you know that this pin's row is the first that needs to be set. If no pin binds, you need to switch to another row. Once all pins in that row are set, you might feel the plug rotating a little, like a false set, after which the pins in the next row will start to bind.

Manufacturers position multiple rows of pins in all kinds of ways. The DOM System D and the ASSA Twin have two rows in parallel, which means the pin stacks aren't perpendicular to the core. These locks are rare because the nonperpendicular stacks make it harder to get the shape of the pin to match the curvature of the plug. Figure 7-19 shows such a cylinder without its plug.

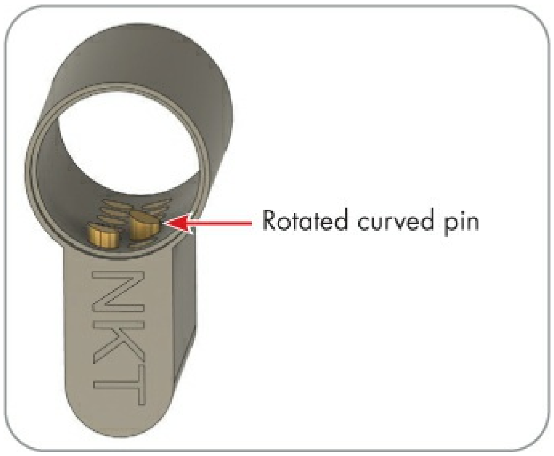


Figure 7-19: A cylinder with two parallel rows of pins

As you can see, two curved pins are elevated beyond the shear line. If such a pin inadvertently rotates, as the one on the right has, it won't sit completely flush at the shear line. Additional features need to be built into the cylinder to prevent the pins from rotating, which makes these locks more expensive.

Mul-T-Lock patented a design, the Mul-T-Lock Interactive, with a second row of pins *inside* an existing row of pins. Figure 7-20 shows a cutaway version of this cylinder.

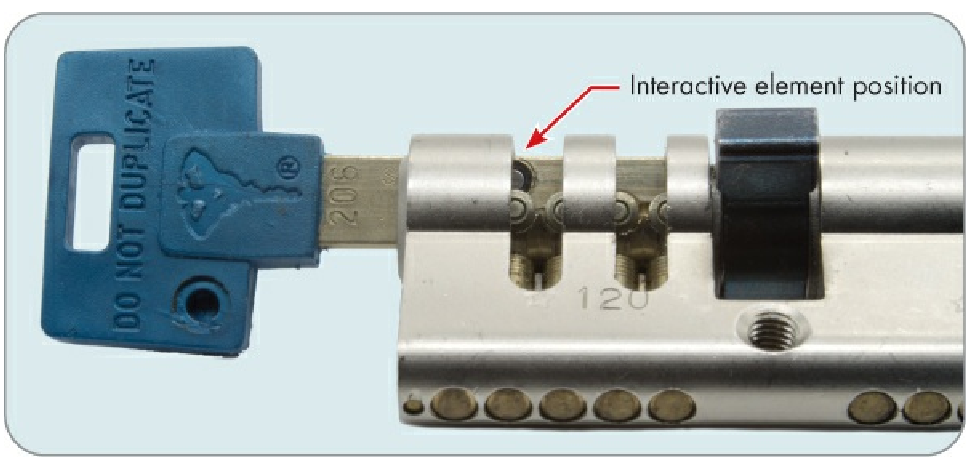


Figure 7-20: Mul-T-Lock Interactive

Here you can see hollow pins with smaller pins inside. When you tension the lock, the hollow outer pins bind first. Once the outer pins are set, the lock will turn slightly as if in a false set, after which you can start picking the inner pins.

Figure 7-21 shows a picking tool made specifically for the Mul-T-Lock Interactive, shaped to allow it to pick the outer and inner pins. You move the tool back and forth to the discrete positions of the pins. You could do the same job, at lower cost, with a standard hook. In a competition, dedicated tools like these are often prohibited.

Figure 7-21: Mul-T-Lock Interactive picking tool

The Mul-T-Lock Interactive is so named because an element in the key *interacts* with an extra pin in the plug. This extra pin pushes on the interactive element, which extends outside the key while pushing on a key pin on the other side of the key. Because the interactive element extends out of the key, this key pin needs to be pushed in very deep—deeper than the others.

The interactive element is always in the second pin position for this brand and type of lock. Therefore, if you recognize a lock as a Mul-T-Lock Interactive, you know that the second pin from the front (the leftmost pin in Figure 7-20) needs to be pushed in very deep. You can use standard tools to do so.

Some locks have a standard row of pins and a second row on the side whose pins are operated by dimples or extrusions on the side of the key, like the ABUS Pfaffenhain KV14 key and DOM RS 8 key in Figure 7-18. The Pfaffenhain key has dimples on its side. In the lock, ball bearings in the plug drop into the holes in the key to make room for a pin that comes in from the side. The DOM lock has a second row of pins that are operated by protrusions on the side of the key. For both of these locks, you have to set the pins in one row before setting the pins in the other.

Dimple locks commonly have three or four or even more rows of pins, which might be next to or opposite each other. The more elements in the lock, the harder it is to pick. Consider the cutaway version of the Kaba Quattro, shown in Figure 7-22.

NOTE

Kaba became part of Dormakaba through its merger with Dorma in 2015.

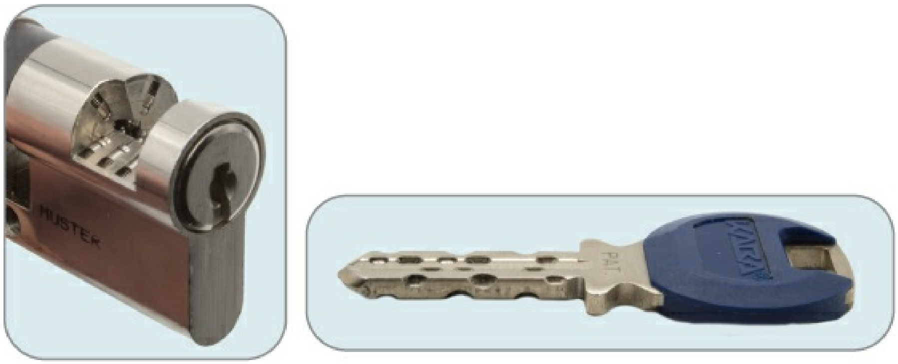


Figure 7-22: Kaba Quattro cylinder and key

This lock has four rows of pins. The pins are very short and fully contained in the plug, which means each pin has only a few possible depths. Since the lock has so many pins, it is challenging to pick. Notice that the pins are also extremely close together, making it harder to keep track of which pin you're manipulating in which row. Since picking these locks is so difficult, they aren't typically included in lockpicking competitions.

Locks with Passive Key Control

Active elements are parts you need to move to the correct position to open the lock, such as the pins we've been dealing with thus far. *Passive* elements are additional parts that are already in the correct position without the key inserted. These are used to verify the key shape, such as a dimple in a certain position; this allows a manufacturer to provide blank keys with specific dimples only to selected locksmiths, providing better key control. If a dimple is missing, the passive element (such as a ball bearing) will be pushed into the locked position. If the passive element has room to stay in its default position, the lock can open.

Let's look at an example. Figure 7-23 shows both sides of the key for a WILKA Carat S1 lock.

Figure 7-23: Wilka Carat S1 key

This key has six cuts, so the lock will have six pin stacks. These pins are active elements. The key also has four dimples on the side that ball bearings within the lock drop into. The ball bearings in the lock that drop into the dimples are the passive elements.

For lockpickers, these passive ball bearings are nothing to worry about; while they can be moved, opening the lock doesn't require pushing them to a shear line against a spring. Instead, the ball bearings just need to have room to move out of the way when the plug turns. The dimples in the side of the key provide that room. Without these dimples, the ball bearings would get stuck and prevent the plug from turning, which is how passive elements verify the key's shape. Passive elements like these are often used in master-key systems. When no key is present at all, the ball bearings have all the space they need to move out of the way.

The lock for this key is shown in Figure 7-24.

Figure 7-24: Wilka Carat S1 cylinder

Notice the round mark on the side of the cylinder. Beneath that mark is an additional active pin with a spring behind it that needs to be set precisely at the shear line, just like the six standard pins. This pin is pushed to the shear line by a movable protrusion in the key (in this case, a ball bearing), which is visible in the right-hand image of Figure 7-23. You set this active pin with a standard hook, just like all the others.

Locks with Sliders

Locks can also contain *sliders* (introduced in Chapter 4) instead of or in addition to pins. Figure 7-25 shows the key for an SEA 3 lock; the wavy lines indicate that the lock includes sliders.

Figure 7-25: SEA 3 key

The 10 sliders (5 on each side) in this lock are flat, rectangular pieces of metal. The sliders have a tiny pin that rides on the groove in the key. When the key is fully inserted, the sliders will be in their final position. If they're pushed up or down to exactly fit within the plug, the plug can rotate, and the lock opens.

You pick a lock with sliders with a standard hook and tension wrench. Use the hook to move the sliders left and right, or up and down, depending on where they're located. For this lock, the key is inserted vertically, so you need to move the sliders up and down. If a slider moves freely under your hook, it's not yet binding. Continue feeling the sliders until you find the one that's binding, and move that binding slider until you feel it's in the correct position. You will feel this in the hook and the tension wrench, just as if you were picking a single pin in a standard lock. In this lock, the sliders will be on either side.

The SEA 3 key also has dimples on the side, indicating the lock has pins as well. These are active pins, meaning they need to be picked. Picking these pins is like picking the pins in any standard lock.

The front of the SEA 3 cylinder has tiny flat-headed pins in the sides of the keyway, visible in Figure 7-26; this is another indication that the lock contains sliders.

Figure 7-26: SEA 3 cylinder

The key for the slider lock is identical on both sides so that it works either way you insert it in the cylinder; this is known as a *convenience key*. When a convenience key is inserted in the cylinder, only the bottom slider grooves and dimples in the keys operate the lock. If you reverse the key, the top slider grooves and dimples operate.

Locks with Rotating Pins

In Chapter 4, you saw the Medeco Biaxial lock, which has chisel-tipped pins that rotate. For the lock to open, the pins need to be set to the correct depth and rotated to the correct angle. The pins have a vertical groove cut into them, and the plug contains a sidebar that drops into these grooves when the pins are properly aligned, allowing the plug to rotate. You can rotate the pins by fiddling with them at the sides with a hook.

Disc Detainer Locks

As discussed in Chapter 3, the discs in disc detainer locks have a little notch cutout called the *gate* (Figure 7-27).

Figure 7-27: Two discs from an ABLOY Classic disc detainer lock

When all the gates in the discs align perfectly, the sidebar (shown at the top of Figure 7-28) can fall into the groove they create, allowing the plug to move.

Figure 7-28: A cutaway ASSA ABLOY Classic lock

The angles of the cuts on the key determine the rotation of each disc in the lock. The position of the gate on each disc matches these angles. Though you could try to manipulate the individual discs with a hook, you'd be left with the problem of tensioning the lock: the tensioning force needs to be applied to the end of the plug deep inside, rather than to the keyway at the front of the lock. A regular tension wrench doesn't have the correct tip to interact with the lock, and would block up the whole keyway in order to extend all the way to the back.

Instead, you need special disc detainer tools that integrate the tension wrench and the hook. These tools vary in price depending on the lock's complexity. Figure 7-29 shows a tool for the ABLOY disc detainer lock in Figure 7-28.

Figure 7-29: ASSA ABLOY Classic decoder tool

The dimensions of the ABLOY Classic locks can vary depending on when they were produced, so this tool comes with detachable end pieces that can be exchanged. This is an expensive tool that works only on ABLOY Classic locks. You shouldn't need such specialized tools for typical lockpicking competitions, though trying them out is a lot of fun if you're looking for a challenge.

Disc detainer tools will not only pick the lock but also decode it, meaning you can use the tool to learn the lock's configuration and then use that configuration to open the same lock as many times as you like. A decoding tool has a knob that allows you to position it at a specific disc. By keeping track as you move from disc to disc, you learn the setting of each individual disc. Some tools also have a clicker (with a scale) that clicks into place for each disc position so you know exactly which disc you're manipulating. If you keep track of each disc's rotation as you set it, you'll know the combination after you've opened the lock.

Locks with Unusual Keyways

Sometimes manufacturers design keyways that hinder tool insertion. The ABUS XP1 lock (Figure 7-30, left), for example, has a zigzag in the keyway, restricting the space available to reach the pins. Your best bet, depending on the bitting of the key, is to try picking with a half-diamond pick.

Figure 7-30: ABUS XP1 (left) and EVVA 3KS (right) keyways

The EVVA 3KS (Figure 7-30, right) and 4KS have sliders on both sides that almost touch each other in the lock, leaving little space to insert a picking tool. Determined lockpickers have had to resort to making tools out of very thin metal.

Specialty Locks

High-security locks have many other mechanisms you might encounter, as discussed in Chapter 4. The EVVA MCS key shown in Figure 7-31, for example, contains four magnets, and the MCS lock requires custom tools to be picked.


Figure 7-31: The EVVA MCS key

Other mechanisms include pins that interlock, locks with multiple shear lines, locks with freely rotating plugs, locks with wafers instead of pins, locks with pivoting elements, and more. Luckily, these are rarely seen in competitions. To learn more about these specialty locks, we recommend *High-Security Mechanical Locks* by Graham W. Pulford (Butterworth-Heinemann, 2007).

Creating or Adapting Tools

You might enjoy making your own tools as an extension to locksport. Locks included in locksport competitions don't require such tools, but picking high-security locks and creating tools for doing so can be rewarding.

Making tools from scratch can require a lot of equipment, prototyping, and knowledge of materials, but modifying existing tools is easy. To create or modify a tool, start by disassembling the lock you intend to use it on and examining the parts to figure out the best shape for your custom tool. Search for videos online of that specific lock being picked to get an idea of details that your tool might require.

Say you have a specific dimple lock, but none of your tools have proven any good for opening it. You could buy a cheap set of dimple picks and change the shape by using a file or a Dremel tool to suit the shape of the lock.

As an example, Walter owns a DOM Diamant lock (see Figure 7-32), a disc detainer lock he hadn't been able to pick with regular tools.

Figure 7-32: DOM Diamant

In the ABLOY Classic, the discs rotate only after you've fully inserted the key and turned it. In the Diamant, however, the discs start to rotate as soon as the key is inserted. When the key is fully inserted, the discs are in their final position.

To customize a tool for the job, Walter started with an existing Chinese disc lock tool. He needed to modify its tip to fit the Diamant in order to apply tensioning; however, the tip included with the tool wasn't suited to be filed down, so instead he replaced the tip with a common nail and used a Dremel to achieve the correct shape. Figure 7-33 shows the result.

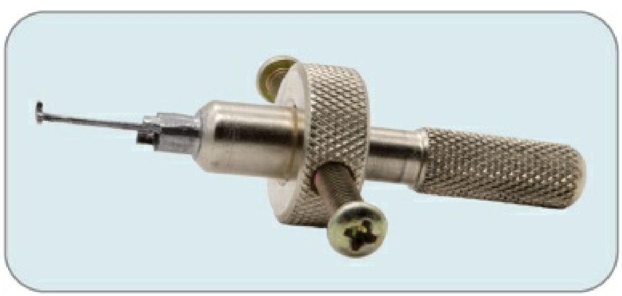


Figure 7-33: Homemade tool to pick a DOM Diamant

Having disassembled the lock, he could test whether the tip could pass the individual discs and file more off whenever needed. Making such a tool requires perseverance, multiple rounds of tests, and many hours.

Getting Experience

To gain experience with lockpicking, try opening a standard pin tumbler lock repeatedly with the same tools. As you start to understand the amount of force to use, the locations of the security pins, and so on, subsequent openings should be faster. Once you've mastered that process, try opening the same lock again with different tools. When you can open a lock multiple times, in the same amount of time, you have truly mastered it.

As you pick a variety of regular locks, you'll begin discovering patterns. Just as we've found the waltering technique works well on Pfaffenhain locks, you might find that the Bogotá rake quickly opens locks of a certain brand, that locks without a brand name often don't have security pins and can be raked open, and that locks with a paracentric keyway typically have security pins inside. These patterns will improve your skill and knowledge.

When practicing with dimple locks and high-security locks, search online for information about their inner workings. For example, consider the lock in Figure 7-34.

Figure 7-34: A lock with two rows of pins

You can see that this lock is made by DOM and that it has two rows of flat pins on one side. The keyway has milled slits and a round recess on the top. Searching for *DOM cylinder* images will lead to similar-looking cylinders. DOM locks with the recess in the bottom are the DOM ix 6SR, and those with the recess on top—like this one—are the DOM ix Saturn. Knowing the locations of the pins, their number, and whether any pin goes deeper than the others will help you pick the lock, and quickly. You can find this information by knowing the lock's brand and type.

Once you know the make and model of a lock, you can search for marketing material showing the insides of the lock from the manufacturer, pictures of the key, and videos on how to pick the lock. A word of warning: some people remove pins or elements from the lock to make it easier to pick, so you can't always trust these videos. You can find YouTube videos of original locks being disassembled after they're picked by searching for the brand and type of lock along with the phrase *picked and gutted*.

After a bit of searching, you'll find the key for the DOM lock from Figure 7-34 (see Figure 7-35).

Figure 7-35: A DOM ix Saturn key

You can see that the key has two protruding ledges with holes in them; these ride on the two rows of pins you saw in the keyway. The key also has two rows of dimples, one between the two ledges and another on the side. This indicates that the lock has two more rows of pins that are operated by those dimples. The key has a movable element shaped like a donut on the tip, which matches the recess in the keyway. The recess allows the donut to move when the key is inserted. When the key is fully inserted, the donut pushes one pin deeper than all the other pins.

The keys' dimples and protrusions push down the pins and release the cylinder. Figure 7-36 shows how far the key from Figure 7-35 can push down a pin. When picking, you'll need to go deeper only if there's an interactive element in the key.

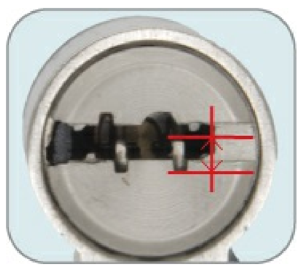


Figure 7-36: Maximum movement of the pin in a DOM ix Saturn

The longer you pick locks and the more variety in the locks you pick, the more knowledge you'll gain that can help you in a competition. If you'd like, you can take notes on what you've learned to bring with you to a competition.

Summary

In this chapter, you've learned how to hold locks and tools and tried techniques to open pin tumbler locks, dimple locks, and locks with special elements. You now know enough to start lockpicking on your own and improve your skills. We encourage you to practice—revisit locks you've already opened until you're sure your success is from technique and not luck, try combining raking with single-pin picking, and experiment with a range of locks and difficulty levels.

In the next chapter, you'll learn about preparing for and attending lockpicking competitions.

8
PIN TUMBLER LOCKPICKING COMPETITIONS

Opening is good; opening fast is better.
—Lockpickers' saying

With practice, you should find yourself getting better and better at picking pin-based locks, and at some point you may be interested in entering competitions. In this chapter, you'll learn what to expect from, and how to prepare for, a competition. We'll go over what to do if you're given a lock you've never seen before, as well as other helpful tips to improve your chances of success. We'll end the chapter by exploring a few well-known competitions from around the world.

Competition Basics

Lockpicking competitions around the world differ in many ways, but they typically consist of several rounds in which you open numerous locks in a limited amount of time. The highest scorers in each round proceed to the next round and, eventually, to the finals. You win a round by opening the most locks. If a tie occurs, the competitor with the fastest total time for that round wins. *Total time* is the sum of the opening times for all the locks in that round. Sometimes competitors are given a button to press when they've opened the lock, but usually everyone keeps track of their own opening times.

In the Dutch system, at the beginning of the competition, competitors are split into groups by random draw; the highest scorers from each group proceed to the semifinals and finals. In Germany, everyone is generally in one big group, with the highest-scoring contestants proceeding to the A- and B-finals. The B-final comprises those who scored just below those in the A-final.

The further you advance in the competition, the harder the locks are likely to be. Competition locks are those typically found in the host country, though standard pin tumbler locks and dimple locks are the most popular. In many German and Swiss competitions, along with some US competitions, people bring their own locks for others to pick.

Competitions might be stand-alone or part of a larger event like a conference. They're often accompanied by workshops and lectures, like the multiday Dutch event LockCon, which evolved from and now includes the Dutch Open competition. For some more-exclusive events, you must be invited or be a member of a particular lockpicking group in order to compete.

Some competitions are just for beginners or have designated areas for beginners, so you can participate in competitions even if you've just started. Competitions allow you to practice picking under stress, but also give you the chance to meet other lockpickers who have advice, tips, and often years of experience to share.

NOTE

Check the websites for the lockpicking groups listed in Chapter 1 to find upcoming competitions near you.

In general, US competitions are easier than European competitions because they use American locks, which have wide keyways and are easier to pick. In terms of difficulty, the US is followed by Australia, Switzerland, the Netherlands, the Czech Republic, and then Germany and France (see Figure 8-1 for a shot of Walter in action at a French competition). Germany also hosts the *Blitzöffnung* competition, which is specifically aimed at beginners. That said, we encourage you to try any competition in your area. Even if you drop out in round one, you've still gained valuable experience!

Figure 8-1: Walter at work during the French competition in 2018 (© William Burkhardt)

Once you find a competition that suits you, you need to register. Competitions generally have online registrations these days, so just find the relevant site and follow the instructions. Some also let you register in person when you arrive. After you've registered and made your travel plans, it's time to prepare.

First, make sure you understand the rules of the competition. If locks are provided, you might be able to find out the kinds of locks being used by checking public announcements or contacting the organizers; in general, the lock type is not a secret. You can then prepare by practicing on locks of the same brand and type to get an idea of how the security pins feel and how much force you need to use on the tension wrench and the picking tool.

Pack everything that you might need, including the following:

- A variety of tension wrenches
- A variety of picking tools and rakes
- Spares for the picking tools you use most (in case they break)
- A vise (optional)
- Any notes you might want
- Pen and paper
- A stopwatch (your phone will do)
- A pick gun for freestyle competitions
- Any locks you might want to trade
- This book!

If you need to travel across time zones, be sure to include downtime in your itinerary to adjust. Locksport events are incredibly social, with a lot of attendees who don't see each other in real life very often. There will be late-night partying. You'll want to have the energy to both pick locks and socialize.

At the Competition

When you're at the venue, register for the competition if you haven't already done so. Note the location and time of your event(s). Be there on time and bring your lockpicking gear. You'll be seated by the organization. When everybody is seated, the competition can start.

The rules will be explained first, and if something is unclear, don't hesitate to ask for clarification. The locks will then be handed out to the competitors.

Inspecting Your Locks

When you pick locks casually, you have all the time in the world to try various tools and techniques. In a competition, you need to open them quickly, so you want to choose the right tool and technique from the start. You might be given a lock, however, that you haven't seen before. You'll have some time between receiving the lock and the start of the competition; use that time to inspect the lock and determine your strategy.

Inspecting a lock can give you a lot of information about how to proceed. If you recognize the lock as one you've practiced on before, you'll have a good idea of which tools and how much tension to use. This is why practicing on many types of locks is crucial. You can look into the keyway to determine whether a lock is a standard pin tumbler lock, a dimple lock, or something else. You should also be able to see whether it has a single row or multiple rows of pins.

You can use various other clues to decide your next steps. For instance, locks without a brand name often don't have security pins and can be quickly raked open. Locks with a paracentric keyway typically do have security pins. Suppose you're given the lock in Figure 8-2.

Figure 8-2: Front view of a standard pin tumbler lock

The keyway looks like that of many Euro profile cylinders, and no brand name is displayed. This tells you it's a simple, cheap lock, and chances are it has no security pins. With that information, you might start by trying to rake it.

The bottom of the lock might show marks where the pins were inserted during manufacturing, which can indicate the maximum number of pins the lock holds. For example, consider Figure 8-3, which shows the bottom of a Euro profile cylinder.

Figure 8-3: A lock that most likely has six pins

This lock has six holes on each side where the pins were inserted. The same housing might be used for locks with five or six pins, so we can't be sure they're all filled, but that's the likeliest scenario. The little round marks at both ends aren't pin stacks, but hardened steel inserts to provide more resistance against brute-force attacks like drilling.

Let's inspect another lock as an example. Figure 8-4 shows a lock with three pins visible —at the top, left, and right—meaning it probably has three rows of pins.

Figure 8-4: A lock with three rows of pins

We can tell that this is a dimple lock because the pins come in from multiple sides, and the brand name KESO is obvious. If you've encountered such a lock before, you might have researched it and found that it's a regular KESO 2000 lock, as the older KESO 1000 doesn't have a rectangular key, and the KESO 2000 S Omega has an Omega symbol (Ω) stamped in the plug. Then you'd know for a fact that the three rows of dimples are the only pins in this particular lock.

Some people use lights to look inside the keyway, but beware that this might leave you with more questions than answers. All the passive pins in the lock (those you can leave as is when lockpicking) will be visible with the light.

> I typically find it easier to feel where the pins are by probing with a picking tool. If a lock won't open, I'll sometimes use a light to see if there is an additional locking mechanism, but you can also feel for those by using a picking tool.
>
> —WALTER

Some lockpickers use a small flashlight with a fiber-optic attachment in various sizes that fits right into the keyway (Figure 8-5). You can also make one using a small USB light, a power bank, plastic fiber (from a cheap fiber lamp), and moldable rubber.

Figure 8-5: A portable light with a fiber-optic attachment to fit in a lock

Figure 8-6 shows the flashlight inserted into the keyway of a DOM ix Saturn lock.

Figure 8-6: Looking inside a DOM ix Saturn

When inspecting the lock, pay attention to anything else that seems out of the ordinary; it might give you clues as to how best to crack it. Consider the lock in Figure 8-7.

Figure 8-7: A Zeiss IKON lock

The keyway looks normal, aside from two grooves milled out to the left and right at the same height. You can assume the grooves match the shape of the key. Maybe they're there to make copying the key harder because you'd need blank keys in the correct shape. But if you have a blank that's missing the protrusions and still operates the lock, they would be pointless. There must be something in these grooves that needs to be activated to allow the lock to open. It could be two rows of pins or just one pin.

For a mystery lock like this, start by picking the standard pins. When it looks like they're set (maybe the lock is in a false set), you can look for pins in the two grooves. If you feel something click or the lock opens, great! Otherwise, concentrate on the standard pins and recheck the grooves occasionally to feel for any extra pins. If you've encountered this lock before and did some research online, you might have found that it has one element at the far end that needs to be pushed aside in the groove, and determined that this lock is the Zeiss IKON Sperr-Rippenprofil.

The WILKA Carat P1 (and its successor, the Carat S1, described in Chapter 7) has a round indent on the side of the lock indicating that something may have been inserted. The insert, shown in Figure 8-8, could be a pin or bar that's operated by the key, or a passive pin.

Figure 8-8: A WILKA Carat P1

Even without looking at the key, you can see from the cylinder exactly where you need to hold your picking tool to operate whatever is in there. Concentrate first on the standard pins and try to get the lock in a false set. It doesn't hurt to occasionally manipulate the spot to see if the lock opens. In this particular lock, the indent indicates an active security pin, so it needs to be set precisely.

Feeling the Lock

In a competition, you can't start picking your lock until told to do so. But generally—depending on the competition's rules—you're allowed to hold it, put it in a vise, and try out a tension wrench before the time starts. You can feel whether the cam is attached to the plug (and, for Euro profile cylinders, on which side) if you plan to apply the turning force to the cam directly with your finger. When inserting the tension wrench, you can try turning the plug both ways. This will give you an idea of how smoothly the lock rotates.

If you use a vise, put your lock in it. Select a tension wrench that fits the lock comfortably, and find a comfortable position for holding it so you don't waste time doing so once the clock starts.

Doing Lock Recon

Talking about the lock with your competitors can be useful (talking *to* the lock, not so much). You can ask whether they know about any peculiarities with the lock, or how they might approach it and with which tools. Obviously, you can't ask how deep or in what order you need to set the pins; that is for you to find out. But asking for peculiarities, which you might know only if you've seen a similar lock before, is not considered unsporting.

In competitions allowing participants to bring their own locks, asking the owner and other contestants about the lock can be especially helpful. The owner may decide not to tell you much, but they won't judge you for asking.

> At a German competition, I asked a fellow competitor if he could tell me anything about the lock I was handed. He said I needed to pick it upside down. It turns out this lock was a Gera 3500 Euro profile cylinder. From the outside, it looks like any other cylinder, but there's a magnet in the key. This magnet pulls up one passive pin, whereas all the other pins are pushed down against springs like any standard pin. To pick the lock, you need to either use a magnet to pull up the one passive pin or make use of gravity and hold the whole lock upside down. The passive pin will drop into place (there's no spring action on it), and you can then pick the remaining pins normally. I saved a lot of time by asking about the lock before I started picking, and now whenever I come across the Gera brand on a cylinder, I know it might have a magnet inside.
>
> —WALTER

If you're a beginning lockpicker, you won't be considered a threat, and most lockpickers you meet will be friendly and helpful. Once you become well versed in lockpicking, you'll be familiar enough with various types of locks that you won't really need to ask competitors.

Organizing Your Knowledge

The more you look at and pick locks, the more you'll learn about them. Remembering every detail about all the locks you've picked can be difficult, so consider tracking your discoveries in a small notepad that you can bring to competitions.

Some locksporters go as far as marking their picking tools with the depth at which they need to be inserted into a specific type of lock to reach the individual pins. You'd need different markings (and thus different tools) for each type of lock. This might be overkill, but taking notes on what you've learned about particular lock types can be helpful.

Observing Your Competitors

Look at what others are doing during the competition, especially whoever is picking the lock you may be getting next. Which side did they pick? With what tool? Was it raked? You may even be able to spot the locations of the security pins and the order in which they were set. As a beginner, you'll probably spend most of the allotted time fully focused on your own lock, so don't worry if you don't have much time to look around. Once you're more experienced, you'll look less at your own hands while you're picking, leaving you with the opportunity to observe others.

This may seem controversial, as you're supposed to compete and win on your own. Watching someone else may feel like cheating. The reality, however, is that to make the competition fair, the exact same lock must be opened by every competitor, so everyone has the same opportunity to watch others before opening it themselves. There are no hard feelings.

If the opening time is displayed, you can gain information by looking at how long it took other competitors to open the lock you're about to pick. For instance, if everybody opened the lock in a few seconds, it's a safe bet that you can open it by raking. Beware, however, of possible negative psychological effects: if you see long times and start worrying that a lock is hard to pick, you may well find it more difficult.

Being a Good Sport

As mentioned, people who practice locksport tend to be kind and helpful. If you ask them for advice, even during the competition, they'll often gladly give it. This camaraderie speaks to locksport's hacker roots, with *hacker* meaning somebody who enjoys using their technical know-how in a creative and playful way to explore and overcome limitations. If you're not already living by the hacker ethic, you can start to embrace it by being a good sport and helping other competitors in return.

Being a good sport also means not using new tools and techniques that might give you an advantage without first consulting the competition's organizers. Lockpicking competitions might or might not specify exactly which tools you can and cannot use. When in doubt, ask.

Keeping Your Cool

No matter how well prepared you are, the competition setting will make you more tense, and you may well find yourself using too much pressure on your tools and struggling to open a lock.

> After a lot of practice, I became pretty good at opening locks, but that skill didn't show at competitions because I wasn't used to picking in a high-tension environment. I would often feel stressed out when others would open the lock before me, and I'd start switching tools and strategies. I would underperform, and underperforming increases stress.
>
> —WALTER

Apart from practicing lockpicking (see Figure 8-9), the second most important thing to master for competitions is controlling your nerves. A technique that works well is mental imagery: as you practice, imagine yourself picking a lock in a competition setting. Try to make your mental image as realistic and detailed as possible. Imagine yourself opening a lock while the clock is ticking. Picture what happens when time is almost up and the lock is still closed. Visualize others opening their locks while you keep cool. Such mental images will help you focus during a real competition and hopefully prevent you from deviating from the strategy you've envisioned.

Figure 8-9: Walter practicing before the Dutch competition at an outdoor hacker event, HAR2009, using a tension wrench and a hook

And, of course, the more competitions you attend, the better you'll perform under pressure. You might join a local lockpicking group and suggest or join impromptu competitions there. This is a good exercise that will create a similar tension. You could even do this via video chat, although being in a familiar environment might be less effective.

To reduce stress, keep your thoughts positive; even if you don't succeed this time, you'll gain valuable experience. If you notice negative thoughts forming, try to recognize them as such and dismiss them. Focus on your body before the clock starts. Relax your shoulders, neck, and face muscles. Breathe slowly and deliberately.

Spending time on the mental aspects of participating in a competition will help you perform better and is worth the effort. By competing as often as you can, you'll become more confident and relaxed with every competition.

The Competitions

At the time of writing, several lockpicking competitions take place around the world. In this section, we'll describe the best-known ones. Check the internet for up-to-date information if you want to participate.

Typically, competitions are held once every year, but the exact dates differ each year. It might cost some money to enter a competition, to cover the cost of the materials and prizes.

TOOOL US

TOOOL chapters host various competitions in the US. At the time of writing, the largest and most international competition is LockFest, which is typically held in Seattle in the spring. The organization often provides the locks, but occasionally contests are held using locks loaned by attendees. LockFest also holds competitions for impressioning, safe-lock manipulation (see Chapter 14), and timed head-to-head challenges (see Appendix A). You may find lockpicking events at hacking conferences too, like the lockpick village at DEF CON.

TOOOL Netherlands

TOOOL NL's first competition was the Dutch Open. As mentioned earlier in this chapter, this has since evolved into the three-day LockCon conference, of which the Dutch Open is just one part. The Dutch Open uses Euro profile cylinders and allows regular tools like hooks, rakes, and tension wrenches, as well as a vise (not that they're always needed; see Figure 8-10). As this is the most international lockpicking competition, we'll go through the details.

Figure 8-10: Walter at the Dutch competition in 2014 using just a hook—no tension wrench and no vise

In the first round, participants are randomly put in one of six groups. Organizers provide each participant with a lock and a five-minute time limit. The locks rotate within the group until everybody has tried to open each one. After successfully opening a lock, the contestant calls out their name, and a jury responds with the time. The contestant writes down their time, and at the end of the round, an organizer collects these pieces of paper and calculates which two contestants go through to the next round. These are the two competitors who opened the most locks from each group.

If more than two people tie in a group, those with the fastest total time go through. If a tie remains because more than two people have the same total time, the person with the fastest opening time of any lock will go through. The competition ends for the other contestants.

The 12 remaining contenders are then paired at random. Each pair gets two new locks of a higher difficulty level and a five-minute time limit. The person with the fastest time of each pair goes through to the semifinal round. The six semifinalists are again paired at random and given two new locks to open in five minutes each.

The three winners go through to the final round, in which each contestant receives a new, harder lock and has 15 minutes to open it. The locks rotate so that each contestant has a chance with all the locks. The number of openings or the total time will yield the winner and runners-up.

The Dutch competition typically uses new locks, provided by the organizers. The contestants get to keep the lock they're holding when the round ends, making participation even more worthwhile.

LockCon also includes other competitions, such as impressioning (see Chapter 11) and picking lever locks (see Chapter 17).

SSDeV, SPASS, and the ACZ

The German locksport organization SSDeV was the first group in the world to organize lockpicking competitions. Nowadays the group organizes four picking competitions: Euro profile cylinders, padlocks, freestyle, and *flash opening* (a quick round). The same setup is used by the Swiss locksport organization SPASS and by the ACZ in the Czech Republic. Sometimes all competitions are held in a multiday event, and other times only a subset of competitions is held.

In Germany, SSDeV holds a separate impressioning competition at another date and location.

Handöffnung for Euro Profile Cylinders

The *Handöffnung* (manual opening) competition uses Euro profile cylinders and allows only regular lockpicking tools and a vise. In this case, the organizers don't provide the locks; the contestants must bring their own.

In the first round, groups are formed randomly. Each contestant must pick the lock they brought with them within five minutes. If they fail, they (and their lock) are excluded from the competition; this rule prevents impossible locks from being brought into the competition. Locks are then passed around clockwise until each person has tried each lock, and everyone has 15 minutes to open it. Not opening another person's lock doesn't eliminate you from the competition.

Depending on the size of the group, the best two to four proceed to the A-final. In Handöffnung, the best is the person who takes the least amount of time; if you fail to open a lock, 15 minutes is added to your total. If you open the locks very fast, you might score better than someone who opens more locks. The two to four people scoring just below the A-final competitors proceed to the B-final.

The contenders in both the A- and B-finals proceed in parallel. Again, each lock needs to be attempted by all contestants, and the fastest total time determines the winner.

Because people can bring their own lock, it's in their interest to submit the most difficult lock they can still open within five minutes.

> I remember Meister Gerhard would always bring a particular lock that had a very deep pin after a very shallow pin, requiring a gonzo hook. Knowing that, he was able to quickly open the lock, but anyone unable to determine that this was the case would find it much more difficult. At one Swiss competition, I managed to open all locks except Gerhard's, so I placed second. For these competitions, it pays to find a lock with a difficult bitting or features like magnetic pins to keep others from opening it, although contestants also bring easy locks to give less experienced lockpickers a chance.
>
> —WALTER

Hangschlossöffnung for Padlocks

The *Hangschlossöffnung* (manual padlock opening) competition uses padlocks provided by the organizers. The rounds are similar in setup to the Handöffnung competition. Contestants get five minutes per lock. Vises are not allowed, nor are pick guns.

Freestyle

In freestyle competitions, organizers provide the locks. As a contestant, you're allowed to use any technique to open the lock that won't cause damage, including pick guns (although the organization typically provides locks that aren't easily opened using a pick gun). In Germany and Switzerland, the lock must be presented open and without any tools still inserted for it to count as being open. In the Czech Republic, no rule indicates that tools can't be left in the lock, which allows for impressioning as a way of opening.

Freestyle rounds are similar to those just described. You have five minutes per lock, and the fastest total time of all openings determines the winner.

Blitzöffnung

The *Blitzöffnung* (flash opening) competition is a fast knockout competition invented to create a spectator event and promote lockpicking. All contestants bring their own lock and must open it in under one minute; bringing a lock that's difficult to open is discouraged, as part of the aim is to get onlookers interested in the sport. If someone fails to open the lock, they leave the competition. If more than three contestants are left at the end of a round, another round follows in which the locks are exchanged. The last one to three people that remain standing are the winners.

> One of my first competitions was the Blitzöffnung contest held by SSDeV in 2003 during Chaos Communication Congress in Berlin. I was a fairly new beginner, standing amidst experienced German lockpickers. I opened my own lock in under a minute, so I advanced to the next round, and then the next, and the next. Everybody was very kind to a newbie like me, giving hints on how to open without me even asking. And I made it to the last three people standing!
>
> —WALTER

TOOOL Australia

At OzSecCon, TOOOL Australia holds a competition with locks provided by the organizers. The competition is set up as an ongoing event. Participants can try to open locks during the weekend OzSecCon is held, but you get only one try on each lock.

ACF France

The competition in France uses locks provided by the organizers. Several rounds are held, similar to the competitions described before. The ACF tends to select difficult locks, which may include dimple locks, for example. Some people, but not all, will speak English at the event. This competition is rather small.

Summary

In this chapter, you learned where to find and how to prepare for lockpicking competitions. We looked at best practices, as well as some details about the competitions that are held around the world.

If no lockpicking competition occurs in your neighborhood, consider setting up your own by following existing competitions as a blueprint. Lockpicking is a fun sport, and participating in competitions can be rewarding.

Next, we'll move on to Part III of the book, where you'll learn all about the technique of impressioning.

PART III

IMPRESSIONING

Impressioning is the method of creating a working key from a blank by reading marks made by the lock. In some scenarios, that's a *huge* advantage over regular lockpicking. Want to open a lock more than once without going through the whole picking process every time? Impressioning has you covered! Lost the key to a beautiful antique desk and don't want to damage it by taking it apart? Yep, impressioning can help with that too. In this part of the book, we'll cover this relatively new and novel way to dive into the game of locksport.

The History of Impressioning

Okay, "new and novel" isn't completely true. Impressioning was once a standard skill for locksmiths, but with the tools and technologies available to them today, those who have mastered it are the exception to the rule.

Within the locksport community, impressioning was virtually unknown until the 2007 release of the book *Impressioning* by Oliver Diederichsen, an excellent locksmith, safe technician, and highly regarded member of the locksport community. A small number of impressioning competitions had been held earlier than that (mainly by SSDeV), but the book's publication was a catalyst for most of today's competitors. With its technical explanations and, even more so, its multitude of pictures, this book made impressioning a staple of most locksport competitions throughout the world.

But how does it work, exactly?

How Impressioning Works

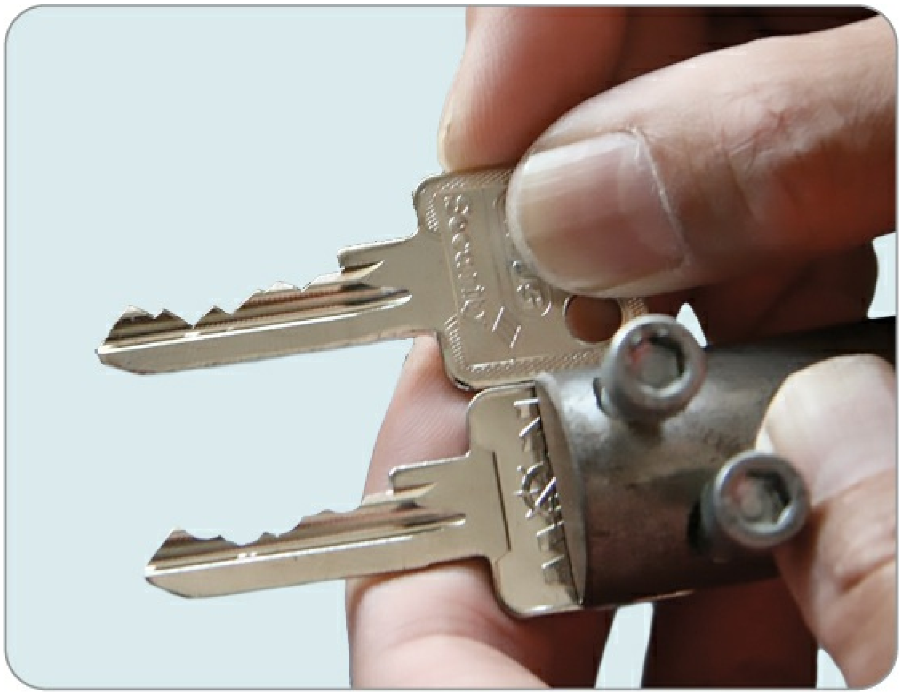
Impressioning starts with a key blank—full, uncut, and straight out of the box, as shown here.

When you turn a blank or incorrect key in a lock, the lock rotates slightly until one of the pins prevents the plug from turning farther, as you know from the element binding order principle. That pin will be caught between the plug and the housing, bound at a particular height. Without releasing the turning force on the key, you can jiggle it in an up-and-down motion so that it pushes all the pins that aren't binding, as shown here.

That lone, binding pin won't move freely; instead, it pushes back against the key blank, leaving a noticeable mark on it. You then use a file to remove material from the key in that spot. Once that's done, you insert the key again, move it up and down to push against the binding pin, and file off a little more material until the pin stops making marks at that position, meaning the bitting is at the right depth and will align that pin at the shear line when inserted.

If you repeat this process for every pin in the lock, the lock will open, and you'll have a working key. The following photo shows an impressioned key (bottom) compared to the original (top).

With those basics behind us, let's get into the specific tools you'll need and how to use them. Following that, in Chapter 10 we'll take a deeper dive into the impressioning process, and then in Chapter 11 you'll learn what goes on during impressioning competitions and ways to improve your chances at success.



9
IMPRESSIONING TOOLS

This chapter provides an overview of the tools you'll need to successfully impression a key: handles, files, vises, and key blanks. We'll cover what to get, what to avoid, and when it's okay to go for the cheapest option. We'll also mention a few tools that you won't need right away but can be helpful to have when you're competition ready.

Key Handles

One important piece of equipment for impressioning is the *key handle* (also referred to as a *key grip*, *impressioning handle*, or even just *impressioning tool*), shown in Figure 9-1. You use the handle to hold the key blank so you can turn it in the lock. To hold the key, most handles use screws that you can adjust with an Allen wrench.

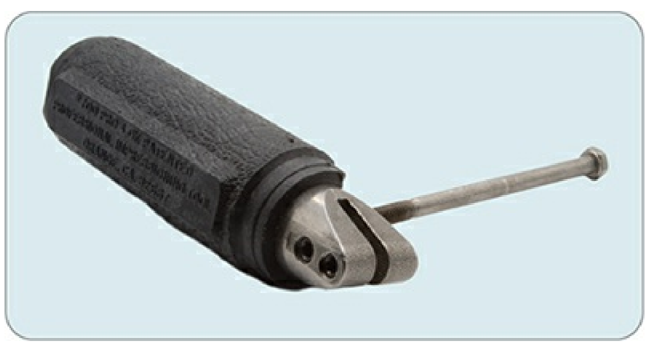


Figure 9-1: A Pro-Lok handle with a low-tech lever upgrade

Since people use keys with their bare hands every day, you might be wondering why you'd need a handle to hold and move the key in the lock. Technically, a handle isn't necessary, but in practice, you'll want one because it will protect your hands from metal shards and provide leverage for you to exert controlled levels of force on the key—way more force than what's considered "normal use."

During a workshop in Melbourne, a locksporter named Gracelyn was showing off her skills to another participant. She was fed up with using vise grips (understandably), so she was using her bare hands. I believe I've tried that myself *once*, and I wholeheartedly wouldn't recommend it (yes, Gracelyn is more badass than I am). The amount of force needed is such that you'll hurt yourself without a handle.

Impressioning involves dents in metal. Not the hardest metal, not the deepest dents, but still: Metal. Dents. Take proper precautions.

—JOS

Some handles have a lever on the side, perpendicular to the key. This gives you even more control over the amount of turning force on the key as you jiggle it up and down in the lock. Without the lever, you might use too little force, which won't make any impressioning marks, or too much, which will break off your key blank in the lock.

Unfortunately, most impressioning handles don't come with a lever, but often you can add one yourself. If you don't have access to a machine shop or hackerspace to modify your handle, you can use low-tech methods. For example, many handles have Allen screws mounted in the head, one of which you can replace with a longer screw to add a makeshift lever, as shown in Figure 9-1.

Mounting an Allen wrench in your handle behind the key will also work as a lever (Figure 9-2). Your handle won't be the nicest-looking one in the room, but who said hacks have to be pretty?

Figure 9-2: A Pro-Lok handle with an Allen wrench as a lever

You have a variety of options when it comes to handles: commercial handles used by locksmiths, custom-made handles sold within the locksport community, and tools made for other purposes that can act as a handle in a pinch. Let's look at examples of each.

Purpose-Built Handles

Whenever possible, we suggest using a handle designed for impressioning, rather than another tool that might do. Here we'll go over what to look for in a handle.

Handles that are light—made with materials such as aluminum, titanium, or plastic—greatly improve feedback and your ability to finely control your movements. More common materials can work as long as the handle is hollow so the grip remains light. The handle shouldn't be so thin that your hand cramps up after a while, or so thick so you can't feel accurate feedback. The most common technique is to use a handle with both hands, though if you prefer to hold your handle with one hand, you'll need a thinner handle so you can reach around it easily. Be sure to try out a handle before you buy it to make sure it's comfortable to hold.

While most handles rely on screws you adjust with an Allen wrench, some have fancy mechanisms designed to allow you to quickly change blanks. This can be useful, as the stresses put on key blanks during impressioning will occasionally cause them to break. However, instead of having one handle with a fancy quick-release system, in a competition setting we recommend having two or three handles on hand with preloaded blanks so you can easily move to the next one if your key snaps. This is a good reason not to go for expensive items.

> I hardly ever break keys while impressioning . . . except during competitions. This could be caused by the stress of competing, the use of less-familiar blanks, or the urge to use more force to get clearer marks. Whatever the reason, having multiple handles preloaded with keys and ready to go means much less time wasted removing a damaged key and getting a new one set up.
>
> —JOS

For beginners, we suggest starting with mass-produced handles. You can find reasonable-quality handles marketed to locksmiths (but sold to anyone) that aren't too expensive. Some common examples are Pro-Lok's Standard Impressioning Tool (our first choice, shown in Figure 9-3), Framon's Impressioning Tool, and HPC's Clean Grip Impressioning Tool.

Figure 9-3: The Pro-Lok Standard Impressioning Tool

Some commercial handle options are detrimentally overengineered. For example, foam- or rubber-coated grips, like those on the HPC handle shown in Figure 9-4, often cause you to clench your grip too hard and exert too much force on your key. Either avoid these or remove the foam.

Figure 9-4: An HPC Clean Grip with an ABUS key inserted

Similarly, the Framon has a quick-change mounting system that tends to come loose during the stress of competition, while the HPC's mounting system relies on the key blank having the keyring hole in the right place, restricting the keys you can use with it. In Figure 9-4, you can see that the ABUS key is set at a funny angle in the handle, because its keyring hole is offset to one side.

Simpler typically means *quicker*, and less opportunity for things to go wrong.

Custom Handles

Some locksporters are also locksmiths or machinists and have used their experience to design custom-made handles optimized for competition. These handles are usually tailored to the size of their hands and the length of their fingers.

Jord Knaap, a fantastic locksport competitor and Dutch safe technician, occasionally sells custom handles and other impressioning-related tools through his company, KJS Tools (*http://kjstools.com*), like the one shown in Figure 9-5.

Figure 9-5: A KJS Tools impressioning handle with lever, custom-made by Jord Knaap

Recently, Foxhole Security, run by well-known locksmith and locksporter RubberBanned, also began selling an impressioning handle (Figure 9-6). It has a detachable lever, which makes it portable and easy to pack. Like all custom tools, these handles are made in small batches, so plan ahead if you want to order one before a competition.

Figure 9-6: RubberBanned's custom impressioning handle

Other machinists in the community make custom tools, including handles, that are often sold only via word of mouth. If you want to get your hands on a custom-made handle, your best bet is to attend locksport conferences and competitions and befriend members of the community. Admiring the tool designer's craftsmanship not only is a great way to see what tools are out there, but also improves your chances of buying one.

Improvised Handles

Impressioning handles are somewhat rare tools, even among locksmiths. You can't just walk into a hardware store and find one on a shelf. Although all the supplies you need to start impressioning can be ordered online, you might want to try out impressioning with tools you already have before investing in dedicated tools. Here we'll go over some options you can use as an improvised impressioning handle.

Vise Grips

You can use a vise grip as an impressioning handle, although we wouldn't recommend it unreservedly. An unaltered vise grip has a slanted grip section that's not aligned straight with the key, so the movements of your hand won't stay within the same plane as the key. Part of the force you apply will torque the key in a way that increases stress on it, leading to breakage. Having said that, a vise grip is better than nothing in a pinch (see Figure 9-7).

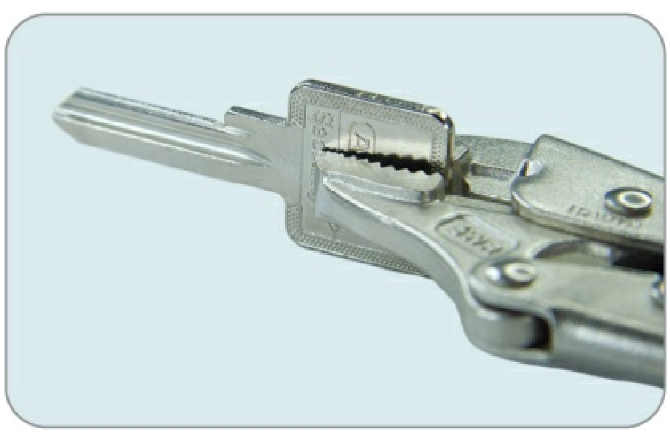


Figure 9-7: A vise grip with a key inserted in a conventional manner—which isn't the way to do it

One way to minimize stress on the key is to open the mouth of your vise grip wide and mount the key face up (make sure the grip is *very* tight, or it will slip), as shown in Figure 9-8. This way, the key will have minimal or no movement within the grip.

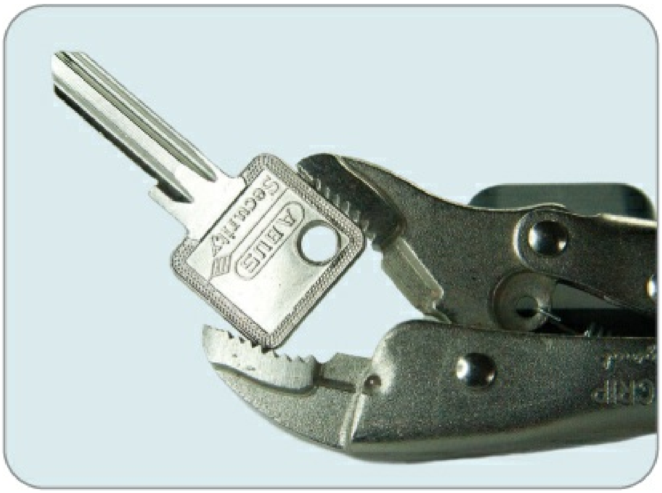


Figure 9-8: A vise grip with key inserted correctly

Hand Vises

Another option is using a hand vise, which is basically a handle with a small pair of vise jaws (Figure 9-9). Hand vises are inexpensive and can be found at many hardware stores.

Figure 9-9: A hand vise

Unfortunately, key blanks often work themselves loose during use, requiring frequent retightening. On some hand vises, you tighten the grip by tuning the backend, so when you use that part to apply torque in the other direction, you might be loosening your grip as well. That will definitely slow you down when competing. Again, stick to a purpose-built handle whenever possible.

DIY Handles

Finally, if you're handy, you could create your own handles. Competitions don't prohibit using handmade tools, and we've seen competitors bring all sorts of handles, from modified screwdriver handles to bent pieces of pipe with a slot and a bolt to hold the key in place (see Figure 9-10 for some examples). Be creative.

Figure 9-10: Examples of DIY handles by Jan-Willem Markus (images courtesy of the Blackbag blog)

One word of caution here: impressioning can be a difficult skill to learn when you're getting started. If you're using DIY tools and not seeing marks on your keys, you might want to switch to a dedicated, tried-and-tested tool before venturing into the homemade tool space.

Files

Now that we've covered some tools to help you make marks on key blanks, let's discuss the tools you'll use to take material off the blanks. The weapon of choice for shaping blanks into functional keys in sport impressioning is a *hand file*. Files are available in several cuts, forms, sizes, and price ranges. At the end of this section, we'll also discuss shortcuts, like using key-cutting machines.

Cuts

A file's *cut* describes the fineness of its teeth, and therefore how much material will be removed from the key with each stroke. A coarse file will eat away a lot of metal, while a smooth file won't do much more than polish the key's surface.

The coarseness of a file is measured in *Swiss cuts*, with #00 being the coarsest and #8 the finest. Most impressioners gravitate toward a #4 cut—enough coarseness to file off decent chunks of metal in a limited time, and not so much that you risk a lot of overfiling. For a beginner, we recommend sticking to that standard.

Shapes

Files come in a wide variety of shapes and profiles: squares, triangles, ovals, rounds, half rounds, tapered, rattails, pippins, and many more (see Figure 9-11).

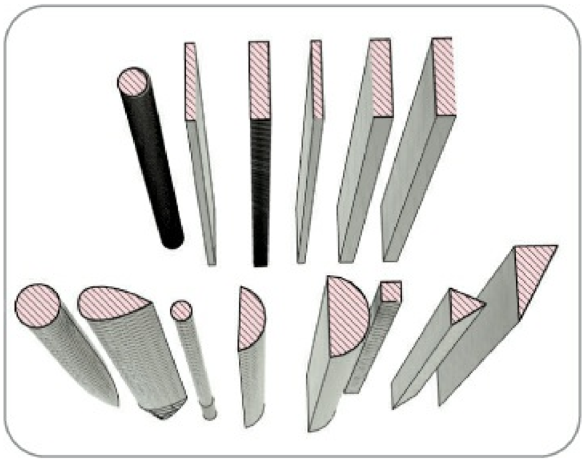


Figure 9-11: Various file profiles

Triangle files create cuts that closely resemble what we all think of when picturing a factory-cut key: V-shaped with nice diagonal edges. These triangle cuts can be a problem, because a mark left by a pin in a narrow valley like this will be hard to see. It's easier to see the marks in U-shaped cuts that resemble a sine wave.

To give your cut a smoothly sloping bottom, you'll need a file with a roundish form. Besides the obvious round files, any oval shape will also do. A round shape works well for speed impressioning because all the sides are exactly the same, so you should never need to reposition the file before starting to remove material. Besides gaining several split seconds, you remove the possibility of ruining a key by using the wrong file side (though plenty of other methods remain to ruin your keys!).

NOTE

If you're thinking that a key made with a round file would bear no resemblance to a factory-cut key with its sharp lines, you'd be correct. However, locks don't care what the key looks like, as long as it fits in the keyway and each pin stack ends up at the correct height. A round cut can accomplish this just as well as a triangle cut.

A *pippin* file has two different sides: one rounded and the other pointier. The cross-sectional view looks like a raindrop. This unique form makes the pippin a jack-of-all-trades; its flat side can be used as a small flat file, the pointy bit can mimic a triangle file, and its round side can be used as a round file. Carrying one single file has merit when you're working in the field, but as we're focused on the sport side of things, speed is the only factor that counts.

Sizes

Ideally, your file's width should be no smaller than the width of the required cut. Too thin of a file could create a cut with almost vertical sides that pins can't travel over, meaning your key could get stuck in the lock. Too wide of a file will cause a cut to *spill over* into an adjacent cut, inadvertently taking off material you didn't want to remove. Figure 9-12 shows various file sizes.

Figure 9-12: Various file sizes

If you buy just one file, you can't go wrong with a Grobet brand, #4 Swiss cut file, 6 inches long and a quarter-inch in diameter.

EXPERT OPINION: CHOOSING A FILE

Holly Poer, an excellent impressioning teacher, said this on a specialist lockpicking web forum: "Generally speaking, a standard 6-inch-long Grobet brand file with a Swiss cut is the preferred file for cutting keys, because it makes a cut wide enough for a pin tumbler. Locksmiths tend to use the pippin shape, while others also use the round. Some even use a half round, but I don't recommend this until you have had a lot of practice filing. An 8-inch-long file has a larger diameter and makes a wider cut. There are times when this is really useful. A file smaller than 6 inches would be needlessly time-consuming."

Invest in a proper file and take care of it. Your file should remove a consistent amount of metal with every stroke so that you have full control over the cut. Keeping your file in good condition is crucial, because damaged teeth can make the file unpredictable. If you treat your file right, it'll last years.

> I tend to carry several files in my standard kit: a big flat file (used occasionally for slimming down key heads), a small half round (mainly for sentimental reasons), and two sizes of round files. The first two almost never get used, and the big round one only comes into play once in a while when the sides of my cuts are becoming too steep. Size matters. Don't believe otherwise.
>
> My main file was gifted to me more than a decade ago. I can't even count the

number of keys I've cut with it, and it still feels like new.

For a video of me impressioning, check out "Jos Weyers Final Round 2010 SSDeV Impression Championships" at *https://youtu.be/Bj9KEmLWRek*.

—JOS

When shopping online for files, note that some manufacturers include the section within the handle as part of the file's overall length, which can be a little misleading. This section is called the *tang*; see Figure 9-13.

Also note that most high-quality files don't come standard with a handle. You usually need to add those to your order separately.

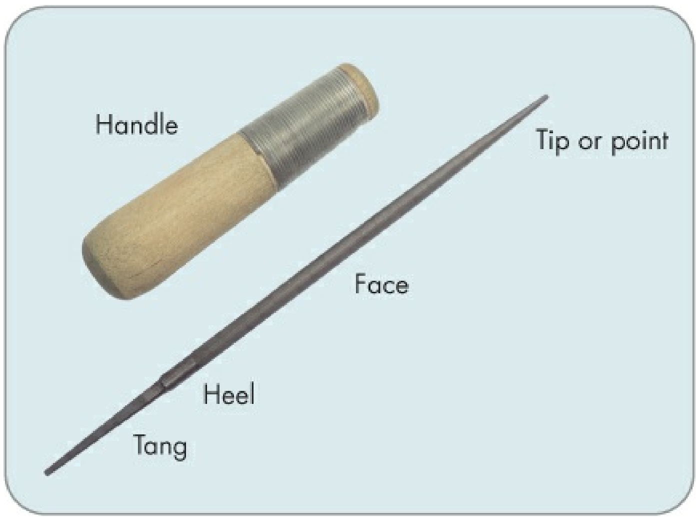


Figure 9-13: Anatomy of a hand file

Key-Cutting Machines

Key-cutting machines aren't allowed during competition (and probably wouldn't beat a hand file anyway), but if you're not yet terribly sure about your depths or spacings and want to practice recognizing marks, you could use a (professional) cutting machine to make your cuts. It's probably best not to use a standard V-shaped cutting wheel, which would present the same problems described earlier: a sharply V-shaped valley can be a tricky hunting ground for key marks. A standard Kwikset key cut has a wide, flat bottom, so if you happen to have a cutting machine capable of producing one of those, you should be good to go.

Handheld key cutters—small, cheap gizmos that can nibble just enough metal off your key blank to deepen your cut one extra depth—kind of work, but they tend to put considerable stress on your key, even distorting it most of the time. Check the rules to see whether they're allowed in specific competitions. Otherwise, they can be useful simply to help you hone your mark-recognition skills while at your own workbench.

Magnification

The marks you'll be hunting for will mostly be small and subtle, so you'll need some type of *magnification aid*. You might be tempted to get the strongest magnification tool to better see the marks. While "moar is better" is something we're usually totally on board with, in the case of magnification, hold off buying an electron microscope for now.

Yes, strong magnification will enable you to see everything, but that might end up being your downfall: under enough magnification, everything starts to look like a mark. Positioning the part of the key you want to see also takes longer under high magnification.

A magnification aid that allows you to see two or three cuts at the same time will probably be the most useful during a competition. Being able to see your marks in the context of other marks is helpful. Also consider a cheap hobby light with a built-in loupe, like Jos's in Figure 9-14. It's effective without breaking the bank.

> This hobby light with an integrated magnifier was probably 20 euros (about $20) when new, but was gifted to me about 15 years ago (the several layers of duct tape and chopsticks holding it together are evidence of all the years of abuse it has taken).
>
> —JOS

Figure 9-14: Jos's magnification light source in better days (left) and after years of abuse (right)

As a backup, you could try an aftermarket accessory that places a magnifying loupe on the working end of a Maglite flashlight (Figure 9-15). This accessory was originally used by geologists to look at tiny rocks. Later, some smart guys slit a groove in the bottom, and voilà: dedicated key-impressioning gear (which is now how it's marketed). This is a useful gadget when you want to be mobile. Simply search online for *key impressioning magnifier*.

Figure 9-15: A Maglite add-on loupe

When shopping for a magnification aid, visit a locksport meeting or brick-and-mortar stores that might carry them, such as hardware or jewelry shops, to look through a few options before you decide what to buy. Don't forget to bring keys.

Lights

If you search online for *impressioning light*, you'll find some fancy-looking options in some of your hits, such as lightboxes with multiple light sources and a lens conveniently packed into one handy portable form factor. These are mainly marketed to covert entry teams and are expensive. Some also have clear design problems, like crumbling rubber parts and lenses you can't adjust, indicating that actual impressionists probably weren't involved in their design. Some people might prefer such tools, but lights don't need to be fancy. For example, the Maglite loupe add-on shown in Figure 9-15 sports a light, and while it's not an ideal primary light, it's a good backup to have on hand.

Head-mounted gear seems to be popular in lockpicking stores. One of the drawbacks of head-mounted lights is that you can't look toward another competitor without blinding them. As eyesight is important in this sport, blinding would be an unsporting thing to do, no matter how unintentional. You can also end up blinding yourself, so make sure your light source is dimmable or not too bright. Some shiny marks will turn into tiny suns when you put an excessive number of lumens on them, usually making them the last marks you'll see in that round of impressioning.

> Of course, I bought a head-mounted set, as you can't be sure what you (don't) like before you give it a spin. I can honestly state that I hate it. I have, however, seen one or two rather competent impressioners use them during competitions, so opinions apparently vary.
>
> —JOS

Some people have experimented with different sorts of light to increase the visibility of marks, such as ultraviolet (UV) light or red-tinted light, but regular white light usually works just fine. Others have tried painting their key blanks with UV-reactive paint and then using UV lights, but the paint tends to rub off in the lock, leaving both the lock and the key a mess. Since locks are passed round-robin between competitors, most competitions ban the use of such additives.

Power

Your light source requires some kind of power source, so make sure you prepare for that in a competition. If the light is battery powered, pack extra batteries. Bringing them along is wiser than hoping you'll find a store near the event.

Most lights, though, plug into an outlet. If you plan to compete internationally, this will require some preplanning. Countries have not only different outlet shapes but also different voltages. A US-purchased lamp that expects 120 V at 60 Hz but encounters 230 V at 50 Hz in Europe might be rather upset and show its displeasure with sparks, smoke, and flames. Make sure you pack an international adapter that not only accounts for plug shapes but also converts voltages.

> My trusty abused and repaired hobby light accompanied me on one of my first lockpicking trips to the US, but when I plugged it in, it didn't light up, and I assumed it was broken during transit. Just before tossing it into a trash can, I was reminded of the peculiar voltage levels the power outlets in this part of the world supply. So, though I did have to source a new light for my onstage demo, my trusted light survived and was packed for the return flight to Europe. The lesson here is you might need more adapters than those you take when traveling casually. (Yes, I was green.)
>
> —JOS

While competition organizers will often make sure the venue has outlets available, those outlets might not be ideally situated. To complicate matters, hobby lights often have rather short cords, which might force you to sit in an uncomfortable spot. If possible, pack an extension cord or power strip so that *you*, not your lamp, can decide where you sit. No need to go crazy here; a 3 m or 4 m cord is probably sufficient.

Vises

We've already covered how to keep a sturdy grip on your key, so now we need to look at the other end of this tug of war: the lock. The jiggling force you put on your key will end up rocking your lock. When it's mounted in a door, this won't be a problem, but most competitions don't use actual doors (the lockpicking community has to answer enough questions about burglary as it is without supplying such visuals). Therefore, you need a way to steady the lock: a vise. Unfortunately, *not any vise will do*; spotting the less seasoned contenders in an impressioning match becomes easy when locks start slipping out of jaws and bench vises start moving tables or coming loose from them.

Here's some general advice on how to choose. Don't bring a vise you haven't used before. Make sure your vise can handle the type of lock you're tackling (Euro profile cylinder, KIK cylinder, padlock, and so on). Make sure the vise will fit and stay solidly connected to your table. Pick a vise that's relatively light: the heaviest table vise in the shop will keep the table more stable, but getting it to the competition venue will be a struggle.

> Some international folks have competed several times on my continent, which gained my local hackerspace a decent selection of inexpensive table vises. Paying those overweight luggage fees is less fun when you have to pay them again on the flight home (thanks, Matt!).
>
> —JOS

Some competitors have started 3D printing lock holders that can be secured to a table with a clamp. This can be a good solution to reduce the weight of your bag, but requires you to know the exact type of locks that will be used in competition; a holder printed for Euro profile cylinders will be useless for a KIK cylinder. Also, if you use 3D-printed lock holders, make sure they're printed with enough plastic (*infill* in 3D printer lingo) that they won't crumble when you clamp them to the table or put force on the lock.

Another solution is a pair of Manfrotto 035 Super Clamps, which are typically used in theaters to rig light fixtures and such. They are light, grip well, can swivel rather easily, and look pretty cool. Two Super Clamps can be connected by using a Manfrotto 061 joining stud, which lets you use the bottom clamp to attach to your table and the top clamp to hold a lock. Manfrotto gear can be purchased from most camera supply shops.

Figure 9-16 shows a Euro profile cylinder mounted in this Manfrotto setup. Keep in mind that clamps and vises can leave marks on the host's tables, so it's considerate to bring some kind of padding like cardboard or rubber to avoid this.

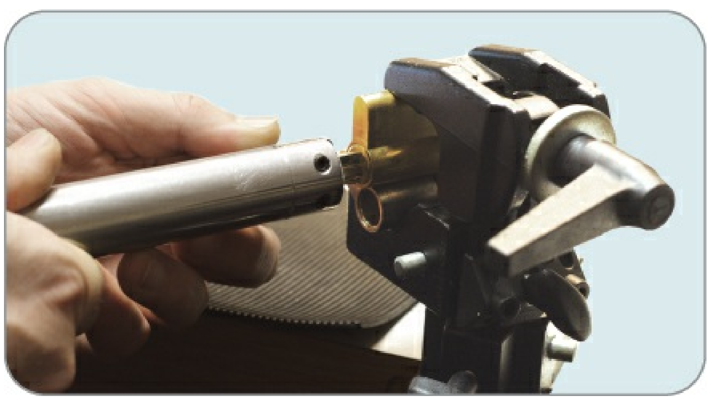


Figure 9-16: Manfrotto Super Clamps (image courtesy of Dennis van Zuijlekom)

Notice that below the lock is the empty shell of a Euro profile cylinder. The shape of the shell lets the Manfrotto get a better grip on the lock being impressioned. If you try this yourself, be sure to use an empty shell and not a complete lock cylinder so that you don't get confused about which lock you're impressioning.

If you plan to participate in lockpicking competitions as well as impressioning competitions, check out Chapter 7 for advice on using vises for lockpicking.

Workbenches

Most competitions provide tables for competitors to use. Depending on the event venue, these can vary from hotel dining tables to large, industrial workbenches. Larger tables are often shared by two to eight competitors at a time. This variation presents a couple of potential issues. First, your vise or clamp will need to be able to accommodate a range of table thicknesses. Second, the table will likely vibrate or wobble while you're working as others seated near you furiously jiggle their keys.

Rather than deal with these problems, consider bringing your own small, portable, folding workbench like the one shown in Figure 9-17. These can be purchased fairly inexpensively at most hardware stores, so if you're traveling for a competition, you can often buy one after you arrive. If you make friends with local competitors, you might even be able to bribe them into storing it for you until next year's competition too.

Figure 9-17: One of Jos's inexpensive folding workbenches (and Dita)

With your own bench, you know exactly what you're working with, and you can set up exactly the way you want with no distracting tablemates.

Depth-Measuring Tools

Overfiling—taking off too much material from the key—is really, really bad; if you overshoot the correct depth by even a little, the lock won't open, but the key will trick you by continuing to mark at this position. In the end, you'll have filed the key until it splits in two. One way to avoid overfiling is to take off *very* little material between each key insertion. However, doing so greatly increases the number of times you have to repeat the key-jiggling process, which not only slows your opening time considerably but also adds more stress to the key, which can cause it to break.

The ideal approach is to take off exactly the amount of material to get to the next possible cut depth. Key depths tend to be measured at certain points, so a depth of 2 is generally standardized across keys for that manufacturer (but not necessarily across manufacturers). If you know the brand of the lock you're trying to open, you may be able to find these cut depths online or in reference books. If you don't have access to these resources, you can build depth charts by measuring existing keys to similar locks and filling in the blanks. If you know how deep a 2, 3, and 5 cut are, you can probably figure out what 1, 4, 6, 7, and so forth are supposed to be. If the lock is completely unknown and no other comparable keys are available, you can use the keys from successful openings as a reference.

If you know the brand you'll be competing on, calibrate your filing so you're taking off the same amount of material with each swipe of the file. Once you know how much material you remove, you'll know how many swipes is one cut depth for a given brand of lock—for example, "I need four file swipes to get me down one possible depth on an ABUS." It doesn't matter if that number is 2 or 20, as long as it's consistent and precise. Mastering the skill of determining exactly how much to file to go one cut deeper minimizes the work needed to form a working key and greatly enhances your chances of winning competitions.

Calipers

Calipers are a great tool for measuring cuts accurately. Calipers with round dials are easier to position and read than vernier calipers (a style that looks like a slide ruler). To make the process even easier, you can mark some of your dials with lines to indicate the possible depth levels for locks you regularly encounter (see Figure 9-18). Then you don't even have to know the depth you've reached, but just that you need to get to the next line!

Figure 9-18: Kroeplin calipers with marker lines added to the dial for quick reference of ABUS cut depths

Kroeplin calipers are recommended, but any brand will do. When shopping, look at the shape of the jaws; the part that goes into the cut shouldn't be too flat or wide, or it won't reach the bottom of your cut. Look for a *pin-shaped* caliper.

Key Gauges

A *key depth gauge*, or *key gauge*, is another tool for measuring cuts. These gauges are flat pieces of metal with holes that match certain cut depths, allowing you to slide in a key to determine the cut depth of any position on it. Your key gauge needs to match the brand of lock you're impressioning, which means you'll need to carry several gauges. Some gauges do include measurements for multiple brands, as is the case in Figure 9-19, though we've yet to see one gauge with slots for the all most common impressioning contest brands: ABUS, Schlage, and Lockwood.

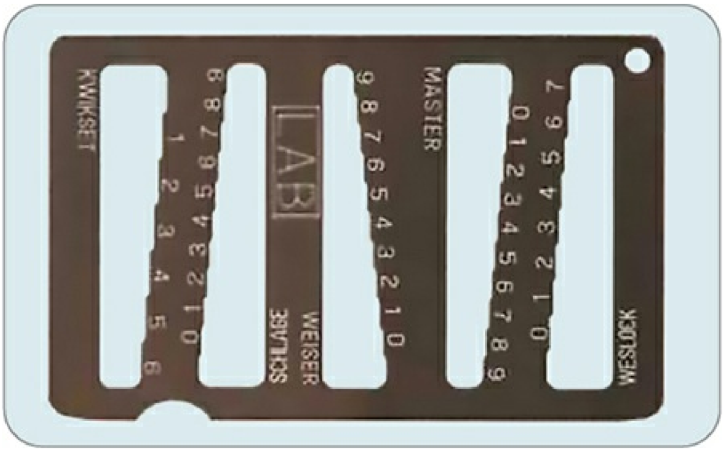


Figure 9-19: A key depth decoder for several brands of locks

Unfortunately, because most key gauges are made of metal, they can scratch your key and create misleading marks. They do work, so if you're in a pinch, try them out. While some are made of material that is softer than metal (less prone to scratching), they're not easy to find. One annual LockCon conference had a handy printed circuit board (PCB) version of an ABUS depth gauge as a conference badge (Figure 9-20).

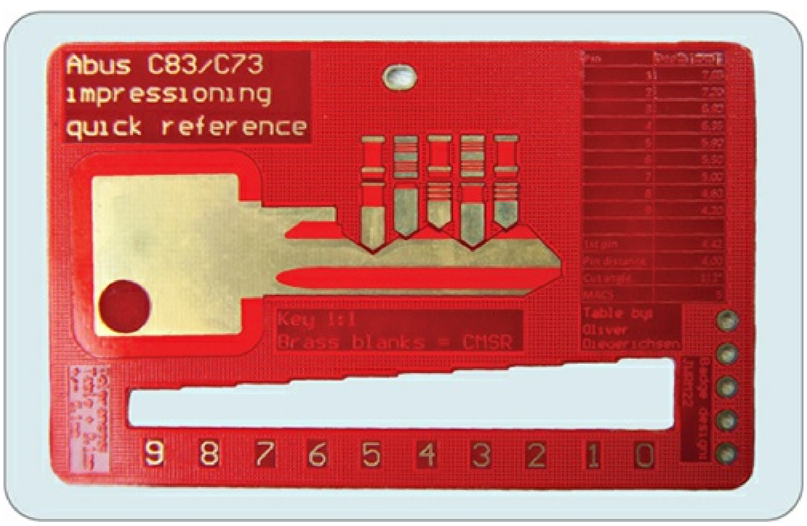


Figure 9-20: A key gauge integrated in a LockCon conference badge (excellently designed by Jan-Willem Markus)

Space-Measuring Tools

You need to know not only how deep to make the cuts, but also where they're supposed to go along the edge of the key. While the pins in the lock leave subtle marks telling you where to file, some guidance about where to look for those can be helpful.

One option is to simply use an empty plug from the same brand of lock you're impressioning. (If you took apart a lock to get the empty shell to use with a Manfrotto clamp, you should have a spare plug already!) In Chapter 10, we'll explain how to file down part of the plug to facilitate its use as a measurement tool, but just having one on hand is a good first step.

Other ways to check the spacing of a key might be to 3D print guides with notches to show the correct spacing. You could also compare a precut factory key to your key blank to see where the cuts go. However, to line up the factory key with your blank would require removing your blank from the handle, which would be rather time-consuming in a competition setting.

If you want to get really fancy, the spacing tool from KJS Tools can make your filing life much easier. The one shown in Figure 9-21 is another custom creation from Jord Knaap.

Figure 9-21: The KJS Tools spacing tool

In essence, the KJS spacing tool is a lock cylinder that has all its pins replaced with hard, drill bit–like material. Some parts of the core are removed to enable it to spin even if the bits don't align to the shear line. When you put a key blank into the tool and gently turn it, the drill bits press into the key, producing obvious markings on its side. You can see two of the marks in Figure 9-22. Because these drill bits sit in the exact spot where the pins used to be, the markings they produce tell you exactly where to make your first cuts.

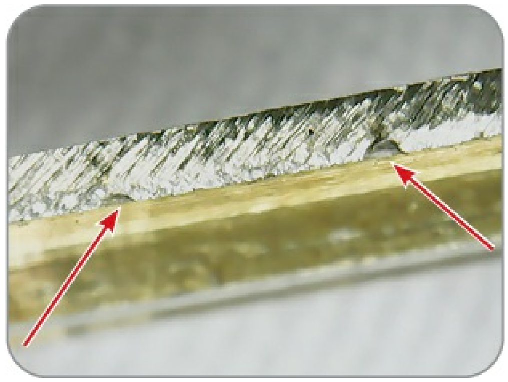


Figure 9-22: Two marks on a key blank created by the KJS spacing tool

The downside is that you need a spacing tool that precisely matches the lock you're going to be opening. If you don't know ahead of time which lock the competition will use, you'll need a wide range of these tools.

Locks and Blanks

Now that you've seen the basic gear, you need some locks and blank keys to start practicing with. If you know the kind of lock that will be used in a competition, you can buy a similar lock to practice on. If you don't know which lock is being used, it's worth practicing on common locks used in the part of the world where the competition is being held.

Currently, the standard locks for impressioning competitions are Schlage in the Americas, ABUS in Europe, and Lockwood in Australasia. Competition organizers often try to pick a brand that is readily obtainable for the potential participants.

> One year, SSDeV mailed boxes of blanks free of charge to anyone who wanted to train so as to "win back the German title from the Dutch." This might sound a bit unsportsmanlike, but they also shipped those boxes to us Dutchies, so the bravado was clearly just for show (thanks again, Steffen!).
>
> —JOS

Keys can be made from various kinds of metal. The softer the metal, the easier it will be for a pin to leave marks, but that doesn't mean you should aim to get the softest keys available. Because you'll be introducing keys to forces that are considerably greater than what they're designed for, breakage is definitely possible. On the other hand, very hard keys will probably never break but will be harder to impress on. We don't recommend steel blanks. Aluminum (and variations thereof) often clogs up your file and tends to be brittle and break without warning. A brass key will get a subtle crack near the bow before breaking, warning you to ease off the heavy handling, so we recommend you always try to go for brass. If it seems unobtainable, ask the competition organizers where they sourced their stock.

You'll burn through a serious number of blanks during practice, so make sure you order plenty. eBay can be your friend, but pay attention to what you actually order; *stahl* is

German for *steel*, which is not what you want.

Befriending a local locksmith or key-copying shop can also be helpful to get boxes of blanks for close to cost. Again, make sure you order what you actually want; sometimes key-copying shops get their supplies through a centralized source that can change your order on a whim. Notably, key-copying shops often use blanks that are a bit thinner than standard stock. For a conventional customer, this makes little to no difference, as the blank will fit in more types of locks (which is why they're called *universal* blanks). If you're training with these, however, your calibration could be way off.

Brand-name blanks are usually more robust than generic ones and are less likely to break, but they typically cost more (sometimes quite a bit more) than the generic ones. When ordering blanks from a company you haven't used before, it's a good idea to get just a few and see how they perform before buying a big box. Some of the generic ones work well enough, but others are so soft they start cracking and bending right away.

Other Accessories

We've gone over all the critical (and some optional) items that you'll need for impressioning. However, a few other small, common items are useful to have with you. First, make sure your kit includes a pen and paper. You'll need these for recording your times during competitions or when you practice. Second, pack a Sharpie or similar permanent marker (red is a good choice) to mark pin spacings on your key blanks. Finally, add a new, soft toothbrush to your gear for brushing away metal filings from your key without scratching its surface.

If you've managed to collect all the gear we've discussed, you probably have quite a big pile of items at your feet. Now the question becomes how to get it to a competition venue. Since competitions happen all over the world, you'll probably want to pack your gear into a travel-friendly container. Many competitive impressioners have found that Pelican brand cases are well suited for this task. They're expensive but typically contain foam inserts that can be cut to the shape of your tools, so they do an excellent job of protecting your gear. Some Pelican cases have wheels and pull-out handles like standard luggage, which saves your arms for competition.

Summary

This chapter has described the basic components of an impressioning kit and given you advice on which tools to buy and which ones you can skip. Appendix B lists some reputable sources for the tools described here and elsewhere in the book.

This chapter was all about the basic list, but a lot of other gear *can* be useful. We'll cover this extra gear in the next chapter, when we go through the impressioning process step-by-step.

10
IMPRESSIONING STEP-BY-STEP

To successfully impression a key blank into a working key, you need to perfect your skills at reading the tiny, subtle marks left by the binding pins in the lock. Then the challenge is to carefully file away at those marks until you have a key that aligns the pins, allowing the cylinder to rotate and the lock to open. In this chapter, we'll go over these techniques in detail as we walk you through the impressioning process.

We'll begin with an ABUS C83 lock and then repeat the steps on a Schlage lock to show you how different locks leave behind different marks. Finally, we'll share other tips and tricks that can help you master this process. Before we start impressioning a key, though, we need to set up our blanks and gear.

Setting Up Your Gear

Predictability and repeatability are key (pun intended) in impressioning, and a well-organized workspace can help maintain that consistency. This section outlines the steps you'll follow to prepare for impressioning in both a practice and competition setting.

NOTE

In competitions, you'll have some time to prepare your equipment before the clock starts. This is when you should set up your vise, key handle, light source, and the rest of your gear as the rules permit. Bring as much of your own gear as possible to keep your setup consistent. We'll talk more about what to pack for competitions in Chapter 11.

Mount the Lock

Mount your lock in a sturdy manner, oriented either American style (with the pins above the core, pointing down) or European style (with pins pointing up). Your vise might be more suited to one of these orientations, so go for whichever is the more stable option.

Mount the Key in the Handle

Also aim for stability when mounting your key in the handle; if your key slips, it won't receive all the force you exert on the handle. That slipping not only is nonoptimal when every second counts, but also means you're more likely to cause damage. Make sure your handle is tight enough on the key blank that it can't move. If it's loose, you'll have less control over the depth and angle of your cuts.

Prepare the Key

Before you begin making marks and filing the key, you can take a few steps to make the impressioning process more efficient. Note, however, that in most competitions, you're not allowed to do anything to the key, besides mounting it, until the clock starts. Always make sure you know the local rules beforehand, and listen when the organizing body goes over them.

Predicting Pin Spacing

Pins are spaced at predetermined positions within a lock, but those distances differ across brands. Because pins are pointed and don't have much wiggle room, you can predict the possible spots at which they can touch a key (and thus where you should hunt for marks and start making your cuts). Table 10-1 shows some pin spacings, measured from the key's *shoulder* (where the bow meets the blade), for common competition brands. Note that the sixth pin often isn't used in competitions.

Table 10-1: Spacings for Common Lock Brands

	ABUS	Schlage	Lockwood
Pin 1 (nearest to bow)	4.42 mm (0.174 inches)	5.87 mm (0.231 inches)	6.10 mm (0.240 inches)
Pin 2	8.42 mm (0.331 inches)	9.83 mm (0.387 inches)	10.07 mm (0.400 inches)
Pin 3	12.42 mm (0.489 inches)	13.79 mm (0.543 inches)	14.04 mm (0.550 inches)
Pin 4	16.42 mm (0.646 inches)	17.75 mm (0.699 inches)	18.01 mm (0.710 inches)
Pin 5	20.42 mm (0.804 inches)	21.72 mm (0.855 inches)	21.98 mm (0.870 inches)
Pin 6	—	25.68 mm (1.011 inches)	—

These measurements represent the placement of pins along the length of the key, not the cut depths. We'll cover depths shortly.

Filing the Key's Surface

Most key blanks fresh out of the box have a surface that impedes the visibility of marks. This occurs for two main reasons.

First, most keys come with a chrome coating that protects them from corrosion, dents, and the like. Chromium is harder than brass, so making good marks on the keys will be easier after that coating is removed.

Second, even if a key isn't coated, the surface will probably be quite rough (see Figure 10-1). Up close it resembles a lunar surface—not an optimal hunting ground for marks.

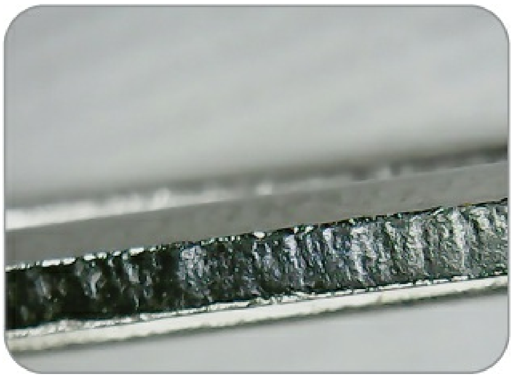


Figure 10-1: An unprepped key (fresh out of the box)

You can mitigate this by gently filing strokes across the entire surface of the key's edge that will have contact with the pins. Notice in Figure 10-2 that the surface of a semiprepped key is by no means flat but *is* consistent, and that consistency will help you see marks. We recommend using a flat file for this step, but a round file will also do.

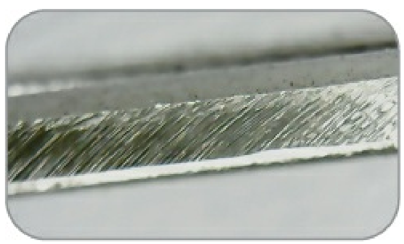


Figure 10-2: On this semiprepped (dechromed) key, notice that the file strokes are at 45°, which makes marks at 0° or 90° easier to find.

NOTE

Chrome can be flaky, literally. These metal flakes or shavings are extremely thin and can easily become embedded in your skin. They can become irritating really fast and shouldn't be left untreated, or you risk infection. As you file off the key's protective coating, use a soft toothbrush to remove these flakes before they have the chance to contact your hands. Safety third is not an option.

A good trick to check your spacing at this point is to put the dechromed key in the lock and, with almost no force, turn it left and right a couple dozen times. You're not trying to bind the pins yet, just letting them ride over the key, so don't apply any jiggling motion. When you remove your key, you may notice spots where the pins gave it a little polish (see Figure 10-3). Hello, spacings! Since the pins are spaced evenly throughout the lock, even if one or two of these polish marks are missing, you can extrapolate their location based on the others.

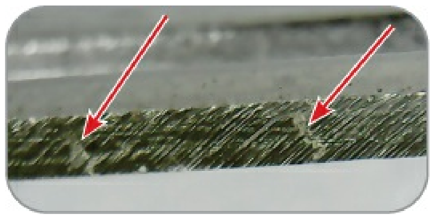


Figure 10-3: Finding spacings by using the polishing technique

Now use a fine-tip Sharpie to draw lines on the side of your blank indicating where the pins are supposed to touch (Figure 10-4). Doing this will enable you to instantly verify your file positioning throughout the whole impressioning process.

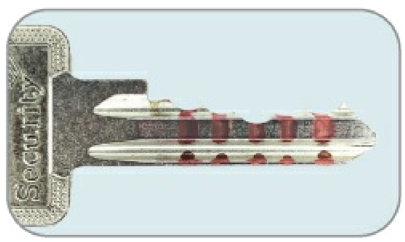


Figure 10-4: A half-cut key with spacing help lines still visible

Cutting a 11111 Key

If you already know the spacings of the brand of lock you're impressioning, you can turn your key into a *11111 depth* key—one with cuts to the shallowest official depth at all possible pin positions—before you even put it in the lock. This way, when you put the key in the lock to mark it, you know to look for marks in the premade cuts, making mark hunting much easier (see Figure 10-5).

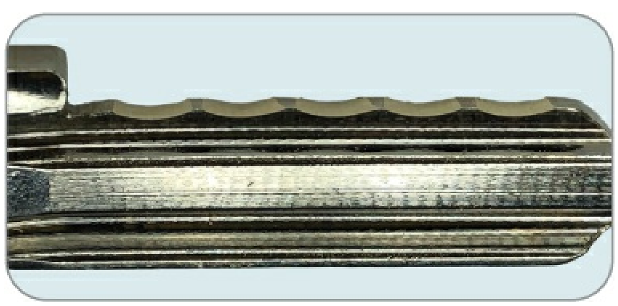


Figure 10-5: The clean workspace of a 11111 key

In this case, you don't have to file off the chromium coating (although you can). Leaving small spots of chrome between the cuts won't influence the rest of the process much.

Key manufacturers tend to have standardized depths for each cut level, so filing to those known depths eliminates a lot of guesswork, translating to faster opening times. Table 10-2 shows cut depths for lock brands that are often used in impressioning competitions. Note that the depth levels (1, 2, 3, and so on) represent how tall that section of the key is after it's filed to that depth. In other words, a 1 cut—the shallowest cut—has the highest measurement, since most of the key blank remains.

Table 10-2: Cut Depths for Lock Brands Commonly Used in Impressioning Competitions

	ABUS	Schlage	Lockwood
1	7.70 mm (0.303 inches)	8.13 mm (0.320 inches)	8.20 mm (0.323 inches)
2	7.25 mm (0.285 inches)	7.75 mm (0.305 inches)	7.75 mm (0.305 inches)
3	6.85 mm (0.270 inches)	7.37 mm (0.290 inches)	7.40 mm (0.291 inches)
4	6.40 mm (0.251 inches)	6.99 mm (0.275 inches)	7.00 mm (0.276 inches)
5	5.95 mm (0.234 inches)	6.60 mm (0.260 inches)	6.63 mm (0.261 inches)
6	5.50 mm (0.217 inches)	6.22 mm (0.245 inches)	6.24 mm (0.246 inches)
7	5.10 mm (0.201 inches)	5.84 mm (0.230 inches)	5.90 mm (0.232 inches)
8	4.65 mm (0.183 inches)	5.46 mm (0.215 inches)	5.50 mm (0.217 inches)
9	4.20 mm (0.165 inches)	5.08 mm (0.200 inches)	5.11 mm (0.201 inches)

NOTE

If you search these depth charts online, you might find versions that include cut depths labeled 0. Zero cuts *(either no cut at all, or one level shallower than 1) do exist in some locks. However, zero cuts are mainly reserved for master-key systems, which shouldn't be used in impressioning competitions, so we've skipped them in the table.*

Starting off with a proper 11111 key can make your impressioning go much faster. Try not to rush this step. Any advantage you gain at this stage by rushing will probably be lost a few times over before you open the lock, so checking the depth and spacings of your 11111 cuts is worthwhile before continuing with the rest of the process. If the measurements seem inaccurate, you can always ditch that key and start on a new one.

> As we were writing this book, Walter came up with a remarkably easy way to check the correctness of a 11111 key: just try it in a lock keyed to that bitting. If it's correct, the lock will open smoothly. I can't think of a faster way to check a key, so now I need to rekey some locks (and I can't believe I hadn't thought of this myself!).

—JOS

For the examples in this chapter, we cut a 11111 key before beginning the impressioning process and marked the spacing with the KJS spacing tool mentioned in Chapter 9.

Impressioning Road Map

With the preparation done, now it's time to see impressioning in action. As mentioned, we'll start with the ABUS C83 as an example, but the skills and techniques here are adaptable. You'll be following these steps:

1. Insert your key fully into the lock.
2. Jiggle the key by using both hands (one to turn, one to jiggle) in an up-and-down, rocking motion a few times.
3. Remove the key and inspect the surface for a mark that's clearer than any other mark. This should be the mark left by the binding pin.
4. Holding your file handle closest to the file blade, use a few strokes to take off just a little material at the marked position on the key. Make sure to hold your file at a 90° angle to the key so both sides of the cut are equal (see Figure 10-6).
5. Check the surface of the cut. You want it to be as smooth as possible so you can easily recognize marks when you reinsert the key. If it's rough, give it a single, gentle swipe of the file.
6. Reinsert the key and start over at step 1.

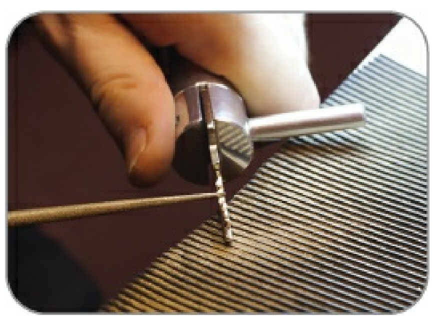


Figure 10-6: Filing at a 90° angle to the key

When you file, you want to take the cut down to the next depth level. Note that the key's width can change at certain depths (see Figure 10-7).

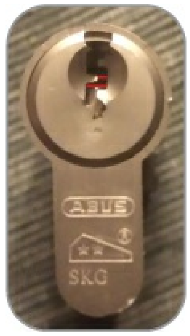


Figure 10-7: An ABUS EC60 lock showing a keyway with huge changes in key width (the C83 has more subtle changes)

As you get used to certain types of key blanks, this variation in width can be a useful indicator; you might start to recognize that halfway through cut depth 4, for example, the key starts widening. These alternating widths will require you to cut through different amounts of material, and you may be tempted to use more force. Instead, just alter the number of strokes you use.

FILING DIRECTION

Metalwork files work only when pushed in one direction—forward—so you have to lift your file off the working surface when positioning for your next stroke. However, some of the world's best impressioners violate this rule. Just because they happen to win competitions doesn't mean they're right. Don't let this zigzag motion become habit, as it won't be easy to unlearn.

Impressioning an ABUS C83

Let's start impressioning an ABUS C83 key. Now's the time to double-check that your lock is securely mounted in your vise, nothing is on the surface of your prepped key that could be mistaken for a pin mark, the key is secured in the handle, and nothing is touching the cam.

Secure Your Key

Insert your key in the lock, keeping it as straight as possible. If you turn it even slightly when it's not fully in, you may get half markings that you later confuse with actual marks.

Get into the habit of checking whether you've inserted the key completely. This might sound weird; you've been using keys all your life, after all, so *surely* you know what you're doing. However, further into the impressioning process, you might end up with steep ridges in your filed cuts (see Figure 10-8). These ridges can prevent the key from entering the lock as smoothly as you're used to, and you might think you've inserted it completely when, in fact, it's only partway in. This can create misleading marks.

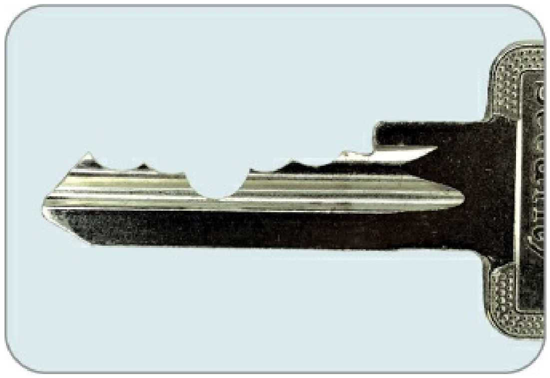


Figure 10-8: A cut with ridges too steep for pins to move up to

If you notice that inserting or removing your key is getting harder, round out those ridges and give the cuts a light polish with your file before reinserting. We recommend using a large round file for rounding out ridges, but a regular file will also do the job.

Make the Initial Marks

With your key properly inserted in the lock, you can start making marks. The easiest way to do so is the double-handed jiggle technique pictured in Figure 10-9: place your nondominant hand on the handle lever and your other hand on the back of the handle. With your nondominant hand, turn the key either clockwise or counterclockwise; you don't need to use much force at all. With your other hand, move the back of the handle up and down to create a rocking motion with the key in the lock. (If your handle doesn't have a lever, you could just use your dominant hand to do all the turning and jiggling, or grasp the head of the key to turn it.)

This action should lift the pins, except for one binding pin that will push back against the key. This pushback will create marks. Now turn the key in the other direction and repeat the jiggle motion. Try to keep all the motion at the same angle as the key, adjusting as needed if your key starts moving any way other than up and down, parallel to the key.

Figure 10-9: The double-handed jiggle technique: the nondominant hand does all the turning, while the other does all the jiggling

Repeat this process a couple of times to maximize the mark making.

> There are different techniques to produce marks; some guides will tell you to tap the head of the key as you apply turning force, whereas some say tugging the key away from the lock or pushing it slightly will make better marks than the jiggling motion. While some of these techniques do have merit in a noncompetition setting, I've never seen someone able to use them at a speed that matches the jiggle technique. Feel free to experiment and prove me wrong!
>
> —JOS

Now take out the key and start looking for marks. Figure 10-10 shows a mark a little left of center in one of the 11111 cuts. Marks should be in the middle of the cuts, so this means our spacing was slightly off to the right in our initial 11111. To counteract this, we'll need to pull the file slightly to the left when making the first cut.

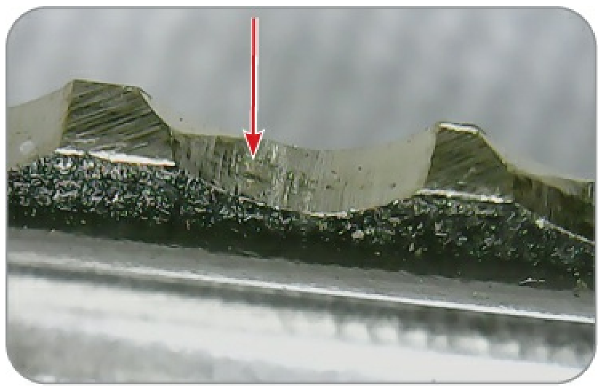


Figure 10-10: The first mark

File the First Cut

It's time to file on the mark. Don't use too much force when positioning the cut; you don't have to do it in a single stroke and will risk overshooting a cut if you try.

File at the marked position (adjusting sideways a bit if you need to counteract a slightly misaligned 11111 as we did) until the cut is one depth farther. If the cut looks rough, smooth it gently with your file to get a nice, uniform surface. You should have a smooth, clean valley to work with; see Figure 10-11, which shows a slightly different angle on the key to better illustrate this.

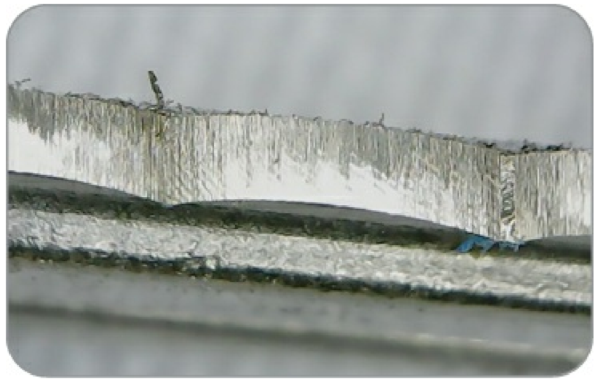


Figure 10-11: A clean key surface after filing on the first marks

Now that you've reestablished a clean working area, you repeat the steps for mark making.

Repeat the Process

Reinsert the key, perform the jiggle motion again, and repeat the filing step. With any luck, you'll have a perfectly centered dent, as shown in Figure 10-12. If so, you can file straight down to the next possible depth without making any sideways adjustments.

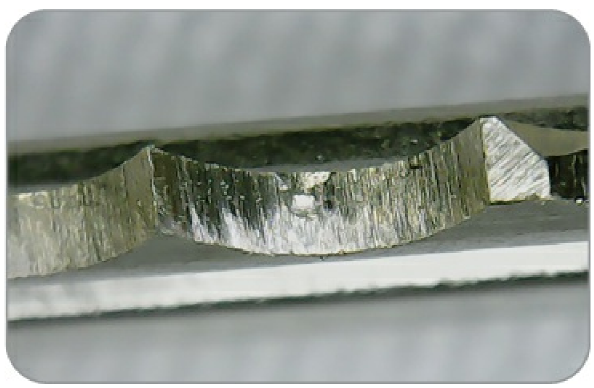


Figure 10-12: A new impression mark after repeating the first steps

If the surface looks rough, smooth it out again (Figure 10-13).

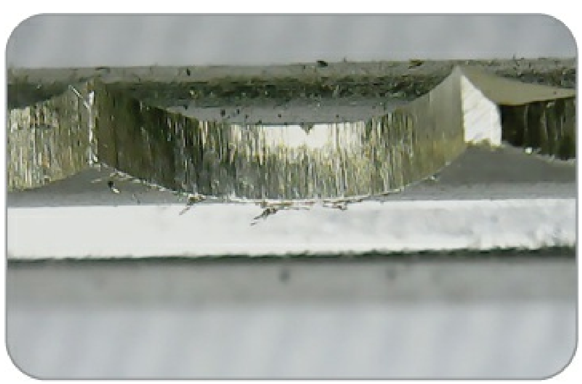


Figure 10-13: Restoring the clean key surface after filing at another mark

The polished surface will enable you to see another mark appear in the same position. Reinsert the key and do another jiggle; your mark should look like Figure 10-14.

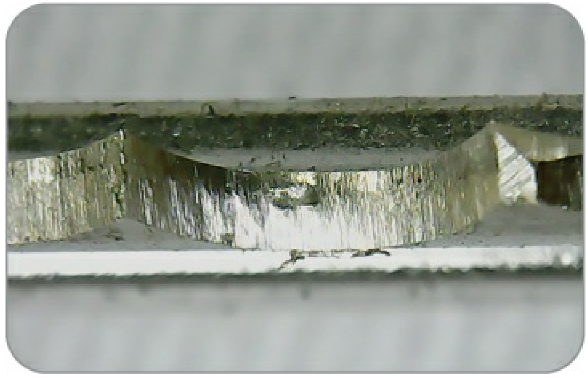


Figure 10-14: The third mark

Again, assuming this mark is well positioned, you can file straight down. Continue the whole process (filing, polishing, jiggling) as long as you keep getting marks in this position (Figure 10-15).

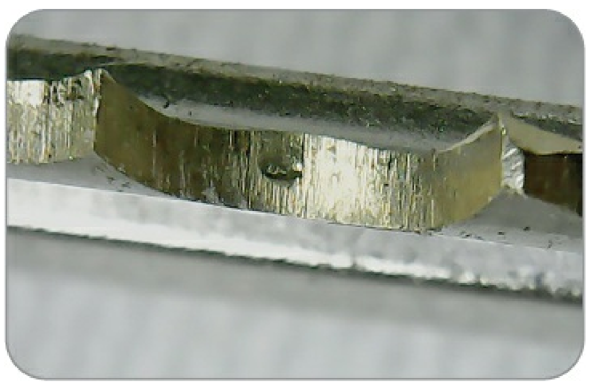


Figure 10-15: The fourth mark

At some point, you'll stop seeing marks in the position you just filed. This means you've reached the right cut depth, and the pin will align with the shear line.

A different pin will now be binding, so repeat the jiggling technique to look for marks in another position on the key. In the example shown in Figure 10-16, the cut next to the one we just completed is now marked.

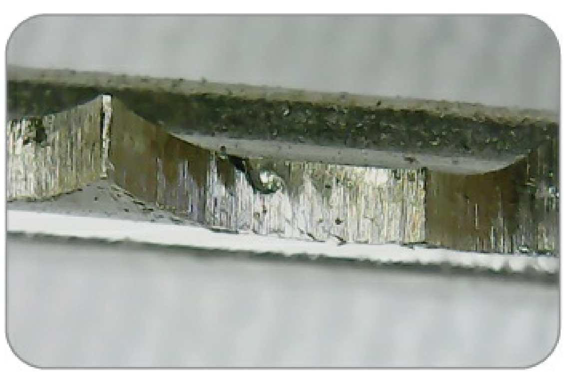


Figure 10-16: A new mark that looks deceptively off-center

Notice that the new mark doesn't appear exactly in the middle of the cut but *does* appear in the deepest part of the cut. Look at the far right of Figure 10-16 and you can see that as we were filing away material in the first cut, we dug so deep (and therefore also so *wide*) that our file took away parts of the hump of the key dividing the first cut from this cut. The new mark is still where it's supposed to be, but its surroundings have shifted somewhat so that the two cuts look like they are slowly becoming one.

After filing this new mark one depth deeper, jiggle your key in the lock again, and—lo and behold—a mark appears on the exact same spot. Again, filing is in order. Repeat these steps until you no longer see marks in this cut.

On the next pass, a new mark appears on the cut closest to the tip (position 5), as shown in Figure 10-17.

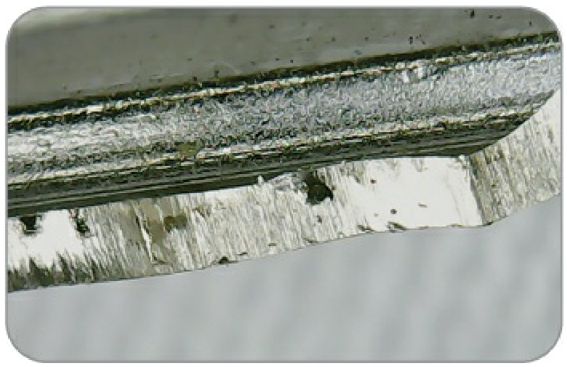


Figure 10-17: A new mark near the tip of the key

This mark also seems to be a bit off-center, but this time, it's again because our initial 11111 spacing was slightly off (you can assume this is the case if you made no extensive filing actions in the adjacent cut and have no other obvious reason for the mark to be off). As we discussed before, if this happens, you can incorporate a bit of lateral movement when cutting to the next depth to bring the cut into alignment with the pin spacing.

In the next pass, we have another obvious, nicely centered mark, as shown in Figure 10-18.

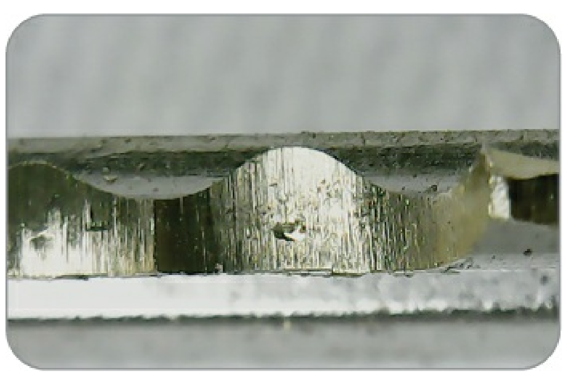


Figure 10-18: A nicely centered mark for the third binding pin

The next round of jiggling produces a subtle scuff mark (see Figure 10-19). The rule is always "When in doubt, don't file," so the appropriate thing to do here is give the cut a quick polish to restore the uniform finish, and then make another marking attempt.

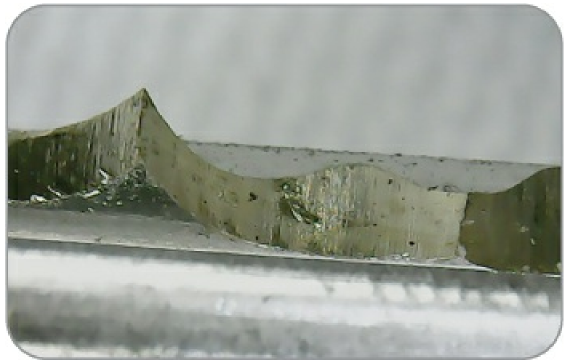


Figure 10-19: An off-center scuff mark

The mark appears again, so you can file to the next depth, correcting the direction if the mark is a little off-center as it is in our example.

After this round of polishing, notice that the key itself is wider at the bottom of the cut than at the top (Figure 10-20). Therefore, filing the cut one depth deeper will require extra swipes of your file.

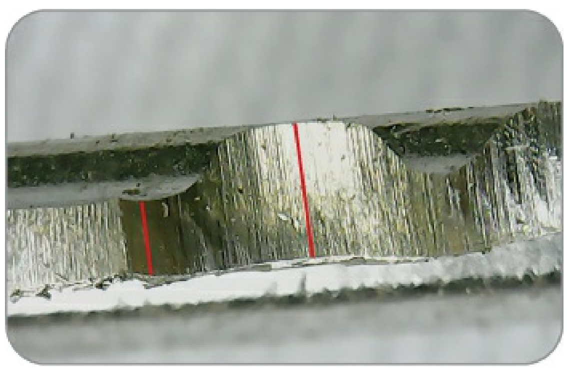


Figure 10-20: A polished key edge that's thicker at the bottom of the cut than at the top

Yet another jiggle produces a smaller mark (Figure 10-21). This one is nicely centered, so there's no reason to distrust it. You can file it down.

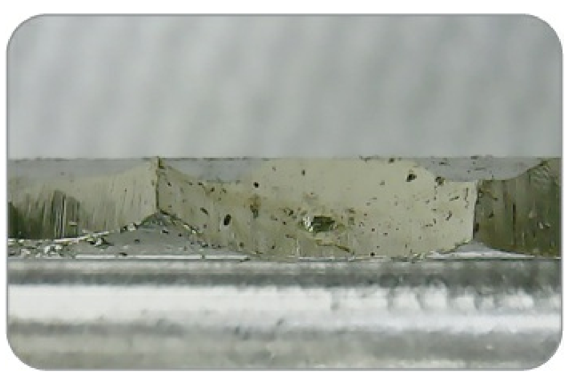


Figure 10-21: A smaller mark that needs to be cut down

At this point in our example lock, when we reinserted the key and applied a turning force on our grip, the plug turned. When you likewise successfully produce a working key (Figure 10-22), try to get into the habit of yelling "Open!" as you would in a competition setting.

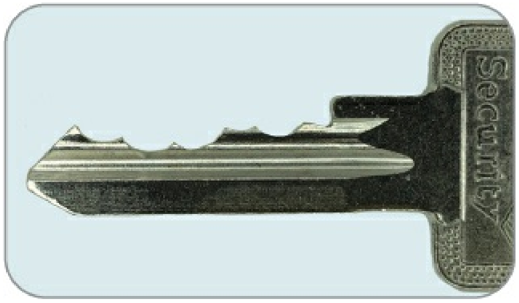


Figure 10-22: An impressioned C83 key

CRATER MARKS

One mark is a different beast than the others: the *crater mark*, shown in the following image. Named for its crater-like appearance that can usually be seen without magnification, this is the most recognizable mark of all.

This deep dent is typically caused when every pin but one has reached the correct height (is at the shear line), so all the force you put on the key is pushing on that single pin. Turning that key will take considerably more force than operating an original key and will probably be noisy. A crater mark is a good indication that the last pin is almost at the correct height and is the only pin left pushing back *hard* against the key. When this happens, you probably have an open, but your filing was probably a bit off.

During a competition, yell "Open!" and be done with it, but during a training session, a crater mark is a sign you should recalibrate. The chances of a pin being pushed one complete depth level into your key are close to zero. Either you were deliberately filing away the tiniest bit of material (which is a good tactic if you didn't know the depths for this particular lock) or you took off the wrong amount of material and just got lucky with this particular opening. You always want to achieve opens with skill, not luck!

Congratulations, you've successfully impressioned an ABUS C83! As we noted at the beginning of the chapter, however, not all locks mark in the same manner. To illustrate this, now let's look at a condensed version of this same process on a Schlage lock.

Impressioning a Schlage

Schlage locks, and clones thereof, are readily available in the US and thus are used in most impression competitions in that part of the world. The pins are a bit softer than those in a typical European ABUS, so their marks can be less obvious, especially when the pins have taken some abuse (like several rounds of impressioning).

NOTE

Kwikset is another commonly available lock brand in the US, but Kwikset pins aren't pointed, so the impressioning marks they make will be even harder to spot than those from Schlage pins. Don't start your impressioning journey with Kwikset locks; you'll just get frustrated.

The impressioning process for a Schlage is exactly the same as for the ABUS, so we won't show a complete step-by-step procedure again. Instead, we'll focus primarily on identifying the marks and how they differ between the two brands.

As with most keys straight out of the box, the Schlage blank sports a rough chrome coating (see Figure 10-23). Begin by filing this off.

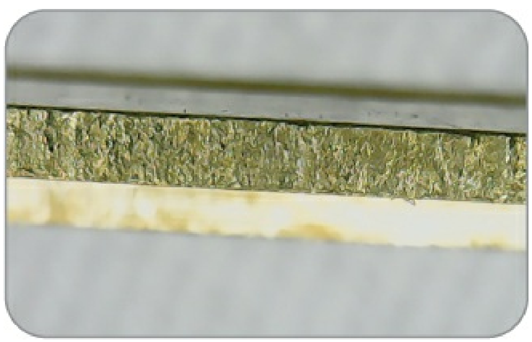


Figure 10-23: The Schlage key straight out of the box

Figure 10-24 shows the dechromed surface.

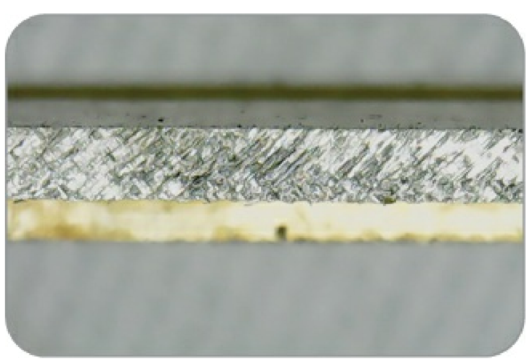


Figure 10-24: The Schlage key with coating removed

Although the filing here could be neater and more uniform, you can clearly see the difference after scraping off the initial finish: the surface is much more silver. To get an idea of where the pin stacks are and where to make the cuts, we used the KJS spacing tool (one tailored to the Schlage now instead of the ABUS) to mark the pin positions on the key (Figure 10-25).

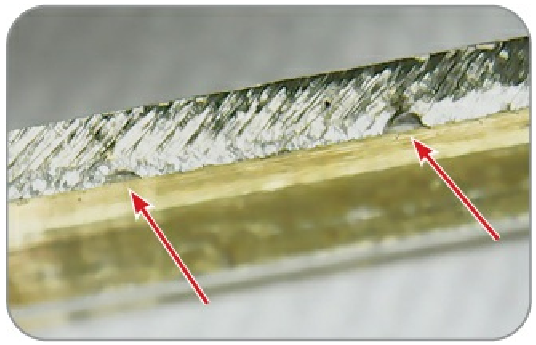


Figure 10-25: The Schlage key with spacings marked

Now you can file the key into a 11111 key. These Schlage keys come straight from the factory almost at depth 0 (which, as you may you recall, is used only for master-keyed locks). Therefore, they look distinctly different because of the mesa-like spaces between the cuts (Figure 10-26). This makes no difference to our impressioning exploits; just file down to your desired depth (11111, at this point) as usual. However, if you didn't know this, overfiling would be quite easy.

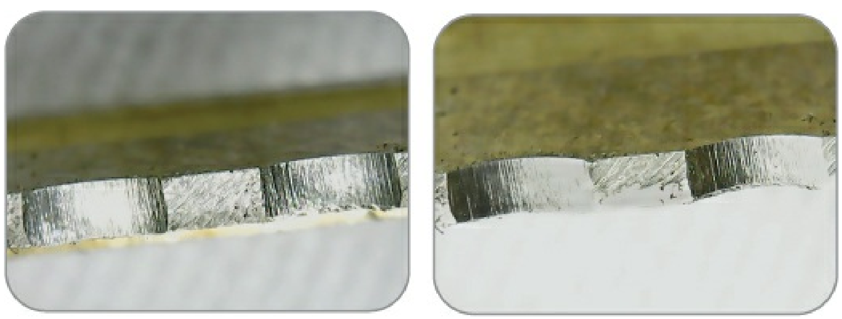


Figure 10-26: The Schlage key surface filed to 11111

Now you should have a fully prepared key with smooth curves at depth 1 for each position. When you insert the key into the lock and start the jiggling process, you'll of course expect marks to appear. However, the lock we're using in this example isn't new and has already been impressioned a handful of times. Some pins lose their pointiness when they get impressioned a couple of times, and this is apparently the case for our lock, since the marks are fainter than expected, as shown in Figure 10-27.

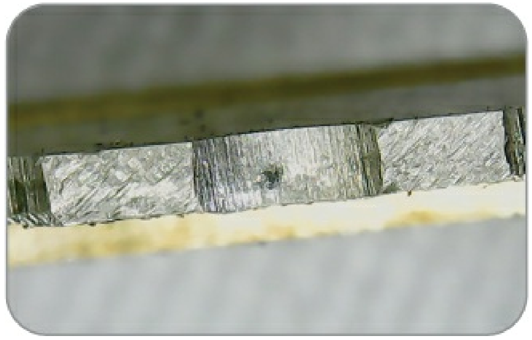


Figure 10-27: First (faint) mark on the Schlage key

Though faint, it's still a mark. As in regular lockpicking, you're looking for the odd one out, so if there are no marks in four cuts but even just a faint one in the fifth, that's probably the position of the binding pin. You can file that mark one step down and then polish if needed (Figure 10-28).

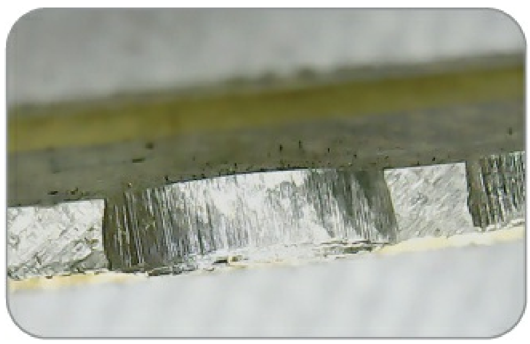


Figure 10-28: The Schlage key after filing down the first mark

After jiggling a second time, you can see a slightly deeper mark appear at the same position, and then again after yet another cut/polish/jiggle cycle (Figure 10-29).

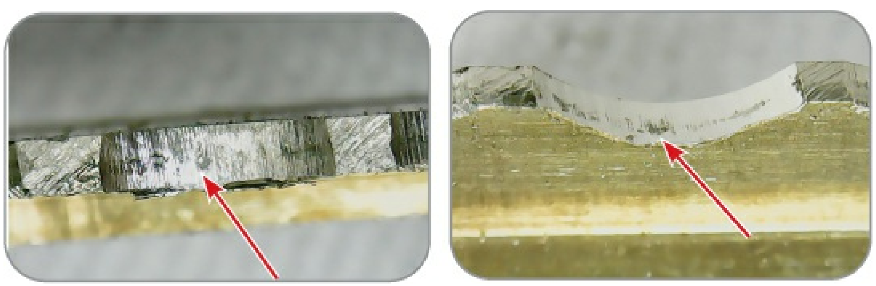


Figure 10-29: The second (left) and third (right) marks on the Schlage

In Figure 10-30, you can clearly see the chromium flakes from filing the key. Remember to remove these with a toothbrush before reinserting the key into the lock, as they can generate false marks or get embedded under your skin.

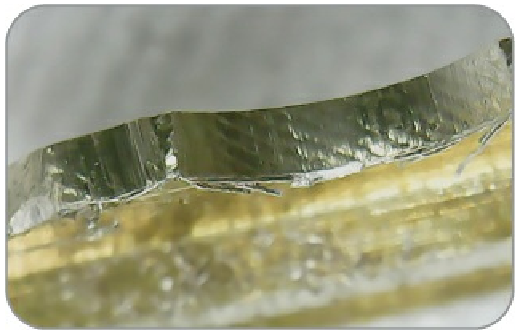


Figure 10-30: A freshly filed Schlage key with chromium flakes

If you're having difficulty spotting any marks, you could try using more force in the jiggling process. Usually, a better option is to use a spacer tool or improve your lighting. Changing the angle at which the light bounces off the marks can be especially helpful (Figure 10-31).

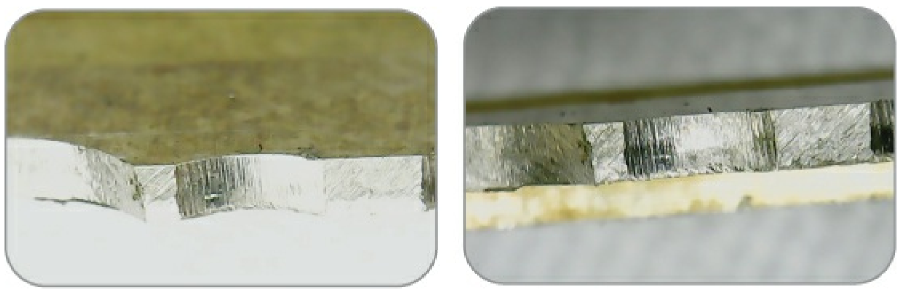


Figure 10-31: Two photos taken from a different angle to see the mark more clearly

As you continue finding marks and filing down your key at these positions, the key should slowly start to resemble its final stage. But since you have no prior knowledge of the actual depths you need to reach, you have to "lather, rinse, repeat" until you get an open or see spot marks past the maximum depth (meaning you've overfiled and need to start over with a new blank).

Figure 10-32 shows other examples of what Schlage marks might look like.

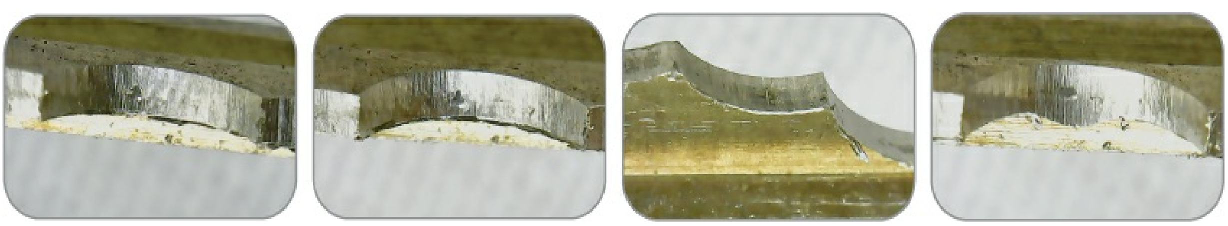


Figure 10-32: Various Schlage marks

If you do every step right, at some point your key will turn. Quickly confirm that you didn't break your key and, assuming you didn't, yell "Open!"

In a competition setting, you'd leave your key in your lock, and that would complete the round. But in a noncompetition setting, this is a good opportunity to peek at your key. As you can see in Figure 10-33, a mark remains. Since you have an open lock, this must be a (rather subtle) crater mark.

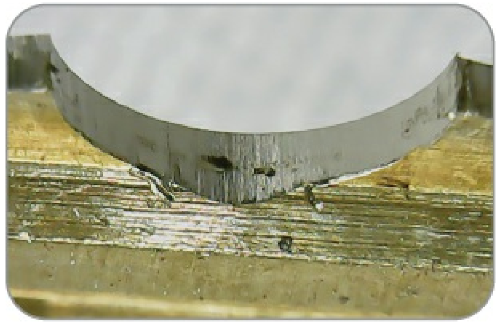


Figure 10-33: A Schlage key with a subtle crater mark

If you want your key to operate more smoothly, you can carefully polish this mark away. Make sure not to overfile after all your hard work.

Well done (Figure 10-34)! Now you know how to check for and file down the more subtle marks on a Schlage key to successfully open that type of lock.

Figure 10-34: A successfully impressioned Schlage key

Using Other Tips and Tricks

You've now seen how to impression two common brands of keys and can start practicing and honing your skills. Before you face an actual competition, though, you should know some tips and tricks to step up your filing and mark-hunting game.

Spacing and Depth Guidelines

If you know the spacings and depth of the lock you're attacking, great! But if you lack that information, you'll need some tricks up your sleeve. One useful tool for checking that you're creating your cuts in the right positions is a filed-down lock plug, like the ABUS one shown in Figure 10-35. The make and model of this plug should match the lock you're impressioning.

Figure 10-35: A filed-down ABUS plug

When you insert your key in this plug, you can see exactly where your cuts are supposed to be (see Figure 10-36).

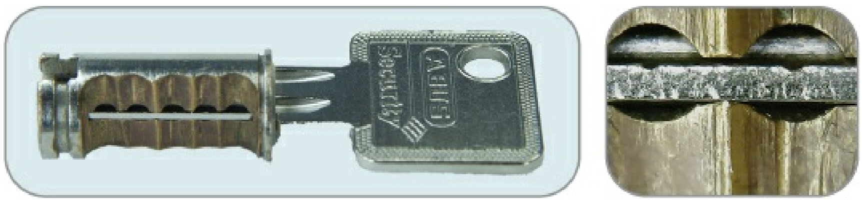


Figure 10-36: The filed-down plug with the key blank inserted

This tool isn't *necessary*, but it can speed up the process and minimize frustrations considerably by eliminating a lot of guesswork. It's especially handy during competitions; when in doubt about the validity of a mark, you can instantly confirm the spacing. Or, if you can't seem to find any marks at all, the plug gives a precise road map for where to look.

> Building your own filed-down plug is easy; I created mine with a lock, a big file, and some elbow grease a mere hour before a competition. Having access to a lathe and ample time would make it look way cleaner.
>
> When I created mine, I filed it down with the goal of prepping a 11111 key quickly: I would slide in a blank key and file the key until I hit the plug. An excellent idea—except that using the cut plug over and over again meant I was filing a little off of it too, resulting in an overfiled 11111 key. Therefore, I don't recommend using the filed plug to create a 11111 key.
>
> —JOS

Next, how do you know how deep to cut? Take baby steps and definitely avoid overfiling while prepping. Try to aim for increments of no more than half a cut depth as a maximum for each round of filing. Two-tenths of a millimeter per step is typically a safe bet (if you have access to a depth chart, use that, of course).

NOTE

When a pin stack with standard key pins stops marking, you've probably reached the correct depth and shouldn't file on that position any farther. If your lock has serrated *key pins, however, chances are you're not done yet. After the other pin stacks have reached the correct depth, the plug will have a tad more room to turn (this can be subtle, so you probably won't see or feel it); this* *additional room might cause the nonmarking key pin to start marking again*.

With standard pins, generally the sudden absence of marks indicates that a cut is at the right level to align the pin with the shear line at that position. You might also see "smudges" like the marks you made earlier when using the polishing technique to figure out your spacings (see "Filing the Key's Surface" on page 171). With that technique, the pins riding the key (but not binding yet) left polished spots on the key. Likewise, when a pin stack is lifted to the correct height, it's no longer binding, so the same kind of polishing can occur. If you find that the bottom of some cuts reflects light a bit differently compared to others, those might be "end marks" indicating that your cut depth is correct.

Filing Tips

In a competition setting, when someone nearby is impressioning, the first thing you'll notice is probably the sound—a screeching, nails-on-a-chalkboard noise that's generally considered unpleasant. Too much of that sound is never a good thing, for your ears or the key. If your file swipes are making a high-pitched squeak instead of a consistent *swoosh*, your file might be skipping (think of a bow on a violin); this indicates you're applying the wrong amount of pressure, which will result in suboptimal results. Putting the tip of the key on a rubbery surface helps minimize the sound, as it lessens the vibration of the key.

If your final swipe for a particular cut seems especially noisy, you might have left a rough surface and need to do one more gentle swipe to give the cut the desired smoothness. Give it a try; if your file is loud, chances are you'll see ripples in the cut, not unlike a sandy beach. Smooth it out so you can see the marks better.

Mark-Reading Techniques

Finding marks and distinguishing true ones from false ones is probably the most important skill in impressioning. Here are some quick tips:

- Make sure your cut surface is clean so you can more easily spot marks.
- Put ample force on your key in the lock to make nice, obvious marks.
- Stay within your predetermined spacings so you know exactly where to look for marks (at the bottom of the cut "valleys").
- Use decent magnification and proper lighting.

What you're looking for when hunting for marks depends on a variety of factors, and not all marks will look the same: not all pins are pointy or hardened, and some pins are altered by years of (ab)use.

To ensure the best chance of getting clear marks, refine your jiggling technique. Using both hands, insert the key into the lock, and go through the jiggling motion discussed earlier. If you don't see any marks when you remove the key, reinsert it and try again.

Change either the up-and-down force or the turning force to see which works best for creating marks. Make sure to use both hands for the greatest control.

As with other lock-manipulation techniques, you're looking for the mark of the binding pin. If you see a smudge-like mark in four positions and a more distinct mark in position 5, odds are that number 5 is the mark for the binding pin. File one depth down at that position, give the other positions a light polishing, and then reinsert the key to see if the filed position is still marked.

Marks on the key can be very, very subtle, so it's important to start every jiggle with a fresh, scratch-free key blank. Misreading a scratch, dent, or abrasion as an actual mark is easy, and marks created by pins are clearer to spot if the blade has no other blemishes. Be wary of mistaking the following for pin marks:

- Debris, oil, or graphite in the lock, whether introduced by you, a previous user, or normal wear and tear
- Added material, such as the key's coating or coloring aids
- A change in the lighting that might create misleading shadows
- Slips from your file
- Shavings from your previous filings

Keeping the cutting edge of your key clean will help avoid accidentally marking your key with anything other than legitimate pin marks.

Marks can sometimes be tricky to spot. As noted earlier, bouncing light off them from different angles can make that hunt easier. If you don't see any obvious marks, turn your key while looking at it through your magnifier. At certain angles, the light will bounce off a legitimate mark differently from the rest of the surface.

The takeaway of all these tips and opportunities for experimentation is *never stop progressing*. Read, watch, train, learn, and absorb knowledge, but embrace the hacker ethos and never stop thinking of how to improve.

Summary

In this chapter, we walked you step-by-step through the process of impressioning basic pin tumbler locks, including preparing the lock and key, identifying legitimate pin marks, and determining where and how deep to file. With this chapter and some practice, you should be able to open a lock with only a key blank, a file, and basic tools.

You can't learn impressioning from just reading books and watching YouTube videos alone. Sure, you can learn *about* it and pick up tips and shortcuts that will make the process more manageable. But truly mastering this skill requires plenty of hands-on attention and real-world practice.

Once you're comfortable with the impressioning process and feeling more confident with your abilities, you might want to start exploring events in your area. In the next chapter, we'll give you a tour through the world of impressioning competitions.

11
IMPRESSIONING COMPETITIONS

Now that you've gone through each step in the impressioning process, it's time to get you competition ready. You're welcome to enter an impressioning contest no matter your skill level, though as a beginner you probably won't reach the finals round quite yet. If you practice the training tips in this chapter, however, they might help you do just that. We'll also review what to bring to a competition, what the environment is like, and how to organize a competition yourself.

Honing Your Contest-Level Skills

The only way to figure out how you measure up against the rest of the field is to compete. Competitions are meant to take away as many variables as possible so that the only thing being measured is the skill of the contenders.

The best way to hone your skills to the international championship level is, not surprisingly, practice, practice, practice. Or, as the TOOOL mantra goes, practicing over and over and over (hence the three *O*s in *TOOOL*).

NOTE

TOOOL originated in the Netherlands, so the original mantra was in Dutch. The three Os then (unofficially) stood for oefenen, oefenen, oefenen (practice, practice, practice*)*.

Let's go through a typical training regime.

Do One Thing Well

First, determine the kind of locks used in the competitions held in your region. If your part of the world doesn't yet host competitions, stick to the more common Schlage, ABUS, or Lockwood brands, or whatever is easiest for you to source locks and blanks for. (Note that two brands in the world are called Lockwood; we're referring to the one produced in the

Australasia region.)

Buy a bunch of locks: 20 to 30 is a good number. You want variety in order to build your impressioning skills, so make sure these locks aren't keyed alike or part of a master-key system. They don't necessarily have to be new; a local locksmith might have some discarded locks you can have. You want to get incredibly good at impressioning that one particular brand of lock. You might think of yourself as a one-trick pony, but outshining the rest of the field by being exceptional at that one trick will help you win prizes.

Calibrate Your Technique

Calibrating your method is critical to consistent opens. For example, say you use the ABUS C83 as your standard. By calibrating, you'll know exactly how much force on the file will take off a particular amount of material, how many swipes you'll need for a single depth level, and what length of file you'll need to get a cut down to the next depth. Then, when you see a mark, you can file down to the next cut in one go and without measuring.

If parameters change—for example, you enroll in a competition that uses Schlage—you can still approach everything with your own standard calibration. One cut might now be an ABUS-and-a-half, for example, so instead of needing four swipes, you now need six to go down one depth. Otherwise, you should change your standard routine as little as possible. This kind of calibration works in all sorts of situations. Say you're handed blanks that seem much softer than you're used to. Just dial back on your tension and maybe use fewer swipes.

Try to keep the number of variables you change to a minimum. You've trained long and hard to get your autopilot into gear, so don't confuse it too much by throwing all this new stuff at it. Changing one, maybe two, parameters at a time will give you insight into which change actually worked.

In the past, ABUS used *alte Stiftung* (German for "old pins"). These pin sets consist purely of solid, nonserrated key pins and use spool pins for all driver pins except one, which is solid. As you can see in Figure 11-1, this pin set is hugely different from the excellent *neue Stiftung* (new pins) ABUS currently uses.

Figure 11-1: Old (left) and new (right) ABUS pins (images courtesy of Jan-Willem Markus)

For years, the good folks at ABUS have been supplying locks and blanks to major European locksport competitions. Its generosity resulted in the brand becoming the de facto standard in the majority of European impressioning games. One year, during the German SSDeV national championships, the old pins were replaced with the new pins, and competitors were unknowingly introduced to the new standard.

> And boy, we were *not* prepared: a lot of people were unable to open their locks in the first round. In one particular round, I was the only one to open in the allotted time of one hour. It was carnage.
>
> —JOS

Experienced impressioners gradually got used to the new playing field, but these new pins proved to have a rather steep learning curve. Thus, if you're in Europe, it might be wise to start your impressioning quest on some Buffo locks instead of the newer ABUS locks. Buffo locks have the same depth and spacing as other ABUS locks, so your calibration will carry over between (sub)brands.

Keep Up Momentum

Keep training and train often. Consider setting up your workbench somewhere central in your home so that you can just sit down and start filing whenever you have spare time. Once you get better and better at this, you'll open three locks before the microwave goes ping! Of course, your living setup will influence how and where you can practice.

Another way to keep your momentum going is to get a training buddy; this doesn't have to be someone exactly at your skill level to be beneficial to both of you.

> In my early years of training, I had the privilege of having Barry Wels, then the Dutch and German champion, as a training partner. The biggest advantage was when we swapped locks. We would both impression a handful of locks, rekey them, and two weeks later, swap again. We began keying the locks at ridiculously difficult settings. The maximum adjacent cut specifications (MACS; introduced in Chapter 5) were completely out the window. We'd start with bittings like 1-1-1-2-1 that make it easy to overshoot your cut depths, and keying that required cuts like 9-8-9-9-9 or 9-1-9-1-9 that aren't even allowed at competitions. Competition locks started to seem easy by comparison.
>
> —JOS

Break Keys

During training, you'll definitely break keys—and that's a good thing. In impressioning, you're trying to put as much force on a key as necessary to noticeably mark it. The more force you use, the better the marks, but too much force will break your key over time. You need to find the balance. If you never break any keys, you have no idea where the breaking point is. Failure can be good.

You can also learn from a broken key. Did you feel confident in your filings before the breakage? If you think the breakage occurred from too much force on the key, but your cuts were good, you can re-create those cuts in a new blank. You don't have to start your new key with a 1-1-1-1-1 bitting; you could file it down to where you were when the breakage happened. Since your new key hasn't been introduced to a lock or had any jiggling torque applied, you should see no signs of metal fatigue.

Listen to Your Body

While in training, you'll burn through blanks much faster than standard usage requires; it's not unusual to use a full box of 50 blanks before a tournament. Not surprisingly, then, *repetitive strain injury (RSI)* can become an issue. One example is tenosynovitis, inflammation of the fluid-filled sheath that surrounds a tendon (the tenosynovium), typically leading to joint pain, swelling, and stiffness. According to Wikipedia, RSI is "caused by repetitive use, vibrations, compression, or long periods in a fixed position." This sounds an awful lot like impressioning training.

You can take steps to minimize these risks. First, when it hurts, *stop*. Your body is trying to tell you something, and if you ignore it, it'll only yell louder. During competitions you might choose to continue this overexertion since it's short-term, but during training, *just don't*.

Stop and consider what your body is trying to tell you. Are you sitting in an uncomfortable position? Do you need to alter your stance for a particular step in the impressioning process? Is your grip as comfortable or convenient as it could be? Are you clenching your grip too hard? You don't need to clench your grip, as the torque is applied through the lever; if you're jiggling your key with a clenched fist, you'll be moving all over the place, causing breakage. Often you can make sufficient up-and-down movements with only your fingertips. Your tenosynovium will be grateful.

> After closely examining my own process, I concluded that mounting my lock in the American configuration, with the key's cutting surface facing upward, eliminated the need for an extra turn of my handle. Fewer movements mean a smoother workflow and less likelihood of injury. The fact that this change also shaved a few seconds off my opening times is a bonus. I even started working with an occupational therapist to analyze my impressioning process. Introducing a side-handle lever to my impressioning grip proved to be a huge advantage healthwise while simultaneously enabling me to apply force in a much more controlled manner.
>
> —JOS

Optimizing Training

When in training, well ahead of a competition date, you might opt for slowly altering your routine. It's important to regularly reflect on improving your way of working, but make sure you don't change anything about your process immediately leading up to a competition.

Change only one factor at a time, such as the placement of your vise or not putting your file down while jiggling. If you change everything at once and notice a difference for good or bad, you have no way of knowing which variable introduced that difference.

Focus on consistency; only when you've figured out that part should you work on improving your speed. Competitors can still lose if they open locks at record-breaking speeds; the time to open is considered only if the leading competitors all opened the same number of locks. Opening a bunch of locks quickly but failing to open just one means you'll be beaten by that one person who opened every lock reliably.

Packing

Before you leave your home or hotel room, double-check that you've packed all the gear you'll need. Bring as much of your own gear as possible, and don't rely on others to have backup equipment for you. Here's our recommended packing list:

- Primary file
- Spare files
- Handle
- Backup handles
- Allen wrenches
- Spacing tools
- Sharpie, pen and paper
- Toothbrush
- Locks and keys (for practice and warmup)
- Light source
- Backup light source
- Extension cord
- Workbench
- Rubber sheeting as a work surface
- Snacks
- Cash for drinks

> Always bring spare files! I once had a file break during a competition, which I'd never experienced before. It took a second for me to realize what had happened, and during that very brief timeframe a fellow competitor had already put his spare on my table. True sportsmanship! (Thanks, Django!) It was highly appreciated, but you shouldn't count on that chivalry happening in all cases.

—JOS

Try to bring backups of your items where feasible, even if your gear has never failed before. Flying internationally with two bench vises might not be the best course of action, but grips, lights, and files shouldn't pose a problem.

As noted in Chapter 9, if you use anything electric that you need to plug in somewhere, bring an extension cord and international adapters. Remember to get an adapter that can convert voltage. And always bring gaffer tape—lamps can fail during competitions because their power cords fell out of the socket; gaffer tape will come in handy in some surprising situations.

Finally, to assure yourself that everything is in place and in working order, impression a key before the competition. Pack a lock that you know you can impression but don't necessarily know the combination to; this also serves as a confidence builder.

Set up your gear in advance. The competition schedule should account for setup time, so you'll have ample time to MacGyver any problems you might run into. Don't use any equipment you just acquired pregame; use what you trained on. Remember, your autopilot will work only when all the variables remain the same.

Understanding the Competition Environment

Generally, impressioning competitions all follow a similar format, with slight variations. The competition includes two rounds. In round one, each competitor works on a keyed-alike lock for an hour at most. The first six competitors (or whatever number is decided beforehand) to open their locks progress to the finals.

Each of the finalists gets a uniquely keyed lock and a specified period of time—usually 15 to 20 minutes—to open it. When that time is up, the locks change hands (whether or not they've been opened) so that all six contestants are working on another lock. The process repeats until each contestant has tried each lock. The competitor who opens the largest number of locks wins.

In the case of a draw, the person with the fastest total time wins. Opening consistently, even if you're not the fastest, can—and in many cases, will—earn you the win.

> My first official subminute opening was during a German competition which, despite setting a new world record, I didn't win because I failed to open one of the six locks.

—JOS

We'll dive deeper into the specifics of competing in "Going Through a Competition" on page 202.

The competitions are long and laborious: you must survive the first hour and then two subsequent hours (six rounds of 20 minutes each). Being fast does help, because if you open before the allotted time runs out, you can leave the room and relax a bit. Official breaks occur too, but they might be scarce.

It's easy to underestimate how exhausting competitions can be; contestants have almost passed out during the heat of battle, requiring medical treatment. Make sure you take in plenty of fluids, but not too much (official breaks include bathroom breaks) and avoid drinking a lot of alcohol or caffeine. If things turn out well, you'll have ample reason and opportunity to party afterward, so pace yourself.

High-protein snacks are also advisable; bring your own, or at least stick to something that you know agrees with you (remember those scarce bathroom breaks).

These tips might sound a bit overcautious and far-fetched, but once you've progressed to an international level of competing, you've also progressed to the level of "filing with jet lag," "filing in different time zones," and "filing while digesting that weird curry you had late last night because you were partying with folks you hadn't seen in ages." *Hic sunt dracones!*

It would be a shame to travel half the globe for a competition only to fail because you didn't pay attention to these details. Failure is always a possibility, but you can at least minimize the kinds that would be embarrassing!

Arriving at the Venue

Taking a look at the competition room the day before the game is a good idea. That will help you get a feel for the environment, figure out where you want to set up your workbench, and determine whether the host's tables will hold your vise securely or you'll need to bring your own table. You can also find the locations of the power outlets and check whether they'll fit your power cords. Knowing details like this ahead of time will help you feel more comfortable and confident on competition day.

Other questions to consider include the following: Are there outside windows where the sun might help or hinder you? Will there be a crowd? Where will they be? You might prefer to set up close to the judges and timekeeping table, or you might prefer a quieter corner.

Once you get your first championship title under your belt, people (you included) will expect you to do well in subsequent competitions. If having four cameras pointed at you or the public hovering over your shoulder might throw you off your game, speak up. When you run into non-openings, these factors can quickly become a nuisance, and the cameraperson can set up outside your personal space and just use their zoom functionality. This advice applies for anything that can potentially throw off your mojo. Simply saying, "Excuse me, you're in my light" will go a long way. Whether you're a perceived backbencher or a probable finalist, you deserve to compete in a fair and pleasant way.

Some venues may have assigned seating arrangements. Bringing your own workbench typically doesn't work well with these arrangements. In these cases, if you're worried about the tables provided, work together with the competition's organizers to come up with a solution. Don't be demanding; they're probably all volunteers, working hard to make sure you can show off your skill. Leave the rock-star attitude at home.

Registering to Compete

Make sure to find out about the registration system beforehand. A lot of venues use a whiteboard of some sort to register contestants. If this is the case, write your name on the whiteboard to enter. Spots are usually limited, so the sooner you register, the better. Have someone else put your name down if your travel plans don't permit you to show up early. Make sure the organization knows your name is on the board despite you not yet being in the room (or town, or time zone).

If you plan to use an irregular tool or technique in a competition, remember to let the judges know well in advance—at least one day prior to the competition. Your new tool might give you an unfair advantage and therefore could be considered cheating. When in doubt, ask. You don't want to get disqualified, and organizers have a lot on their minds right before a game, so the sooner, the better for everyone.

Choosing Competition Tactics

You're sitting at your competition table, well fed, properly hydrated, fit, trained, in a zen-like state, ready to have your muscle memory take over and go into autopilot. Now what?

While opening your lock is more important than opening your lock quickly, you must be one of the first six to open in round one in order to progress to the finals. So you face a bit of a dilemma: if you take your time, you'll probably open the lock, but opening fast can boost your confidence and potentially get you to the finals. You must decide to what extent you're willing to sacrifice accuracy for the chance to score well. Make this decision deliberately; don't be tempted to outpace yourself because of all the hectic activity around you, but also don't lose access to one of those six spots because you feel the need to double-check everything.

Being on autopilot doesn't mean not paying attention. For example, at one German competition, multiple subminute openings occurred in the first round. After about 20 minutes, some competitors were still filing their keys to almost maximum depths. Some of them were likely on autopilot, but hearing "Open!" multiple times within the first minute should have clued them in that the bitting of the key to open the lock was probably rather shallow, so their cuts should be too.

> An important decision during competitions is when to discard your key because you suspect you overfiled somewhere. I once saw a very competent impressioner toss three keys for that exact reason. When his fourth attempt came up at the exact same bitting, he decided to file a bit farther because he was still getting marks. Twelve seconds later he'd opened the lock, and he realized his opening time could have been a fraction of what it was. Remember, impressioning is part mind game, part art, and part sport skill.
>
> —JOS

Here's another question to ask yourself: if you know the MACS for the lock you're working on, do you use that knowledge to determine whether a mark is a true mark? If you're feeling confident about your cuts and notice your key is starting to not adhere to MACS rules, there's technically no reason not to file down an adjacent cut. This might get you to open the lock faster and prevent your key from getting stuck in the lock. But, of course, being overconfident could lead to overfiling. Again, you have to strike a balance.

If breakages happen in a competition, you might have problems getting your key out. In this case, keep a few points in mind. Don't use a key extractor until you get permission from a local judge. Putting anything but a key in your lock is typically grounds for immediate disqualification. In round one, where locks won't be passed around among contestants, you need to extract all key bits within a reasonable timeframe before your opening time becomes official. What constitutes a "reasonable timeframe" will probably be decided then and there by the judges. In a final round, if you opened the lock but the key broke, your clock will be stopped, but the remainder of the key needs to be taken out so the next contestant can try opening the lock.

SPORTSMANSHIP

We need to discuss a potentially tacky subject: trash talk. The short version of this discussion is "Don't," and the slightly longer version is "Seriously, just don't." You're not competing in an MMA-style, gloves-off, cage-fighting match. While we've seen blood spilled during competitions on several occasions, all those instances were self-inflicted (files are pointy, and keys can be sharp!).

Try to keep this sport as inviting as possible for anyone who wants to have a go at it. Comments like "I'm sure I'm gonna win!" are okay, but it's best to let your files do the talking and cash in on bragging rights after the finals are over.

Going Through a Competition

Now let's take an even more detailed view of each step of the competition. First, you'll find a space and set up your gear. Connect your vise to the table and give it a good shake to make sure it's properly attached. Connect your light source to double-check that it works, and consider securing it to the table with tape. Also check whether your cords are a tripping hazard, and if so, hold them down with more tape.

Unpack everything else you'll need and place it on your work area/workbench (see Figure 11-2 for Jos's typical setup). You can then file a key as a warm-up. This practice will reveal whether you forgot anything and confirm that all your tools are properly connected and placed in the manner you trained for.

Figure 11-2: Jos's typical impressioning setup

Round One

Round one is the qualifier. At this point, everybody has their gear set up and is spread out throughout the room. Most competitions supply you with blank keys. Usually, those are the only blanks you're allowed to use during the competition. Make sure you know the local rules. If you *are* permitted to use your own blanks, use those since they're what you trained on.

Typically, you're allowed to put your blank in your grip before the competition starts. Other than that, you're generally not allowed to prepare that key any further, such as by smoothing the surface or marking pin positions. Again, check for any local rules you might be unfamiliar with.

Mounting extra keys in any spare grips you've brought is also an excellent idea. In case of breakage, you can just reach for the next grip and immediately start preparing that key. Having one or two backup handles ready to go could shave several seconds off your opening times. (Having five backups, however, would probably raise some eyebrows.)

Next, you'll be asked to remove any locks from your table before the competition locks are handed out. These should be new locks, often keyed alike, and they can be marked or numbered.

You're allowed to mount the lock in your table vise. Give the lock a good shake in the vise to confirm that it will stay in place when you're jiggling your key—but don't insert your key or any other tools at this point.

A judge will ask, "Everybody ready?" There's almost always a no or two, so after a moment the judge will ask again. Once everyone says yes, there will be a short countdown and then the judge will call "Start."

NOTE

This might be your first match ever, but that doesn't mean you don't have a voice in matters. If a judge asks whether everybody is ready and your honest answer is no, speak up! If you have any doubt about whether you completely understand the local rules, speak up! If you need extra blanks, speak up! Don't wait until you break your last one.

You'll hear a cacophony of high-pitched sounds as everybody starts filing away on their blanks.

At some point, someone will shout "Open!" and a referee will call out the current time. If that someone is you, you should write down your time, leave your key in the lock, and wait for an official to show up. They will check that your key works or ask you to demonstrate that it does. Once the open is confirmed, they'll relay that to the timekeeper, and you'll have an official opening time!

Most competitions require you to leave your key in the opened lock until the end of the round to minimize the risk of a competitor getting a look at the correct biting.

If you're lucky enough to be among the first six contestants to open, you'll progress to the finals. Some events will also have a B-final, during which the six runners-up go through the same round-robin match as the finalists to give more people firsthand experience of what the finals entail.

After the first group progresses to the finals, the rest of the field still has the remainder of the allotted time to open their locks. Try to keep the chatting to a minimum, even if all six slots have been filled. Everybody should get the same chance to score an open during a competition.

If fewer than the required number open within the allotted time, the finals will include fewer people than intended. Still, all finalists will usually be given all six locks in turn.

Finals

After a short break (not enough time for lunch, dinner, or a nap!), the six finalists are given fresh locks, all keyed differently. Write down the number marked on your lock. Some venues supply score sheets. Sometimes these sheets move with the lock during the final rounds, and sometimes they stay with the contender. Either way, don't forget to bring a pen and paper.

Every final round will start similarly to the first round: someone will ask if everyone's ready, give a short countdown, and call out "Start," and the screeching sounds will begin. When you open your lock, call "Open!" and write down your opening time.

Each round is typically 15 or 20 minutes. When that time is up, remove your key, put it somewhere out of sight, and swap your lock with another contestant in a predetermined order (this part can be a bit chaotic). While the lock you handled in round one was likely brand new, the locks in this round will have been handled by your competitors and won't be as fresh. Bear this in mind as you hunt for marks.

You'll repeat this process until all six locks have been handled by all six finalists. If a B-final is held, its contestants will do the same with their own set of locks. The number of openings and opening times will be tallied up, and a winner will be declared (see Figure 11-3 for a photo of a victorious Jos). Congratulations! You're done and can take a bow.


Figure 11-3: Jos after winning an impressioning trophy

Organizing an Impressioning Competition

If no impressioning competitions are held in your area and travel isn't an option, you might consider hosting one yourself. Before you start organizing it, you should bear in mind a few pointers.

Make sure you have ample room for every contestant to work. Remember that numerous competitors will be bringing a metric ton of gear in Pelican cases, toolboxes, and other sturdy, bulky containers. Also, the judges will be walking around a lot and should be able to do so without bumping into people trying to compete.

Make sure your judges and officials know the rules. It's great if they know the game well, but most people who are knowledgeable about the sport are probably competing instead of judging, so a thorough explanation of the what, when, and how of the game should suffice. The officials will be the first point of contact for questions from the competitors and crowd.

Make sure everybody can hear the announcers and timekeepers. Test the sound levels from the back of the room; you may find you need microphones for the announcements. It's also worth bearing in mind the languages of the host country and those who might enter the competition. Words like *ready*, *start*, or *stop* will probably be understandable for most folks, but if the communication gets more detailed, you might want to switch to a common language or have translators.

The clock should be clearly visible from everywhere in the room, for spectators as well as competitors. Schedule a competition with ample time to spare. If contestants need an extra break, the schedule shouldn't be the reason you can't accommodate this request.

Locks used in competitions should be widely available and easy to acquire. If you strike a deal with a lock manufacturer who wants to have its über-secret, not-yet-released lock field-tested, that's okay, but don't call it a competition. Call it what it is: research. In that case, as with any research, participants should be aware they are research subjects and may need to be compensated as such.

Don't try to make the games "more interesting" by deviating from standards. Having contestants file dimple or lever keys can be fun, but these should be separate side events, not part of the standard pin tumbler impressioning competition. If you organize a marathon but place hurdles all over the track, it's not a marathon anymore. The same principle applies here.

The locks should be as the factory supplied them. Avoid adding or subtracting pin stacks, swapping pins out for harder or easier versions, or making any other modifications. The sport is hard enough without these additional obstacles.

If you expect international contestants to show up, try to accommodate starting times that correspond reasonably to their time zone. If you have competitors from all over the globe and host a multiday event, don't start the games on day one.

Order more blanks than you need, and give contestants one or two blanks beforehand so they can get a feel for the softness. If you have blanks left after the competition, handing them out to people who may have trouble sourcing them is a nice gesture. It's also appreciated when organizers allow competitors to keep one of the locks from the competition, so they have at least one lock to practice with after the event. They're also a nice souvenir for first-time competitors and winners alike.

If the competition is part of a bigger, non-lock-related event, starting off with a short explanation may be wise so the spectators have a general idea of what they're witnessing. Perhaps plan a workshop the day before.

Summary

In this chapter, you learned what an impressioning competition looks like, how to train for it, some strategies for success, and tips for organizing your own event. We hope this has inspired you to pick up a file and give it a go. Keep it safe, keep it open, and, above all, keep it fun!

This concludes our exploration of impressioning. Next, in Part IV, we'll introduce you to tools, techniques, and competitions for manipulating safe locks.

PART IV

SAFE-LOCK MANIPULATION

You've likely seen movies where the heroic spy or the dastardly villain nonchalantly cracks a safe. They lean in, their ear close to the dial to listen to the tumblers moving, then give a few confident spins, and voilà: the safe opens. If only it were that simple. While dialing a safe open without knowing the combination, called *manipulation*, is possible for many locks, it's usually not that easy for beginners and amateur hobbyists.

This hasn't stopped the locksport community from adding safe manipulation to the ever-growing list of events as more and more participants expand their skill sets. Plenty of folks are intrigued by the next challenge, and that's exactly what manipulation is all about: each lock presents its own puzzle. Notable events for the locksport crowd featuring manipulation have included LockFest (typically held in Seattle), LockCon (in the Netherlands), and the Czech Lockpicking Championship. Here Matt is manipulating a safe lock at LockFest 2019, where he worked his way to a second-place finish.

But if all safe locks are actually . . . well . . . safe, then how can anyone dial one open without knowing the combination? Before we get into the details of the tools and steps involved in safe-lock manipulation, let's take a brief look at what exactly makes it possible.

Safe Locks 101

Simply put, a safe lock's mechanical design and manufacturing tolerances give us enough wiggle room to open it without the combination. If you've read the chapters on pin tumbler lockpicking and impressioning, you're probably sensing a theme. We'll exploit these factors with our senses of sight, touch, and sometimes hearing to glean clues about the numbers in the combination.

As Chapter 3 explained, the general concept of safe locks is that you turn a dial in a particular sequence to align the components inside the lock, which releases the bolt and allows you to open the safe. We'll break this into a methodical process and then look at ways to streamline it, significantly reducing the steps and the time required, to prepare you for competitions.

While overly complex and so-called manipulation-proof locks are out there, the locks used for locksport manipulation aren't terribly complicated. We'll disassemble them and cover each part in Chapter 13, but the main components are generally the same across brands. The lock on this thick and sturdy safe is a good example of the locks used during training and competitions.

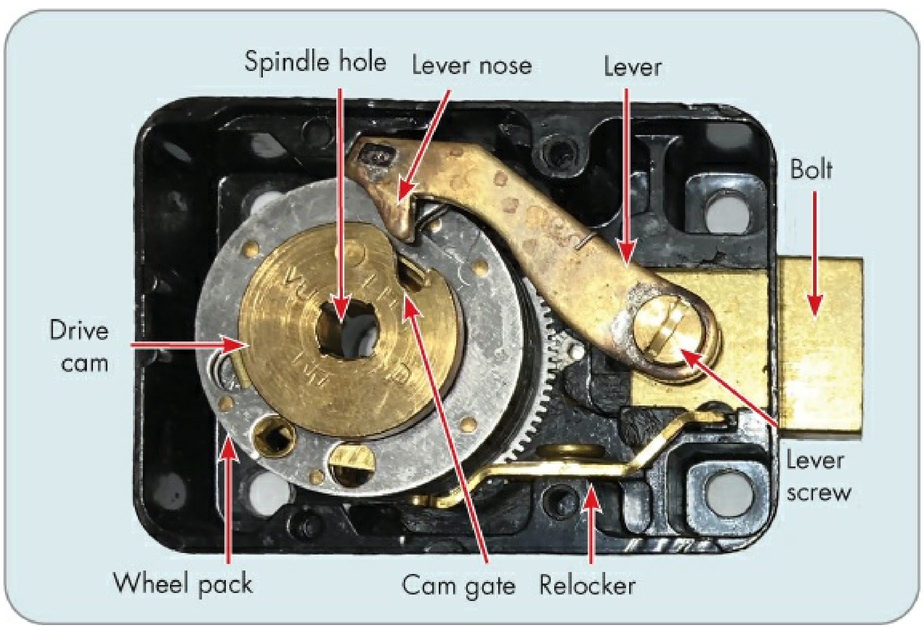
The numbers on most modern safe-lock dials range from 0 to 99. Historically, exceptions have included dials with letters (both upper- and lowercase), a range from 0 to 85, the inclusion of the number 100, the use of a star instead of 0, and more. Thankfully, competitions stick with the standard 0 to 99 *front-reading* dial (that is, the numbers are readable from the front, as shown here), so you won't encounter any of those variations.

While manufacturers make several dial options, for locksport purposes, avoid purchasing top-reading or *spy-proof* dials—those that include an extra ring to limit others' view of the numbers, as shown here. In addition, avoid gold dials, which reflect too much light and can obscure the black index lines.

A safe lock's back cover generally isn't that exciting, as it's usually unadorned except for a manufacturing stamp or two. However, you should always ensure that it's firmly attached when changing combinations or dialing the lock open; otherwise, combinations can be set askew or internal components can jam.

The safe lock's housing also isn't much to look at. It has holes to screw it to the safe, as well as one or two holes that pass into the lock. One is for the dial's *spindle*, the long, threaded screw that extends from the dial through the door and into the wheel post in the lock body. The second is usually a smaller change-key hole, where you insert the change key (described in Chapter 3) to update the combination.

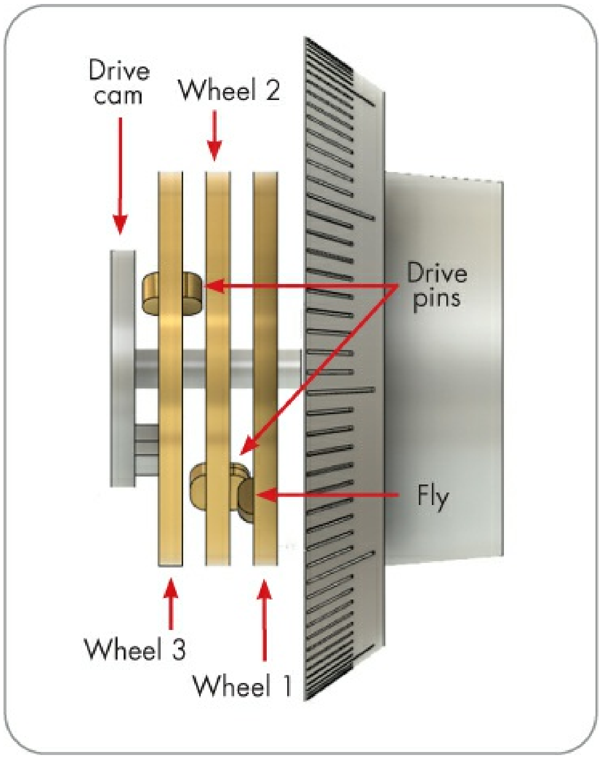
Inside the lock is where the magic happens. Here you'll find the wheel pack, a few springs, the lever, the drive cam, and screws to hold it all together, as shown in this example from S&G.



NOTE

Under typical conditions, the lock's owner has no reason to open it up, but you'll spend plenty of time taking your locks apart to build a better training device and to ensure that you can mount or remount a lock.

Let's go over how these parts interact during the operation of a standard three-number combination lock. When you spin the combination dial, it turns the spindle, which is connected to the drive cam by a spline key. A *drive pin* (a small, fixed protrusion) on the drive cam catches the *fly* (a slightly movable pin on the underside of the wheels) on wheel 3, causing wheel 3 to rotate; wheel 3's drive pin then catches the fly on wheel 2 to rotate it; and finally, wheel 2's drive pin catches the fly on wheel 1 (the wheel nearest the dial, corresponding to the first number in the combination) to rotate it. We'll go over this sequence in more depth in Chapter 13.



When the correct combination is entered, the notches, or *gates*, on all three code wheels line up, allowing the fence attached to the lever to drop into the groove they create. The lever is connected to the bolt, and when you spin the dial again, the nose of the lever catches on the cam gate, causing the bolt to retract and the lock to open.

You might have noticed four pairs of letters stamped on the drive cam. These refer to the orientation of the bolt when you're viewing the lock from the back, with the *opening index* (the mark where you stop spinning the combination dial) pointing upward. The options are as follows:

- RH (right horizontal)
- LH (left horizontal)
- VU (vertical up)
- VD (vertical down)

You set the bolt orientation by inserting the spline key in the appropriate position on the drive cam for your mounting scenario. The manufacturer's guidelines usually provide specifications.

The Basics of Safe-Lock Manipulation

Manipulating a safe lock relies on finding and measuring the *contact points*, the area on each side of the drive cam that the lever nose touches, while also contending with manufacturing and mechanical limitations that can obfuscate the clues you're trying to find. As mentioned earlier, wiggle room in the manufacturing tolerances is what makes lock manipulation possible, but sometimes it can be inconsistent and actually prevent an easy opening.

A second challenge is the sheer number of steps involved in the process; safe-lock manipulation has a steep learning curve. You'll be repeatedly spinning dials and recording minute variances in your number readings, and these steps must be done with precision. But the good news is that the process gets easier and much, much faster as your eye for variations develops. Eventually, you'll be able to trim the number of steps significantly, or even skip some altogether given the right conditions. When all these factors align in your favor, you can achieve some remarkably fast opening times.

NOTE

What's "remarkably fast"? You might hear of three-minute openings in competitions, but this is often due to a combination of an extremely skillful manipulator and good luck. A dozen minutes is more realistic for some on a good day, or several locks in an hour. Most competitors at SAFETECH, the annual convention of the US Safe & Vault Technicians Association, open the first lock under the 20-minute mark. Regardless, if you put in the training, even working a little slower and more methodically, you'll be able to open within reasonable competition times.

Let's break this down so you can get some good news out of what might be feeling like a daunting task to undertake for the first time. Manufacturers often state that their locks have a million possible combinations. This is true in the sense that each of the combination's three numbers have 100 (0–99) possibilities, or 100 × 100 × 100 = 1,000,000 combinations. However, because of the lever-fence design, the last number in the combination precludes the full use of the dial. Specifically, if the combination of the last wheel is set too close to the point where the lever nose enters the cam gate, the lever nose can get trapped in the cam gate, preventing the bolt from being relocked or the lock from opening altogether.

For this reason, manufacturers specify a *forbidden zone*, the prohibited range of numbers that would position the third wheel's gate too close to the cam gate. Usually, the forbidden zone includes approximately 20 numbers, leaving 85 possibilities for the third combination-dial option. That already brings the options down to 100 × 100 × 85, or 850,000 possible combinations. Even if you were just going to guess your way through, this saves you 150,000 unnecessary attempts.

Next, in your first investigatory efforts, you'll skip around the dial in either 2 or 2.5 increments. That can be as few as 40 stops on a dial with 100 numbers. By trying this on each of the three wheels in the lock, you're now looking at 40 × 40 × 34 = 54,400, a much smaller number of dialing tests to look for clues. That's still way too many options to dial in sequence, but it's a significant reduction from the million possible combinations advertised, and we haven't even talked about what happens when you find clues. Security analyst and researcher Matt Blaze has estimated the number could be as little as 38,720 likely combinations (*https://www.mattblaze.org/blog/nsa_safecracking*). Even better.

Thus, while you might think finding one out of a million combinations is impossible without a miraculous stroke of luck, in the next chapters we'll show you that it's very possible. Safe-lock manipulation is more than just a numbers game. We'll teach you how to find the subtle clues that enable you to dial purposefully and open locks more efficiently.

Our goal isn't to make you an expert safecracker, safe technician, or safe engineer, but with enough practice following the training path outlined here, you'll be opening safe locks quickly and proficiently at your next convention or locksport meetup. Let's dive in, beginning with the tools you need to get started on your safe-lock manipulation journey.

12
SAFE-LOCK MANIPULATION TOOLS

In this chapter, we'll go over the tools and equipment for safe-lock manipulation, starting with the lock itself. We'll discuss several brands of modern safe locks that are readily available and appropriate for manipulating, as well as techniques to make them into better training aids. You'll also learn about other gear and resources that can help you develop your manipulation skills and reduce the confusion that hinders some novices.

Choosing a Lock

This section provides a brief overview of the types of locks currently available so that you'll be able to make an informed decision when you go shopping for your next practice lock. Before we jump into specific model numbers, let's look at how modern safe lock types are classified.

NOTE

Not all safe locks are candidates for manipulation. In fact, many manufacturers produce locks labeled manipulation resistant *or even* manipulation proof. *Manipulation-resistant locks aren't found in competitions, nor are they suitable as training aids, so we won't discuss them further.*

Lock Classifications

In the US, Underwriters Laboratories (UL) Standard 768 covers the classification of mechanical safe locks. Classification is necessary for a couple of reasons. For one, insurance companies demand exacting and measurable standards for safe locks so they can evaluate risk and prescribe minimum security measures. Furthermore, the extra security features found in locks are complex and significantly raise their price.

UL 768 lays out four possible ratings, known as *Groups*, for combination locks; from least to most secure, they are Group 2, Group 2M, Group 1, and Group 1R. To attain any rating under UL 768, a combination lock must meet certain minimum criteria for the mechanism's design and provide at least a million unique combinations.

In Europe, the most common standards are EN 1300 and VdS certification. While none of these standards are directly interchangeable, many Group 2 locks have also obtained a VdS or EN 1300 certification. For our purposes of training and eventual competition, we'll focus on Group 2 locks and their equivalently rated foreign locks.

Group 2

In *Group 2 locks*, the combination dial must be accurate to 1.5 digits or less. This group is considered to have a moderate degree of resistance to unauthorized opens. These locks are the most prolific and usually sufficient to prevent opening by safe-manipulation amateurs. Modern, readily available Group 2 locks include the S&G 6730, LaGard Model 3300, and Big Red Model CDL-3.

Group 2M

Group 2M is a recent addition to the UL 768 standard and indicates a slightly higher level of security against manipulation than the basic Group 2 designs. Group 2M locks provide up to two hours of resistance to expert attempts at manipulation. Generally, Group 2M locks simply include a few of the inexpensive, specialty parts that are also found in fancier Group 1 locks. While not manipulation proof, these locks are more difficult to manipulate using the techniques covered in this book because the addition of these upgraded parts masks the readings we're attempting to get.

Group 1

Group 1 locks offer up to 20 hours of resistance to manipulation by a single expert. This is generally accomplished by adding new features and tightened tolerances, which significantly increases lock costs. These locks are more mechanically accurate, requiring a dial accuracy within 1.25 digits on a three-number combination lock. Additionally, Group 1 locks must also include a spring-loaded piece of metal known as an internal *relocker* to immobilize the bolt if the lock housing is compromised. This is not to be confused with an external relocker, a device added to the safe itself. Internal relockers are also found on most Group 2 locks, and the safes to which the locks are attached often have external relockers as well.

Examples of Group 1 locks include the S&G 8400 series locks, which use an additional knob mechanism in the center of the dial, and the 8500 series locks, which use an accelerator spring mechanism to hide your contact-point readings and frustrate your manipulation attempts.

Group 1R

Group 1R locks are the same as other Group 1 locks except that they resist decoding attempts using X-ray or similar radiological imaging techniques. (Think *R* for *radiological*.) If you use

X-rays on a lock that has no protection against it, you can see the shape and position of the wheels inside. By dialing the lock to a specific state and then looking at these positions, you can deduce the combination that opens the lock. This provides quick entry but requires specialty equipment that obviously isn't used in locksport. Some electronic safe locks are also included in this group because they have well over a million possible combinations, but again, electronic locks aren't included in safe-manipulation locksport events.

To prevent or obscure X-ray imaging, Group 1R locks may use shielding (such as lead) or X-ray transparent materials like certain types of plastic, such as Delrin. The S&G 8430 lock is an example of a Group 1R lock.

Again, while some of these locks are specifically designed to stump manipulators, we'll focus on Group 2 locks because few people would want to participate in a competition that could take 20 hours, nor could we safely run an event if everyone were lugging around X-ray machines! Let's look at some of our specific recommendations from Group 2.

Lock Recommendations

Each lock brand has its own pros and cons, which we'll lay out here so you can choose which option best fits your requirements and circumstances. These manufacturers offer several model variations, some purely cosmetic and others more structural. Yet all of them operate generally the same way, and you can employ all the methods described in these chapters with any of them.

S&G 6741

Because of its low price point and ready availability, the *S&G 6741* is an easy practice lock recommendation (Figure 12-1). Because this lock is made of inexpensive components, you should be able to find it cheaper than other S&G locks, and you won't be upset if you break it. Sometimes these locks are sold inexpensively in new or like-new condition on online auction sites, having just been pulled off new safes to be replaced with an electronic lock at the customer's request. That said, a lack of quality materials used in the lock's construction can sometimes make for inconsistent manipulation results.

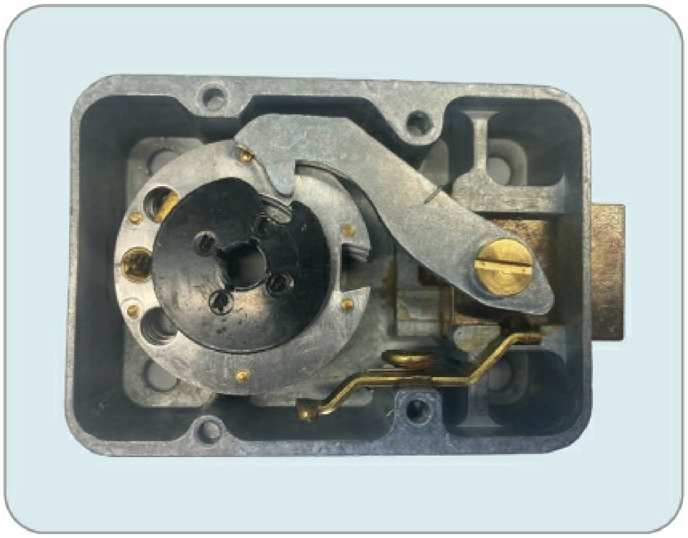


Figure 12-1: In the affordably priced 6741, S&G saves some expense by reducing the overall amount of brass used and stamping only one letter for each direction on the drive cam.

This economy-class model doesn't have the greatest reputation from safe technicians because apparently it doesn't withstand the vigor of commercial applications. However, because you're just training with these locks and don't have to worry about locking yourself out, and because we'll teach you ways to make any helpful modifications later, it's still a viable option if you're on a tight budget.

S&G 6730

The *S&G 6730* is as good as it gets for a Group 2 lock, and it's seen universally at competitions. One caveat is that S&G locks and their parts are often 50 percent more expensive than other brands. Also, they have black dials with white index lines that occasionally are painted sloppily.

> I just sampled 30 new ones. One was a distracting mess, and one was a little light on the paint. I know that sounds nitpicky, but when you're trying to learn by eyeballing tiny changes in alignments, a smudge can be frustrating.
>
> —BANDEATOZ

This lock has long been the industry standard. If it's in your price range, absolutely start with an S&G. Make sure to buy it from somewhere that allows returns, just in case. If you purchase one with a poorly painted dial, you can then exchange it for one that's more legible.

LaGard Model 3300

The price point for the *LaGard Model 3300* often can't be beat. If you're going to modify a lever (which you'll learn about in Chapter 14), this is the easiest lock to do it with. Also, the index lines are always clean and crisp. If you want to make your own cutaway, generally you'll see significant savings with a LaGard; if your experimentation should go amiss, replacement is less costly than for many other brands.

On the other hand, and this may sound strange, but LaGard locks seem to be the loudest to manipulate. This excess noise may distract you from getting accurate readings at first. Some excess movement in the wheels also could introduce confusion when you're just starting out. We'll show you how to test for and deal with this in Chapter 13.

Big Red Model CDL-3

The *Big Red Model CDL-3* is a wonderful, less-expensive clone of S&G's lock. The red wheels look sharp in a cutaway—there's no need to hide something that flashy inside the lock housing!

Many Big Red dials have a rubber coating. It's gentle on the fingers when you put in a few hours of dialing, but some people argue that it also lessens the feel of the contact points. The lock housing is a little thicker than some other lock bodies, but modifying it with a Dremel tool is still manageable. Spare parts to modify this lock may be harder to acquire, as Big Red has a much smaller market share than the other manufacturers listed.

SPARROWS Challenge Vault

The release of the *Challenge Vault kit* from SPARROWS has gone a long way in increasing both the number of folks who want to take a crack at learning manipulation and the availability of a functioning, affordable safe lock to train on. The other major benefit is that all the work has been done for you. The tapered fence on several of the levers supplied with the kit makes this a great training device (see Figure 12-2).

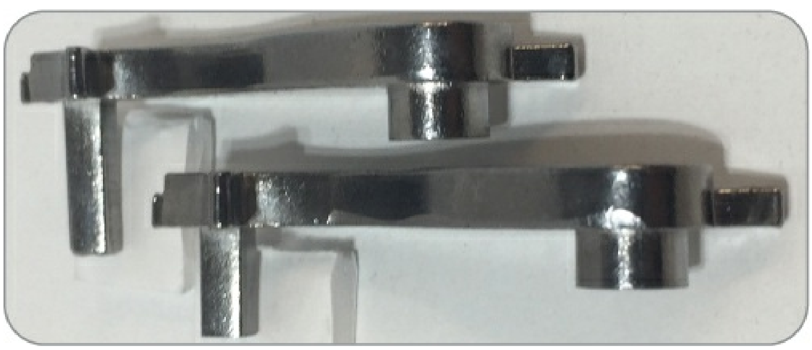


Figure 12-2: The inclusion of multiple lever arms, each with a different fence, is the best part of the Challenge Vault and can greatly aid in the learning process.

The main disadvantage of this option is that you can usually get a better manufactured lock for the same price point. The SPARROWS lock is essentially a slightly disappointing knockoff of the S&G 6730. It works, but the few samples we tried didn't shine.

The kit also doesn't provide a cutaway view, which can be helpful when you're learning to move only certain code wheels. We'll show you how to put together a better training lock, likely for a lower price, in "Making Your Own Cutaway Lock" on page 228.

Lock Sources

You have a few options for sourcing safe locks. The major online auction sites usually have several up for bid at any given time. If the seller can guarantee that all the parts are there, a used lock is often a great deal.

Most of the locksmithing supply companies are reticent to sell to the general public, but some have a small Amazon presence. Keep in mind that some Amazon sellers charge a large premium and, if some reviews are true, they might also be selling incomplete locks. Beware of used lock sales with photos of extra holes in the lock body! These locks may have been drilled open, and you don't want to risk unnecessary burrs or other damage keeping the parts from operating smoothly.

Regardless of where you decide to purchase, before you bid or place your order, make sure to look up the model number's specifications, including UL group, on the manufacturer's page, lest you mistakenly purchase a Group 1 or 2M lock. Also note that front-reading dials are more comfortable to use when you're dialing at a desk or table, whereas top-reading (aka spy-proof) dials can be seen only from a narrow point of view, forcing you into an awkward position.

Gathering Other Safe-Lock Manipulation Supplies

Once you've decided on a lock that best fits your budget and needs, you'll need a few more supplies to round out your safe-lock manipulation toolkit.

Lock Mounts

You don't need to have a spare safe door sitting around to mount your lock. Several portable, commercially available options are available for mounting (see Figure 12-3), or you could build or 3D print your own mount. Wood is user-friendly: with simple tools and an old scrap piece of lumber, you can drill a small hole for the spindle, thread in some screws, and be good to go.

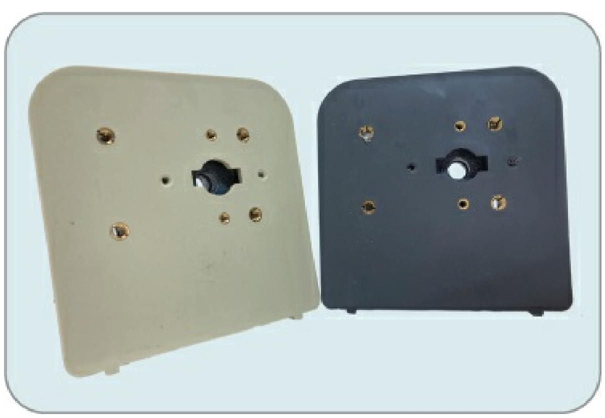


Figure 12-3: Manufactured mounting options

If you opt for a plastic mount, try to get the ones with threaded brass inserts (like those shown in Figure 12-4) in case you want to remove one lock and mount another. Plastic threads can sometimes be finicky after multiple uses.

If you have a plastic or wooden mount without threaded brass inserts, adding them is an easy retrofit. Options vary, depending on the material you're threading them into, but in the US, you'll need four ¼-20 (M6 in Europe) inserts to mount the lock body and two 8-32 (M4) inserts to hold the *dial ring*, the flat circle on which the dial spins (see Figure 12-4). Generally, mounting a safe lock is a straightforward process, but it does demand exact alignment.

Figure 12-4: Several varieties of threaded inserts used with screws to hold the dial ring and to mount the safe lock

> I understand not everyone has access to a metal shop, but my favorite mount is a small metal one. Some folks can fabricate them with little trouble. I just use an old safe door or safe drawer parts. The use of a metal mount allows me to magnetically attach my amp, aka my "bionic ears."
>
> —BANDEATOZ

Attaching an Amp to Your Mount

While an amplifier isn't required, any assistance in identifying contact points can be an asset. The EZ AMP from Taylor Technologies, shown in Figure 12-5, is an excellent option. According to the marketing specifications, its amplification circuitry is designed to selectively amplify specific sound frequencies associated with safe work while tuning out background noise, resulting in great sound quality.

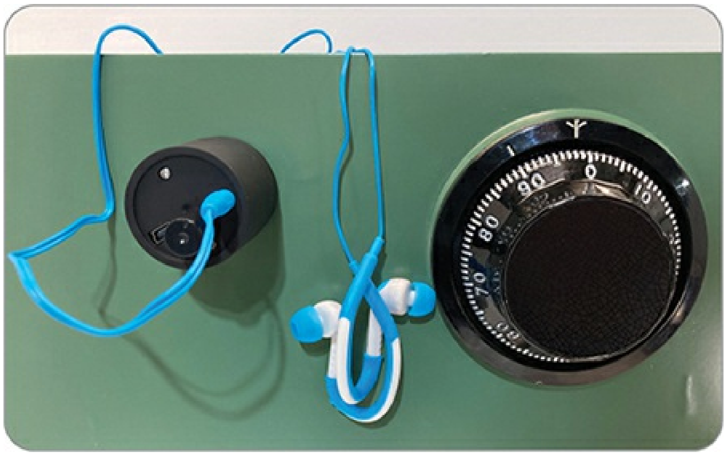


Figure 12-5: This old filing cabinet drawer has been turned into a dialing station—not particularly handy to carry around, but the EZ AMP attaches to this solid metal surface magnetically.

Amplifiers usually aren't allowed in contests (except for use by competitors who are visually impaired), but as a training aid they have the benefit of adding your sense of hearing to the sight and touch you're already leveraging. Again, while an amp is truly a nice-to-have item, it's not a necessity, especially if you don't have a place to mount it. Before you purchase one, learn the manipulation process, practice on several locks, and then decide if you want to try an amp.

Sizing the Lock's Spindle

If you're not purchasing a premounted lock, you'll need a way to cut and file the spindle in order to size it to your specific mount. Spindles are intentionally left long so that you can cut them to size when you install the lock in the safe. A Dremel or a small hacksaw will suffice and make short work of the task. Any metal file already in your possession will *deburr* (smooth out the rough edges) and *chamfer* (add a bevel to) the spindle easily.

Before cutting your spindle down to size, fit the entire lock/dial assembly together and make sure the drive cam is aligned and tightened in accordance with the manufacturer's directions. Mark where the spindle comes out of the drive cam (see Figure 12-6).

Figure 12-6: If you have to mount and cut your spindle to size, assemble the lock first to mark the fit.

WARNING

Don't attempt to cut your spindle while it's assembled in the lock. If you do, your cut will be off and you run the risk of burring something important.

Then follow these steps:

1. Remove the spindle from the lock.
2. Before you cut your spindle, temporarily attach your drive cam again. Spin it down well below your cut mark and close to the dial.
3. Cut the spindle off at your marked location (see Figure 12-7).
4. Deburr and chamfer your cut with a file. Now spin your drive cam back off. Any threads that were bent during cutting will straighten when the drive cam passes them.
5. Reassemble your lock. Spin the dial back off one turn to match the spline in the spindle with the appropriate orientation on the drive cam (most likely RH). Lightly tap in your spline key, facing the direction specified in the manufacturer's instructions.

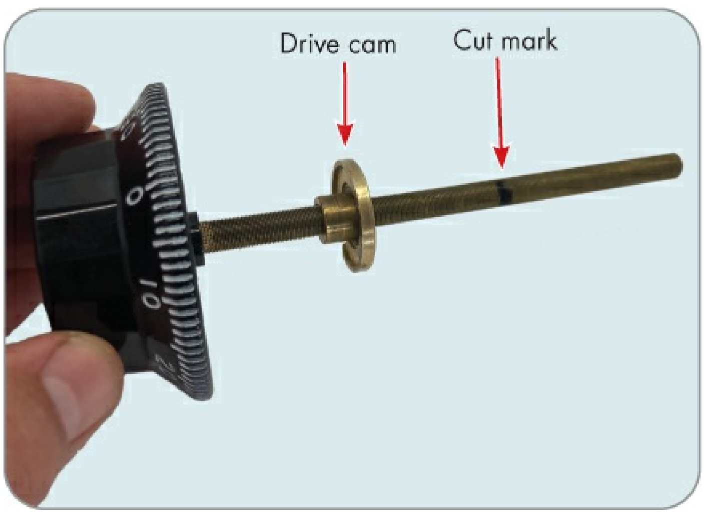


Figure 12-7: Before cutting your spindle, screw the drive cam back down below your cut mark.

Graphing Charts

Generally considered the foundation of the manipulation learning process, *graphing charts* allow you to plot your contact points as you work. These charts will help you keep track of your safe-dial reading during manipulation and also work to refine your reading of the minute changes you are looking for. You can choose from the many available commercial options, make your own, or use a free version shared online by members of the locksport community. In Chapter 13, we'll go over exactly how to use them.

SPARROWS shares both the Vault instructions and its printable graphing chart for anyone to download. A simple internet search will pull up the latest instruction book, including the graph as a PDF file.

The folks at Locksmith Reference share several mechanical safe-lock instructions as well as versions of their graphing charts, which have increments in both quarters and fifths for your charting pleasure.

Deviant Ollam and the great team over at the CORE Group also provide some fine manipulation charts on its Safe Manipulation page *https://enterthecore.net/safe-manipulation/*. They use charts with increments in tenths for a more nuanced approach (see Figure 12-8).

Figure 12-8: The CORE Group's graphing chart

Lockmasters and MBA USA provide some unique options. Lockmasters, which essentially invented teaching manipulation, offers a graph that has the feel of a detailed flowchart (see Figure 12-9).

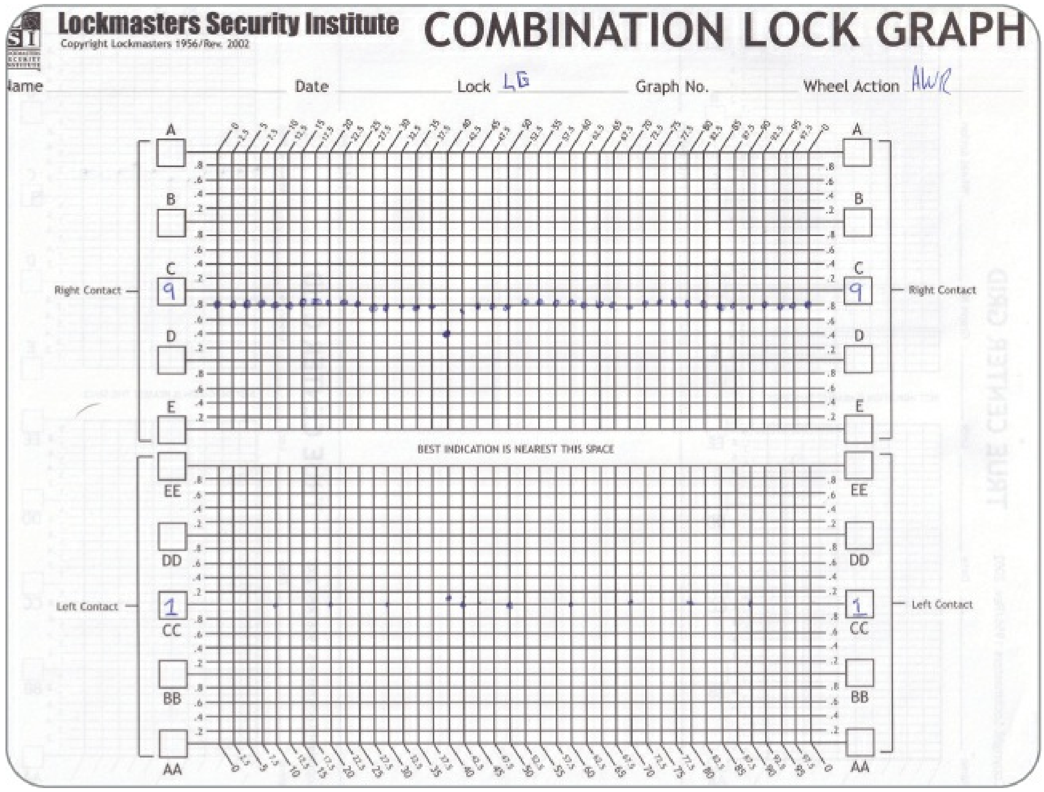


Figure 12-9: This Lockmasters chart breaks the increments into fifths.

However, MBA's laminated, reusable, circular chart paints a detailed picture that's hard to argue with (Figure 12-10).

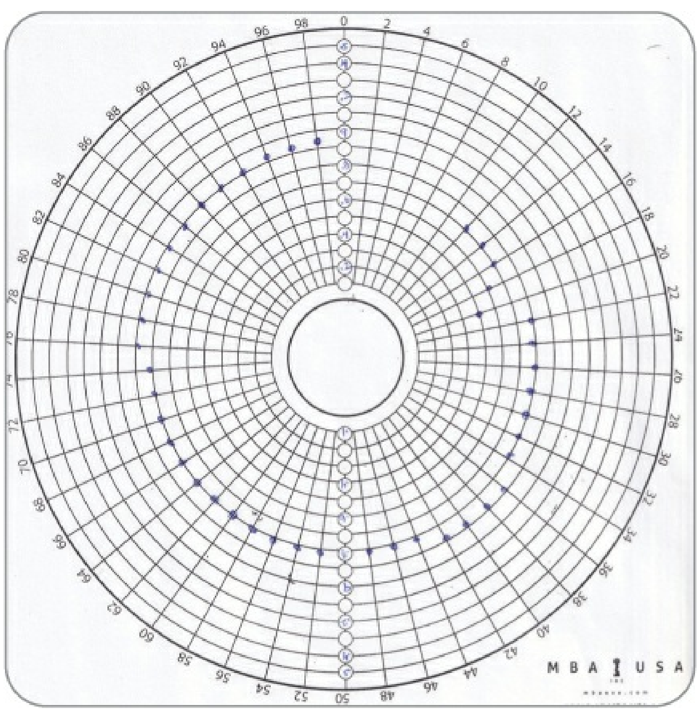


Figure 12-10: The circular graphing chart from MBA USA

On your first spin around the dial, measuring contact points in quarter increments can be faster and easier, reducing the number of nuanced decisions that can slow you down when you're first learning manipulation. But once you've gotten the hang of finding and documenting contact points, the charts divided into tenths offer greater fidelity, especially for troublesome locks. We recommend getting both, since you'll put them to good use over your learning journey—that is, until you're running full speed without them and crushing the competition.

Index-Line Stickers

Sometimes a visual aid can help you get more accurate readings for your contact points, particularly when the lines on the dial are chunky or sloppily painted. If applied properly, index-line stickers can be a great asset.

> My only issue with stickers is with how I use them. My imprecise application can often defeat their purpose.
>
> —BANDEATOZ

Some folks make their own stickers, and others use the tried-and-true commercial options. The simplicity of Fine-Line dial indicators by Taylor Technologies (Figure 12-11) is unmatched.

Figure 12-11: Fine-Line dial indicators by Taylor Technologies highlight subtle changes and can make all the difference in your search for clues.

Lockmasters Read Eze stickers are a bit more complicated but can be especially helpful for getting precise readings (Figure 12-12).

Figure 12-12: Lockmasters Read Eze stickers help define the increments between these blurry lines.

These stickers are totally optional; if you have no trouble manipulating safe locks without them, feel free to skip them.

Performing Lock Disassembly and Assembly

We highly recommend owning a cutaway lock so you can see the wheels moving instead of trying to picture what's happening inside the lock. If you already own a cutaway lock or have no intention of making one (as we'll describe in the next section), you shouldn't need to disassemble your lock unless you want to modify the lever to give you specific clues during your practice (see Chapter 12 for instructions).

Removing the lever is as simple as removing the back cover, the lever screw, and one spring. All you need is a Phillips-head screwdriver for the back-cover screws and a flathead screwdriver for the lever screw. Figure 12-13 shows an example cutaway from Big Red.

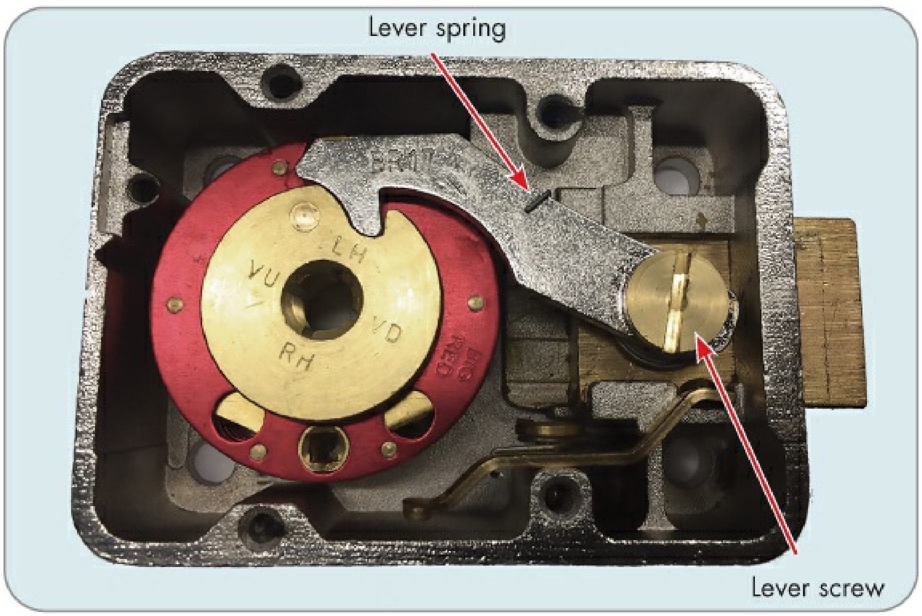


Figure 12-13: The lever screw and spring in a Big Red lock

To remove the lever in the Big Red lock, you simply unscrew the lever screw and unhook the lever spring. The other end of the spring hooks inside the lock bolt in a tiny hole or groove, and the center of the spring wraps around the lever screw's bushing.

SPARROWS levers work a bit differently in that the spring attachment point fits inside a hole in the lever versus being hooked in, but otherwise they're the same as Big Red and S&G.

LaGard doesn't have a lever screw but instead uses the lever spring to secure the lever directly to the bolt (see Figure 12-14). You'll have to undo the lever spring near the top of the lever first, and then rotate and slide out the spring.

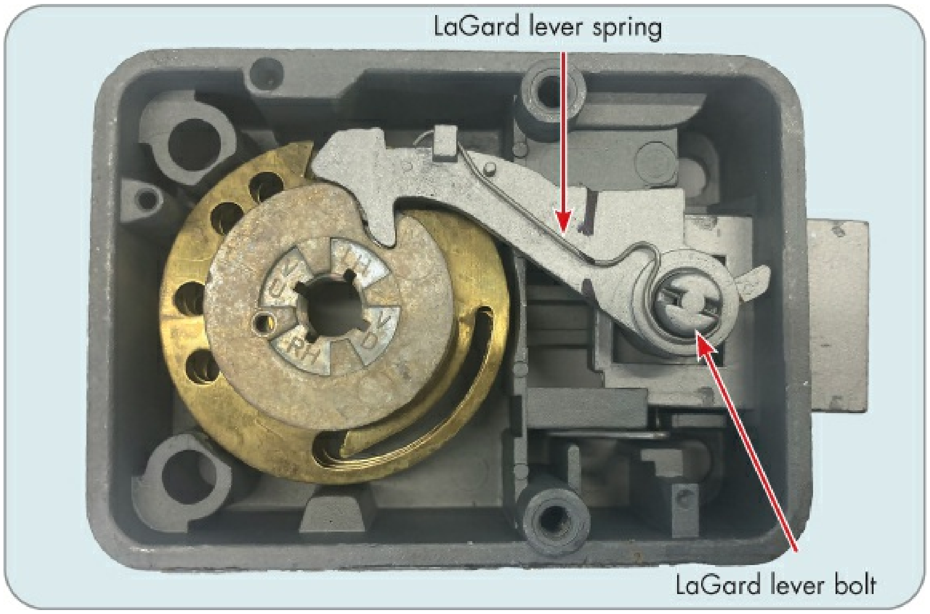


Figure 12-14: The LaGard lever attachment differs from that of other manufacturers.

You have only two things to worry about during disassembly. First, the retaining washer, or Spirolox washer, can be a pain to take on and off until you've mastered the technique. Try lifting the lead edge, then working it around in the appropriate direction (Figure 12-15). A small screwdriver, nail, or ice pick will work. Second, the lever spring usually has some kind of turn to keep you from bending it out of shape.

With both steps, take your time and don't force anything. Also make sure you're doing this in an appropriate workspace—you'd hate to lose a small washer or not have space to lay the parts out for easy reassembly later. Consider putting the washer in a resealable clear bag, just to be sure it can't go far.

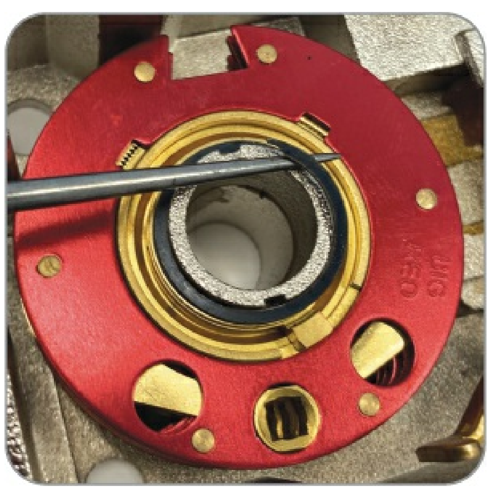


Figure 12-15: Removing the retaining washer with an ice pick or similarly pointed tool

For reassembly, simply put everything back in the correct order. Keep in mind that two of the wheels are interchangeable, as are two of the flys, so make sure you don't put the odd one out in the wrong spot.

NOTE

The Sargent and Greenleaf Mechanical Safe Lock Guide *mentioned in "Using Other Resources" on page 234 is a must-own, and its exploded view of the wheel pack will definitely help you with reassembly. Even if you have a different manufacturer's lock, about 95 percent of the steps are the same.*

Unlike wheels 2 and 3 (see Figure 12-16), wheel 1 doesn't have a fixed drive pin on the bottom, as it rides against the lock body and has no room for one.

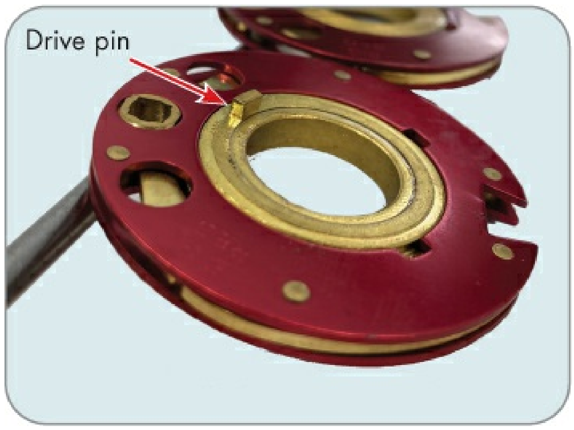


Figure 12-16: Because this wheel has a protruding fixed drive pin, you know it must be wheel 2 or 3.

Wheel 3's fly (the topmost fly) protrudes to ensure that it will be caught by the cam's drive pin (see Figure 12-17).

Figure 12-17: Wheel 3, the one closest to the drive cam, always has a protruding fly, while all the other flys are flush with the wheel.

Once you have your flys and wheels correct, the last thing to remember is your spacing or isolation washers, found between each wheel. You'll also want to have a change key, used to set a new combination for the lock. While new locks usually come with a change key, a used lock might not. Make sure you get the correct key for your lock (see Figure 12-18 for some examples). A few, especially the S&G clones, can often use the same key, but S&G and

LaGard keys differ significantly.

Figure 12-18: From top to bottom: S&G, LaGard, and Big Red change keys

Making Your Own Cutaway Lock

Having a lock that you can see into during your learning process can be invaluable. During manipulation, you'll find yourself not just dialing combinations, but dialing to specifically include and exclude wheel locations you're testing. This process can be tiring for the mind *and* the wrists, so get a cutaway lock.

> Some locksporters fabricate a clear acrylic back cover for their lock to allow them to see inside, so that's another option you might want to explore. I can be a little rough on plastic, so I usually stick with the cutaway method.
>
> —BANDEATOZ

You might be apprehensive about cutting into a newly acquired safe lock, but with a few simple tools, you can easily and quickly produce one that will more than meet your needs—and at a significant cost savings over some of the machined cutaways available. Let's look at a couple of examples of those first. Figure 12-19 shows a LaGard lock cutout that gives us a view of the fence when it interacts with the wheels as well as the lever nose when it interacts with the drive cam.

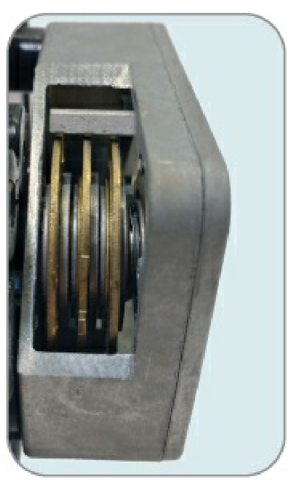


Figure 12-19: A LaGard side-view cutaway lock

What's nice about this cutaway is that it leaves some of the lock body intact, where the side-view hole was cut. This provides a surface you could affix tape to if you wanted to obscure some of what's going on inside the lock to better focus on a specific area.

Figure 12-20 shows a back-cover cutaway from LaGard. It keeps all the important parts uncut but still affords you a view of the wheels, lever nose, and cam gate.

Figure 12-20: A LaGard back-cover cutaway lock

Figure 12-21 shows another example from Big Red, this time a side-view cutaway. This is likely something you could replicate with a hacksaw or flat file.

Figure 12-21: A Big Red side-view cutaway

And finally, the Big Red cutaway in Figure 12-22 is another back-cover version, but with the cutout shifted to the left edge. This displays the shiny red code wheels to full effect.

Figure 12-22: A Big Red cutaway lock with the cutout on the left edge of the back cover

Having access to premanufactured cutaway locks, 3D-printed cutaway back covers, or a machinist shop can make them easier to acquire, but a DIY version requires only the simplest of tools: a Dremel or any small rotary tool with a cutting wheel, a dollar store hacksaw, and eye protection in case of flying parts. Admittedly, the cutaways won't be as cleanly cut as their manufactured counterparts, but they'll be perfectly functional.

You don't need to disassemble your lock any further than what's shown in Figure 12-23.

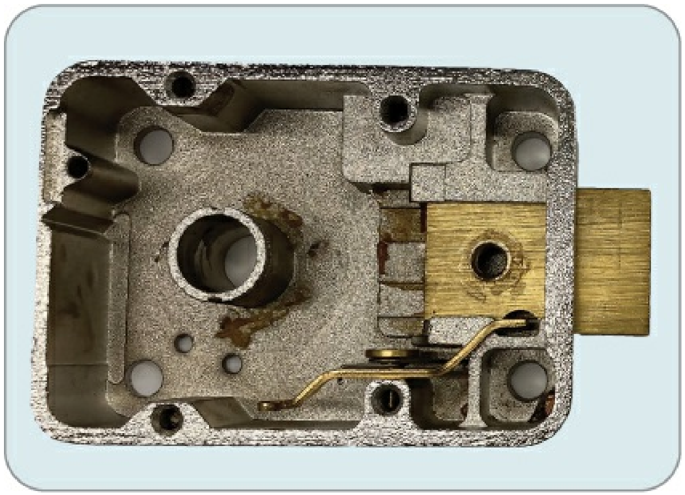


Figure 12-23: A disassembled lock ready for cutting

As you can see, you want to remove the wheels and lever (to avoid damaging them), but you can leave the relocker and bolt intact.

Now you can use your rotary tool to start cutting, as shown in Figure 12-24. (This example shows some overcutting, but it turned out fair enough.)

Figure 12-24: Making your first cuts

You can cut off a section of the back cover, being careful to leave the change-key hole and at least one screw hole, as well as enough of the back cover to keep the internal relocker in check. Using a Sharpie to first mark up the cutting area and spots to avoid can be helpful (Figure 12-25).

Figure 12-25: Cutting the back cover, being careful to avoid the outlined areas

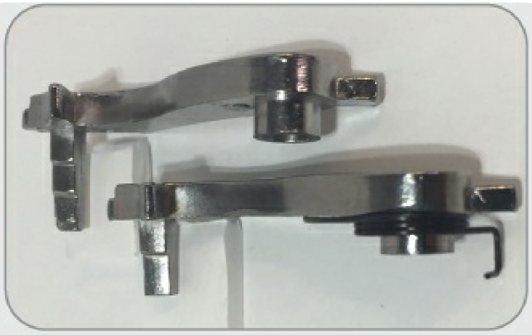
Figure 12-26 shows the finished result.

Figure 12-26: A little beat-up-looking but fully functional DIY cutaway lock

MODIFYING THE LEVER

Modifying the safe-lock lever is a simple, optional way to force a specific wheel to interact with the lever's fence in order to verify which wheel is indicating. During the learning process, this modification can save you time and steps, which you can always add back in by replacing the modified lever with an unmodified one.

The SPARROWS Challenge Vault training lock shines in this area. As you can see here, it includes a lever with a shortened fence (left) so you can get an open with a fraction of the work, and an indented lever (right) to ensure that it contacts a specific wheel inside the lock.



Some manipulators suggest adding a slight bend to the fence to make it indicate on a specific wheel. However, fences can be fragile and frequently break or come unsoldered when you try to bend them. Instead, you can file them down to ensure that they make contact at the location you want. You don't need a fancy milling machine to accomplish this; a simple hand file or rotary tool will do the trick. This lever has been modified with two progressive steps to force wheel 3 to indicate first.

You can mark the fence with two black dots indicating the approximate space between the wheels, so you'll know where to remove some of the metal on the fence. Here the fence has been *terraced* with a rotary tool. The fence is currently touching wheel 3; if the fence drops into wheel 3's gate, wheel 2 will indicate next.

LaGard locks, with their skinny wheels, facilitate the imprecise work of hand filing or rotary-tool grinding and are the most forgiving if you make spacing errors. Regardless of the lock brand, you'll need to remove very little metal from a fence.

Setting the Combination

Before you begin the safe-manipulation process, you'll need to set the lock's combination. Although not technically a requirement, having a friend or two available to help is a good idea. Sure, you could always set your own combination in accordance with your lock manufacturer's instructions—but then you would know it. That would almost certainly throw off your manipulation practice, as you'll be anticipating your next clue. While training, going in without any idea of the combination is best, and doing that is easier if you have assistance. Getting someone to join you on your dialing journey also allows both of you to bounce your understanding of an idea or technique off each other.

If you opt to go it alone, there's a way to set the combination without knowing it. Generally, to dial open a combination lock, you spin the dial around four times in one direction, three times in the other, two times back again, and then one final turn in the opposite direction until it opens. Setting a combination without knowing it involves just the first three steps of that process.

First, align the change-key holes and insert the change key. Turn the key 90°, and *without looking* (you can use tape if necessary, as shown in Figure 12-27), give the dial a handful of spins in any direction to "scramble" it. Then—still no peeking—give the dial eight half spins to the left. These half spins equal about four full spins but spare you from having to do any wrist acrobatics while the lock is turned away from you. Next, give the dial six half spins to the right, then four half spins to the left. Stop spinning.

Turn the change key back 90° and remove the key. Give the dial a final scramble spin and then you're free to look. This process is almost like setting the combination the usual way. In the worst case, if something is off, you can simply remove the back cover, align the change-key holes again, and repeat the process.

Figure 12-27: With the help of a little blue tape, you can still access the change-key hole to reset combinations while avoiding the temptation to sneak a look.

Using Other Resources

Finally, you might want to check out the following helpful references before you begin the hands-on process of safe-lock manipulation:

Sargent and Greenleaf Mechanical Safe Lock Guide

This is updated periodically but a worthwhile resource no matter the version. It is available from S&G's website (just search *mechanical safe lock guide* from *https://sargentandgreenleaf.com*) or search online for *book_mech_locks.pdf* to bring up lots of hits. This guide includes instructions on dialing, changing the combination, mounting the lock, and detailed diagrams that will help you reassemble your locks properly. Although it is brand specific, the operations and assembly principles also apply to other brands' safe locks. Plenty of commonalities exist across all combination-safe-lock manufacturers, so if you understand one, you'll know what to look for in others.

NOTE

Although the mechanics of safe-lock manipulation are fundamentally the same in every one of the references that follow, each author explains it their own way and emphasizes different aspects based on what they think is most important. If you're confused by any of this book's explanations, see how these other folks have stated it. Think of these recommendations as additional tools in your toolbox.

Matt Blaze's "Safecracking for the Computer Scientist"

This 2004 paper is available from Blaze's website at *https://www.mattblaze.org/papers/safelocks.pdf*. He does a fine job breaking down how everything works, giving plenty of definitions, and keenly emphasizing the need to practice to learn the techniques. A couple of standouts are his suggestion of using one-eighth increments of measurement for charting (versus the standard quarters, fifths, and tenths) and his simple back-cover cutaway—his use of a simple drill hole makes for a smooth-looking machined cut.

Jared Dygert's *Safecracking for Everyone!*

A few years ago, BandEAtoZ watched this energetic and passionate young man give a lock manipulation class at a large conference, but was unaware that the man had already produced a simple, 45-page manipulation book when he was younger. While obviously self-published, the book does more than cover the basics and is filled with LaGard locks, making it a nice complement to the S&G safe lock guide recommended earlier. Dygert loves to use color-coding to group ideas and doesn't shy away from graphing photos and detailed tips. Like Blaze, he suggests charting increments of one-eighths. *Safecracking for Everyone!* is available from Amazon and is also linked from Dygert's YouTube page (*https://www.youtube.com/@lockmanipulator*).

SPARROWS Challenge Vault manual

SPARROWS also shares the manual for its recently released Challenge Vault (*https://www.sparrowslockpicks.com/pages/vault-manual*). While the manual focuses on using modified components to force a reading, the rest of the manual procedures are just as applicable to other openings. The manual also comes with a hand graphing page.

Robert Sieveking's *The National Locksmith Guide to Manipulation*

Back in the late '80s, *National Locksmith* magazine produced this top-notch book on manipulation. Sadly, the magazine closed down in 2016, but print copies of the book can frequently be found for sale online. Sieveking includes study questions at the end of each chapter to ensure you're following along. A digital version is available on the Internet Archive; simply search the book's title from *https://archive.org*.

Summary

In this chapter, we gave you an overview of the tools—most importantly, the lock itself—and techniques you need to practice safe-lock manipulation. You learned the basics of lock disassembly and lever modification, as well as how to make your own cutaway, reassemble the lock, and set the combination.

In the next chapter, you'll put your practice lock through its paces as you start manipulating and learn how to chart your readings.

13
SAFE-LOCK MANIPULATION STEP-BY-STEP

You have your lock mounted and set with an unknown combination, and now you're ready to learn how to open it. In this chapter, we'll walk you through each step of finding and charting the clues that will enable you to determine the safe's combination.

Here's the general process you'll follow:

1. Graph to get clues to one of the numbers in the combination.
2. Use those clues to find True Center, the exact number in the combination.
3. Run High Low tests to determine which wheel the number corresponds to.
4. Search for clues to another number in the combination, and repeat steps 2 and 3 to determine which wheel it corresponds to.
5. Use the brute-force technique to determine the final number in the combination and open the safe.

As you work, you'll be keeping meticulous notes on graphing charts. This process might sound daunting, but remember, the more you dial, the easier it will get. If it were as difficult as it seems to beginners, no one would be spinning open locks for a living or at competitions!

Before we begin, keep the following points in mind:

- If you aren't using a cutaway lock to follow along, you'll need a screwdriver to remove the lock's back cover and the correct change key to complete the steps listed here. Keep in mind that if your lock has an internal relocker, it won't let you retract the bolt with the back cover off even if you've dialed the right combination.
- Instead of *clockwise* and *counterclockwise*, we'll refer to dialing either *right* or *left*, respectively (see Figure 13-1). Additionally, when we write *3× left to 50*, that's shorthand for dialing left three times to 50; that is, you dial left, passing 50 twice, and then stop when 50 aligns with the opening index for the third time.

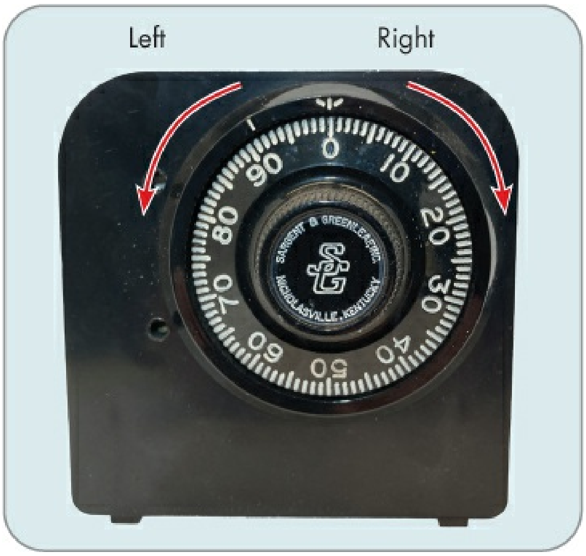


Figure 13-1: We'll refer to turning your dial counterclockwise as dialing left, and to turning it clockwise as dialing right.

Let's get started!

Dialing with Precision

When you're trying to find the right numbers to open the safe lock, what you're really trying to find is the gate (the notch or open space) on each wheel. Let's look at some examples to see what this means.

Design Tolerances

First, set your combination to 20-40-60 in accordance with the lock manufacturer's instructions. (When changing your combination, remember to use the *change index* instead of the opening index; use your finger or some tape to cover the opening index if needed.) Dial the lock open a few times to ensure that the numbers align with the opening index and are set perfectly correctly.

Now, dial the combination 20-40-60 again and stop there—don't make the last turn right to retract the lock's bolt. Viewing your cutaway or your lock with its back cover removed, notice how the wheels' gates are aligned perfectly under the lever's fence. If they're not, you either dialed imprecisely or were looking at the opening index instead of the change index when you set your combination. Redial your lock carefully, looking at the wheels and the gates, and correct the problem before continuing.

Next, dial the following combinations and see if they open your lock.

19-39-59	20-39-59	21-39-59
19-39-60	20-39-60	21-39-60
19-39-61	20-39-61	21-39-61

19-40-59	20-40-59	21-40-59
19-40-60		21-40-60
19-40-61	20-40-61	21-40-61
19-41-59	20-41-59	21-41-59
19-41-60	20-41-60	21-41-60
19-41-61	20-41-61	21-41-61

How many variations opened your lock? With some vigorous oscillation, our test lock opened with all 26 additional combinations. This means we have a lot of wiggle room, or space, we can take advantage of to manipulate the lock. The space is a result of design tolerances rather than mechanical imperfections, and these tolerances are significantly reduced in Group 1 locks, which is why they're not used in competitions.

As you can see from this example, getting a lock open is more about finding the right space than the right number. But we still need the numbers on the dial to help us track where those spaces are.

Wheel Rotation

Next, you need to set your combination to All Wheels Right (AWR) 50. This means when setting your combination, you spin the dial right at least four times, then stop when the 50 is under the change index. Now turn and remove the change key. Give the dial a few fresh spins, dial AWR 50, and stop on the opening index. Don't make the last turn right to retract the lock's bolt. Again, all the edges of the wheels' gates should be aligned perfectly straight under the lever's fence. If so, good job on both your combination setting and your dialing.

Now, using the same method in the opposite direction, dial All Wheels Left (AWL) 50 and stop. Notice that the gates are now in a stairstep pattern. Why? For now it suffices to say that dialing left or right has a specific action. Eventually, you'll be rotating a wheel in a direction it wasn't moving when you set the combination, and you'll need to expect and be able to interpret the small offsets that result. The takeaway here is that numbers can be a little tricky to align with spaces, depending on which way you're turning the dial, and you won't always be dialing in the same pattern in which you set the combination.

Remember that when you spin the dial, the drive pin on the drive cam catches the fly on wheel 3, causing wheel 3 to rotate; this is known as *picking up* the wheel. Wheel 3's drive pin catches the fly on wheel 2 to rotate it, and wheel 2's drive pin, in turn, catches the fly on wheel 1 (the only wheel without a drive pin) to rotate it. As you turn the dial during manipulation, you'll be able to feel and hear the contact between the drive pins and movable flys, giving you clues about how to proceed. Let's take a closer look at this.

Reset your combination to 20-40-60. Then, dial left four times and stop at 50; your goal is to have every wheel picked up by the drive cam and moved to 50. Watching from the back of your lock, dial right. The first thing you should see moving is the drive cam. Keep watching and keep dialing right. Eventually, you should see wheel 3 move. Dial right until you see wheel 2 move, and continue until finally you see that wheel 1 is also moving. The drive cam and all three wheels are now moving right (although it looks like left because you're viewing it from the back of the lock). Stop your right spinning. Dial left, and note that the same sequence happens again.

If you had the drive cam and all three wheels moving right, why didn't they all move left when you changed direction? This is a result of the drive pins for the drive cam, wheel 3, and wheel 2 having to make an almost full rotation before they pick up the movable fly on the next wheel. (Wheel 1 doesn't have or need a drive pin; not only is there no room for one, but there's no additional wheel for it to pick up and move.) This rotation requirement has two significant implications.

First, this is why you have to dial four times left for the first number in a combination. You don't know where the wheels were last, so dialing four times left will ensure that you pick up wheel 1 and park its gate under the fence (that is, three rotations to pick up each wheel and then a fourth to set the first number in the combination).

The same goes for dialing three times right for the second number in a combination. Wheel 1 is already parked in its correct spot after you spin four times, so when you change directions, the cam needs to make a full trip around (rotation 1) before it picks up wheel 3. Then, wheel 3 needs to make a full trip around (rotation 2) to make contact with and pick up wheel 2. Finally, you dial wheel 2 to its corresponding number in the combination (rotation 3).

Dialing two times left for the last number in the combination is much quicker. You change directions, and the drive cam makes one full turn to pick up wheel 3 (rotation 1), and then you dial to the final number and stop (rotation 2). That was four times left, three times right, and two times left (and one final right to retract the bolt if the combination was correct and every gate correctly aligns)—just like the manufacturer's opening instructions. Wheel 3 is always set last because otherwise you'd reset it when setting wheels 1 and 2 (see Figure 13-2).

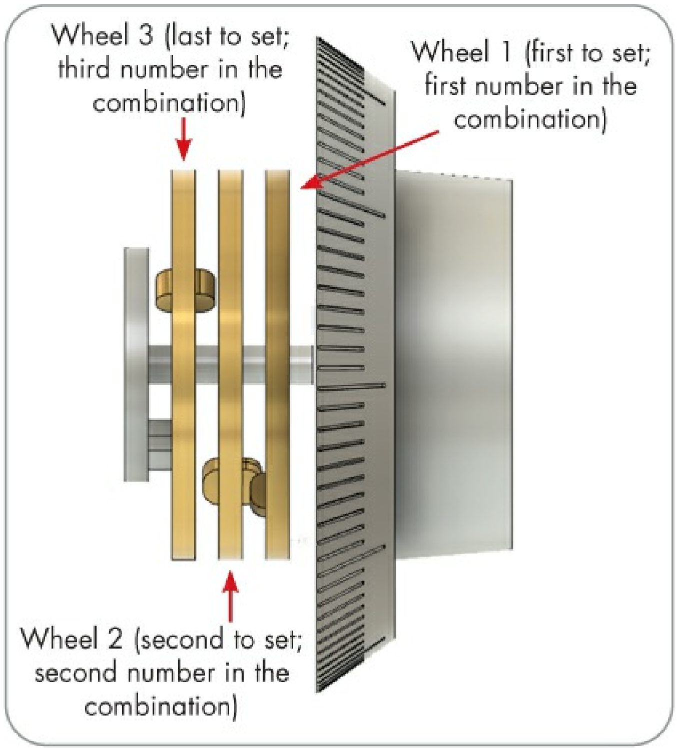


Figure 13-2: The gate in wheel 3 corresponds with the third number in the lock's combination, the gate in wheel 2 with the second, and the gate in wheel 1 with the first.

Second, and most important for our purposes, is each wheel's ability to complete almost its entire revolution without disturbing its neighbors. This isolation of movement allows us to selectively test one or two wheels at a time when searching for our gate indications.

Now dial AWL to 50; that is, dial at least four full rotations so you can be confident that every wheel has been picked up and stopped at 50. Looking at your dial and not the wheels this time (that is, viewing the lock from the front), repeat the same steps. Start dialing right. This time, you're trying to feel the pickup of each additional wheel. You'll know this is going to happen at 50 because that's where you just parked them all. Continue to dial right until you have picked up and are moving all three wheels.

If in doubt, peek inside. Some locks dial "tighter," so if you're dialing too slow, you might miss the slight increase in resistance when you pick up a wheel. Other dials are "loose," and you might hear rather than feel the impact of the drive pin hitting and moving the next wheel.

You can approach these wheel pickup clues in a couple of ways. First, as you near the point where you parked your wheels, make sure that you're mid-rotation; at the end of a rotation, your wrist's inability to rotate farther might make it hard to distinguish the drag of another wheel. Another method is to speed up your approach, thus ensuring you can hear the impact between the drive pin and fly and subsequent wheel pickup.

Dials vary, so one or both techniques should help you determine when you've hit a fly and picked up another wheel. This is a useful skill because sometimes you won't want to pick up an additional wheel, or the fly might be in the way and you'd hate to misinterpret that as a contact point.

Finding Contact Points

As we've discussed, a contact point is the area on each side of the cam gate (the V-shaped notch in the drive cam) that the lever nose touches. You take measurements of the contact points for the purposes of manipulation; your readings will change as the fence is able to fall into an open wheel gate and the lever nose begins to drop into the cam gate. The deeper the lever drops, the less room its nose has to move before it touches both the left and right sides of the cam gate.

To find the contact points on your lock, dial AWR 50. Now dial left one half turn. Somewhere, usually around 0, and within a range of around 10 numbers (such as 95–05, 0–10, 5–15, 98–6, or 1–9), you'll feel and hear the lever nose make contact with the edges of the cam gate. This range is known as the *contact area*, and it varies for each brand (for that matter, each lock). Move your dial left and right within the contact area to hear and feel both the left and right contact points (see Figure 13-3).

Figure 13-3: Left: The right contact point as seen from the back of the lock. You dialed left to get to the right contact point, which is on the right side of the dial when facing the lock. Right: The left contact point as seen from the back of the lock.

If you have a cutaway lock, you can watch this happen. Take your time and try this many, many times until you detect both. Respin the wheels AWR 50 and do it again. Picking up these contact points should become second nature the more you practice. Notice that you originally dialed right, parked the wheels at 50, then changed directions to left to find the contact points. If you had continued dialing right, you wouldn't have parked the wheels at 50 but instead moved them to the contact points. Then you'd be stuck with a wheel fly contacting the drive cam's drive pin in the middle of the cam gate. All these crowded parts could get in the way of, or mask, the true contact points.

If you spin too fast, you may blow past your contact points. Conversely, you may spin so hesitantly you can't even detect the contact area. Your dialing should be an easy, yet controlled, sweeping motion left and right.

NOTE

How fast is too fast, and how slow is too slow, to consistently pick up these contact points? Each lock is different, but to use an analogy from music class, we'd say that a point-to-point, left-and-right sweep tempo should be around 60 beats per minute (not including the time you spend taking a measurement).

Once you can consistently find—using your senses of sight, hearing, and touch—both contact points, you're ready to start reading and recording them. Position the lock and yourself so that you can see the lock's opening index straight on. Consistency is the key to success here; you'll need to calibrate your workspace to always maintain the same distance and angles so your readings will be accurate.

Your measuring skills will improve with repetition and exposure to different dials. Maybe your lock has skinny index lines with lots of space between them, while other locks have significantly thicker lines with paint outside their edges. This is where a set of index line stickers like those mentioned in Chapter 12 can come in handy. Some manipulators use a single thin line on a small circular sticker or the edge of some blue tape to give them a finer point to focus their reading on. If you don't have any, it's not a problem; just know that you'll need to decide how you'll consistently judge the difference between half, quarter, or tenth readings. Your interpretation might vary from day to day and lock to lock, but being consistent in your readings for an individual lock is vital.

Let's take a look at a few dial readings. We'll state the possible measurements in both quarter and tenth increments (the most common increments found on graphing charts). You don't have to agree precisely with our measurements, as long as you're consistent in how you're reading.

The reading in Figure 13-4 could be 50.5 or possibly 50.4 because it's just slightly off-angle. Again, this is why it's important to always maintain a consistent, straight-on view.

Figure 13-4: A reading of 50.4 or 50.5

In Figure 13-5, rather than having to choose between 50.75 or 50.9, as a beginner you'd probably want to round up to 51.

Figure 13-5: A reading just under 51

Using the quarter scale, the reading in Figure 13-6 is likely 50.75. Using tenths, if the previous figure was 50.9, would you consider this reading 50.7 or 50.8?

Figure 13-6: A reading of 50.75 or possibly 50.8, depending on your individual calibration

Finally, the reading in Figure 13-7 could be 50, 50.1 or 50.2, or 50.25, depending on your chosen increments. Again, just be consistent.

Figure 13-7: Is this reading still 50, or have you made it to 50.25 (or in tenths, 50.1 or 50.2)?

Now we'll take a look at how to graph your readings to get clues to the first number in the combination.

Graphing to Find Your First Number

Chapter 12 mentioned the many graphing options available to you, but for this exercise, we recommend you start with a graph that uses quarter increments. This will prevent unnecessary stress over minute differences and speed up your decision-making as you're getting more comfortable with the graphing process.

Graphing simply means recording your contact-point readings as you rotate one or more wheels, trying to move a gate under the fence. Because the cam gate is generally V-shaped, the lower the fence is, the lower the lever nose drops and the narrower the contact area (that is, the left contact point moves right, and the right contact point moves left). The right contact point is more sloped, so you usually see greater changes in the right contact point indications.

Let's take a look at this from the back of the lock. With the combination set to 20-40-60, dial the appropriate number of turns to 20. While looking at the drive cam and the lever nose, dial to 40. Notice that each time the cam gate passes under the lever nose, you can see the nose drop lower. If you continue dialing to 60, you'll see the lever nose drop completely. When you plot these readings, you'll see the same narrowing of the contact points on your graph. When you see this pattern on your graph, you can assume it indicates a gate under the fence because that's where the lever nose dropped the lowest. When the fence isn't falling into a wheel's gate, it can't sink any lower than the top of the wheels and will touch only the top of the cam gate.

You have options when graphing for the first number. You can take the easy route and move all three wheels around the dial when checking your contact points, or you can isolate a wheel or two at a time. Some isolation maneuvers can get complicated, but running either all three wheels or only wheel 3 is fairly straightforward. We'll look at both approaches.

NOTE

This process differs slightly for LaGard 3300 lock owners; see "Manipulating LaGard 3300 Safe Locks" on page 263 for special testing and alternative dialing procedures. before continuing.

Moving All Three Wheels

For your first try at graphing, you'll move all three wheels, starting AWL. You'll move around the dial in increments of 2.5 to speed up the process. You'll need to know your contact points before you start. For this example, we'll use 1 and 9. Substitute your lock's contact points, entering the value in the appropriate box on your chart. You can also fill in the boxes for the next whole numbers above and below your contact points (0 and 2, and 8 and 10, respectively) for easier reading. Follow these steps:

1. Dial AWL and stop at 10 (one whole number higher than the right contact point).
2. Dial slightly right to check the 1 and 9 contact points. See if you notice a slight change in their readings. Plot your readings for both the left and right contact points on your graph. The vertical lines on the chart indicate the dial location (which would be 10 for this step), and the horizontal lines indicate your contact point measurements in quarters.
3. Dial left to 12.5.
4. Dial right to check the 1 and 9 contact points again and plot your new readings on the 12.5 line of your graph.
5. Dial left to 15.
6. Dial right to check the 1 and 9 contact points again and plot your new readings on the 15 line of your graph.
7. Continue this around the dial, recording your point readings on your graph.

If you were looking at your cutaway or had the back cover off, you should see all three wheels moving as you work your way around the dial.

Now take a look at your graph. The readings will be a little jumbled up when you dial near the area of your contact points, but what about the rest of the points you plotted? Can you see a clear gate indication? Are the points all over the place as in Figure 13-8?

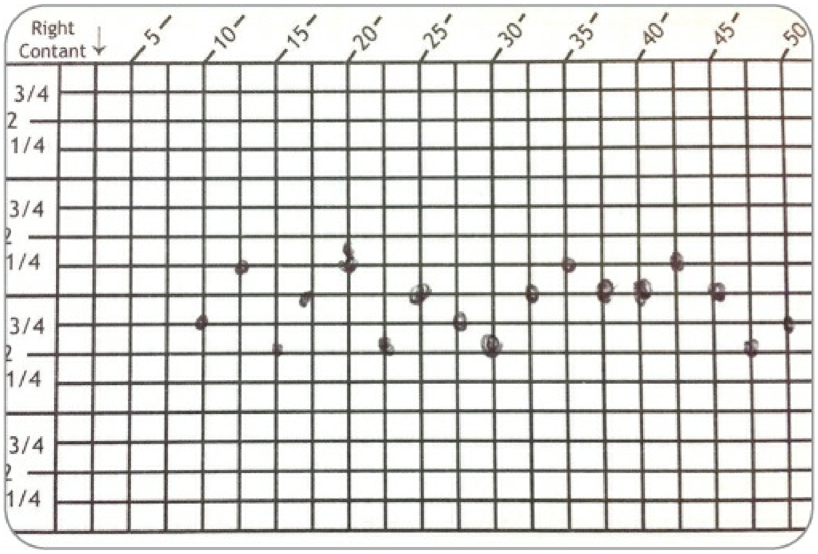


Figure 13-8: These jumpy readings are the result of changing the point of view and mashing the contact points a little too hard.

Graphs like Figure 13-8 are too jumpy to be of much use. You're looking for outliers to spot potential gates, but several of these measurements vary by half a number or more, so there's no strong gate indication yet.

Regardless of how your first graphing attempt turned out, you've seen the process of moving all three wheels at a time and checking your contact points at each stop. This process is tried and true; the more you do it, the better you'll be. Now let's look at the other option.

Running Only Wheel 3

Deciding whether to test all three wheels or just run wheel 3 will get easier over time. There's a good reason to sometimes just run wheel 3 on your first turn around the dial: it's usually the wheel that indicates first.

NOTE

In safe-lock manipulation, to indicate *is to provide a clue as to which wheel's gate is now making contact with the lever's fence.*

For this approach, you'll start out the same way as the previous method. First, identify your contact points (again, for this example, we'll say they're 1 and 9) and dial AWL 10—one number higher than the right contact point. Here are the steps:

1. Dial 2× right to 10. This picks up wheel 3 and moves it one full rotation, while leaving wheels 2 and 1 in place.
2. Dial left one time to 10. This moves the drive cam back to the other side of wheel 3's fly.

3. Dial slightly right to check the 1 and 9 contact points. Plot them on the 10 line of your graph.
4. Dial left to 12.5.
5. Dial right to check the 1 and 9 contact points and plot them on the 12.5 line of your graph.
6. Dial left to 15.
7. Dial right to check the 1 and 9 contact points and plot them on the 15 line of your graph.
8. Continue this around the dial. Record your points on your graph.

If you were looking at your cutaway or had the back cover off, all you should see moving is wheel 3 and the drive cam.

How did your graph turn out? Better than your first attempt? If you've graphed correctly on a lock that will talk to you, you should now have a number or two indicating, similar to Figure 13-9. Notice that one reading for the right contact point clearly deviates from the others.

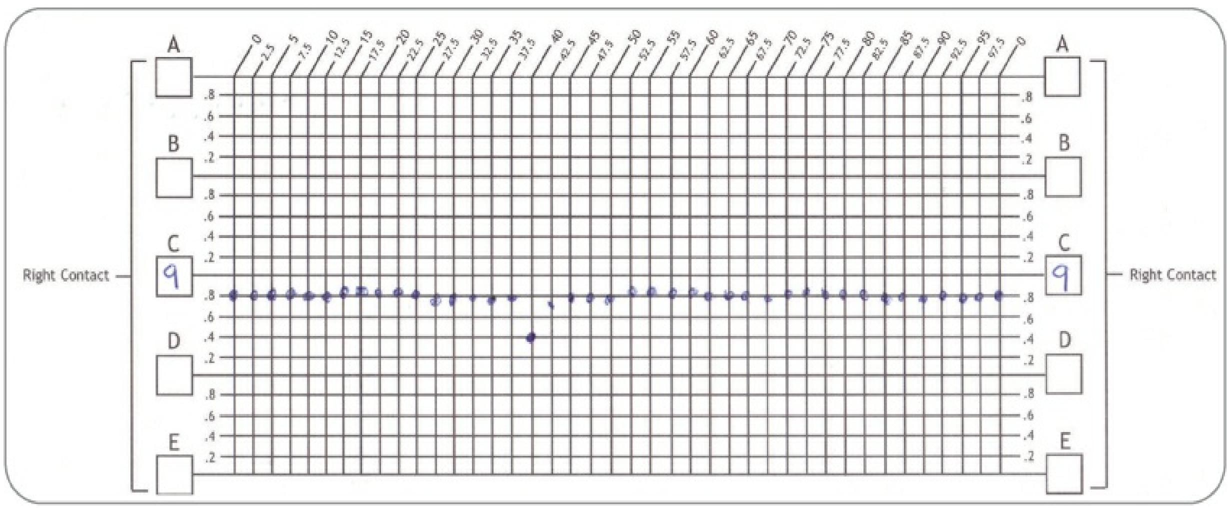


Figure 13-9: The right contact point has little movement except in one area of the dial.

Because the right contact point usually gives the biggest indications while the left is much more subtle, sometimes locksporters plot the left contact points in larger increments to speed up the manipulation process. For illustrative purposes, we tested the left contact point every 10 numbers in Figure 13-10. As you're learning and getting more comfortable with graphing, you should continue to plot them all.

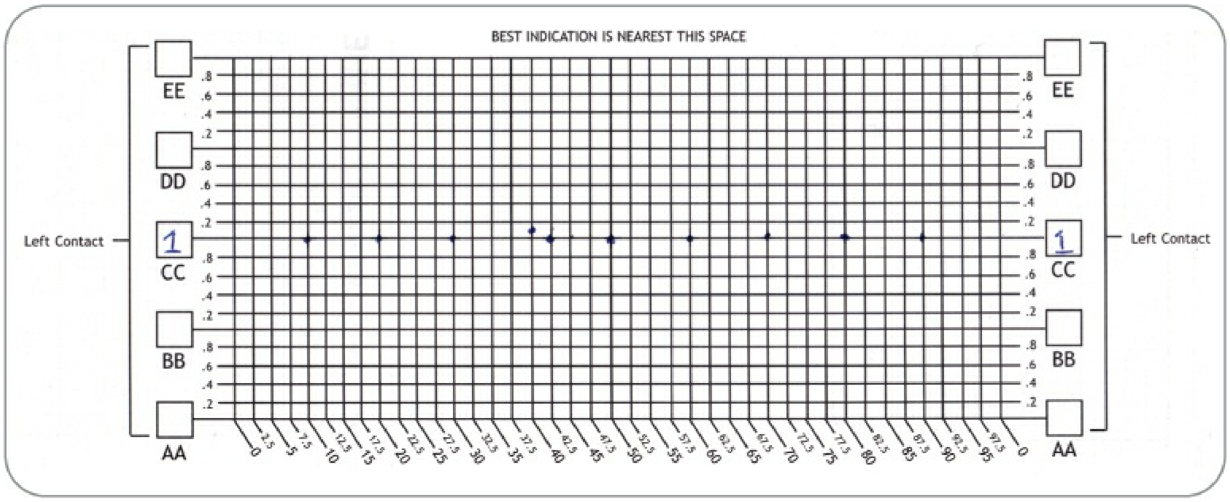


Figure 13-10: Testing the left contact points in increments of 10

NOTE

Figures 13-9 and 13-10 were extracted from Figure 12-9. Look back at the other graphs in Chapter 12, and in the other publications mentioned there, to see if you can spot gate indication patterns.

You can see the difference in a left contact point with and without a gate under the fence. Figure 13-11 shows a left contact reading of 1.5, with no gate under the fence.

Figure 13-11: The left contact point is reading around 1.5 with no gate under the fence.

Figure 13-12 shows the subtle change typical of left contact points when the gate is under the fence.

Figure 13-12: Notice that the reading has shifted slightly right when the fence slips into the gate.

Some graphs increment around the dial by 2 rather than 2.5. Either increment is usually sufficient to catch some gate interaction. When working in smaller increments around the dial, you often see the points gradually narrow into the telltale pattern. With larger increments, some changes start and end abruptly, usually returning you to the previous reading or close to it. Figure 13-13 is a good example of the right contact point returning to the same level after an indication.

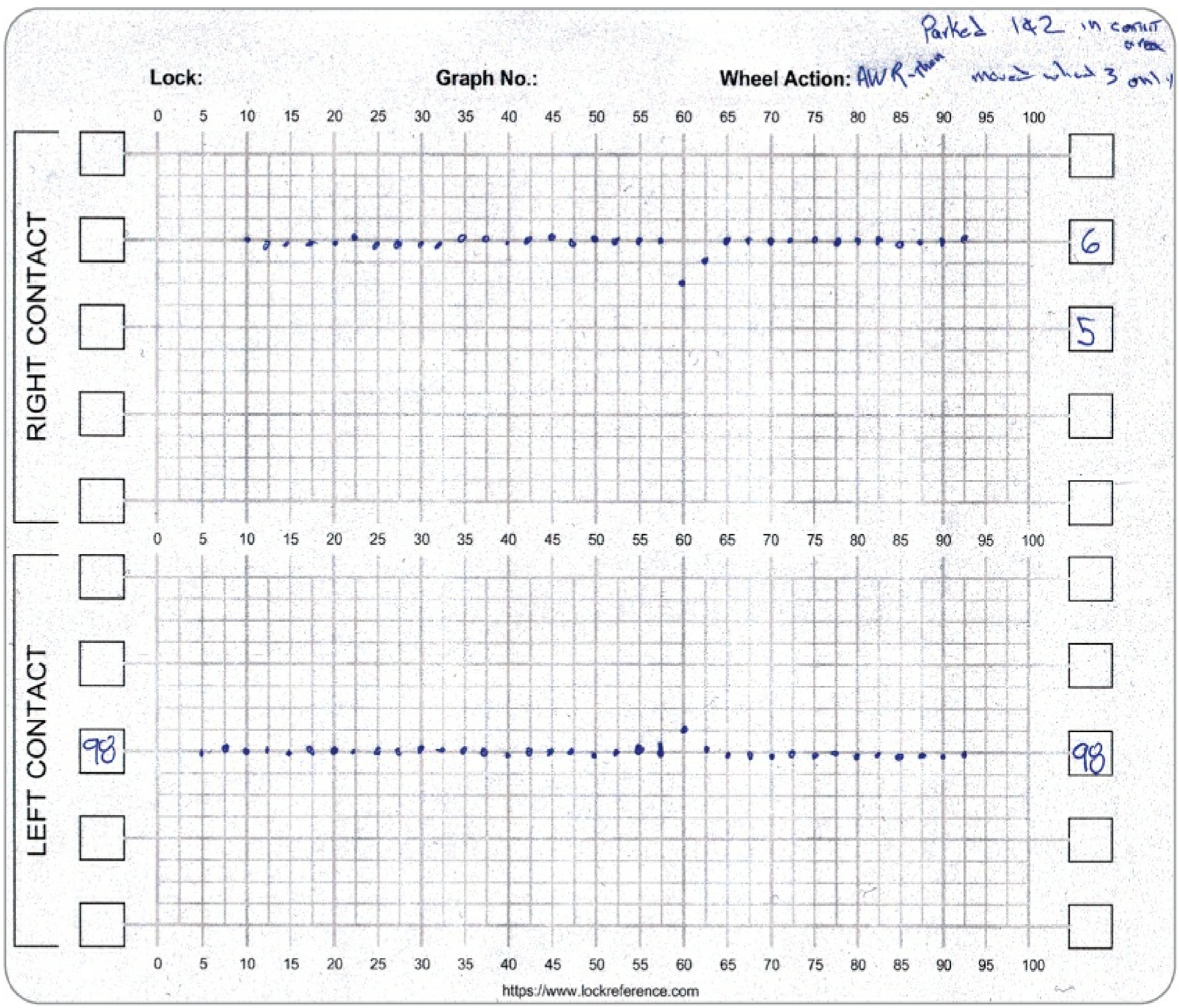


Figure 13-13: This graph is in 2.5 increments and indicates on two adjacent tryout numbers. You don't need to test anything between the contact points because you can already see a solid contact.

Sometimes your measurements don't return to the previous level when you pass out of a gate, but instead settle on a new level. For an example, see Figure 12-8 in the preceding chapter.

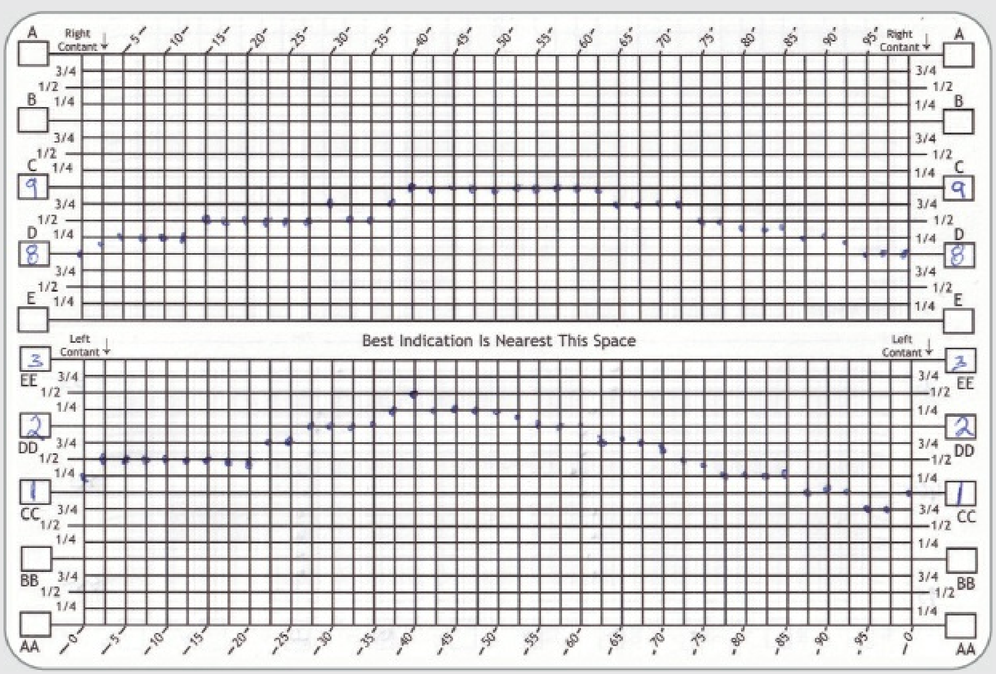
GRAPHING WORK-AROUNDS

The lock space can get a little crowded when the cam's drive pins and wheel 3 get near your contact points. Let's say your right contact point is 10, and you've been moving AWR. You can't move all three wheels from 15 to 12.5 to 10 and change directions to check your contact point without hitting the fly you just parked at 10.

The good news here is that the left reading isn't restricted by the flys in this case and might be of use. You could just use that one contact point as a reference, or you could park your wheels near 10 and check 12, 11, 9, or 8. Call it the "AWR until the flys get bunched up, then dial left" technique.

Gates are usually big enough to show up in more than one spot when you jump around by 2 or 2.5. In this case, you could safely skip the next planned number on the graph as long as you're testing the others nearby. Or, if you already have a good indication, you could skip this area altogether. Skipping steps like this is a technique you might use in competitions to speed up the process if you've already had a good indication; in such a scenario, you have to weigh risk versus reward.

This graph shows an example of feedback that isn't what you intended but is valuable nevertheless.



This matching swell at both contact points isn't uncommon for some locks. The change at 40 for the left contact point looks great and is coupled with a solid change near 40 for the right contact point. While not the textbook indication, it's still worth exploring.

Once you've graphed a few dozen locks, you'll probably notice that your variations have tightened up as you grow more definitive and confident with your readings. Eventually, you'll reach a point where you can make fewer marks or even forgo graphing altogether, especially in a competition setting. Time spent plotting, even with confident readings and exact markings, is time not spent dialing. But there's no rush to get there, and you might still find it useful to keep charting graphs around for special cases.

> I still use a graph all the time, but usually I'm making only a handful of marks, mostly relating to significant changes in my measurements. Some manipulators just put a number down on their notepad every now and then if they see something noteworthy. Still, plenty of folks can manipulate paper free.
>
> —BANDEATOZ

Now that you've seen what an indication looks like on the graph, you need to test it to identify the specific number in the combination. This is known as *finding the True Center*.

Finding True Center

To find True Center, instead of moving across the entire dial in increments of 2.5, you'll move and test every number in the range of the suspected gate and plot your findings on a True Center graph.

Say you have a suspected gate around 20 on your lock. First, write 15 as the low and 25 as the high numbers on the True Center graph.

NOTE

Some True Center graphs use a span of 10 digits, and others use 20. Testing 5 over and 5 under your initial indication should be enough to confirm the position of the gate you're searching for.

The True Center testing process is as follows:

1. Turn 4× right and stop at the high True Center graph number (25 in this example).
2. Turn left to the contact area and record the left and right contact points.
3. Turn right to the next highest number (24).
4. Turn left to the contact area and record the left and right contact points.
5. Continue this process until the True Center graph is complete—that is, until you've tested down to 15.

Keep in mind that the left and right contact points may not move equally during each plot; your indications may favor one over the other, as shown in Figure 13-14.

If you're lucky, you'll be able to easily determine the True Center. See the example graph in Figure 13-15, where True Center is clearly 60.

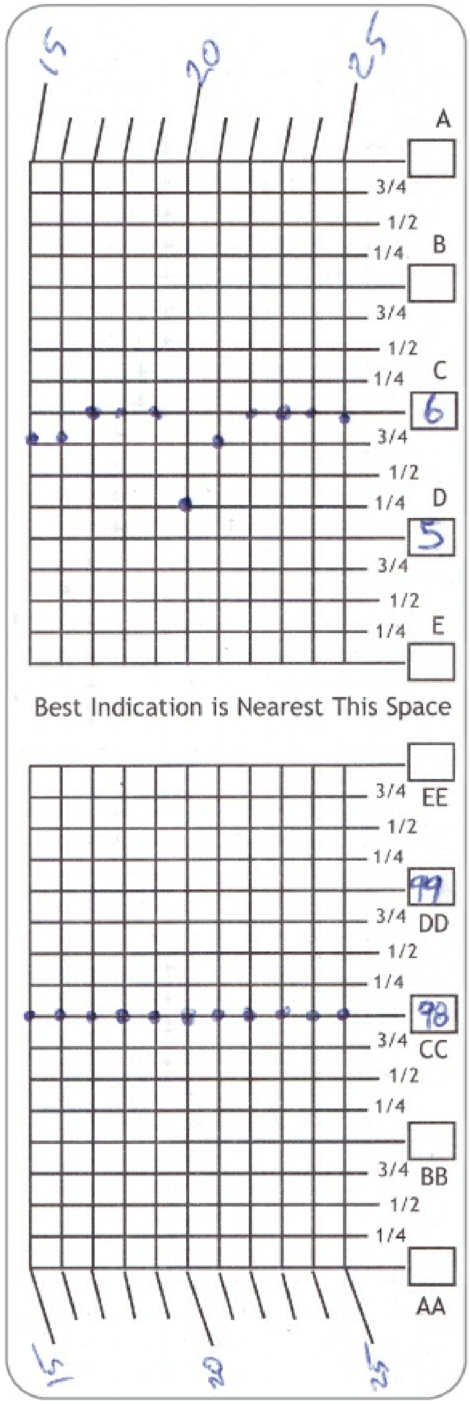


Figure 13-14: While the left contact point in this example runs flat, the right contact point makes a solid jump at 20. It's common to also have examples with either 19 or 21 down as low as 20 is here.

When True Center isn't as easy to determine, you can follow some well-established guidelines. For example, sometimes two or more numbers in a row may indicate True Center:

- If two adjacent numbers indicate and you've dialed AWR, choose the right number.
- If two adjacent numbers indicate and you've dialed AWL, choose the left number.

Always choose a whole number. Using a finding like 20.25 for True Center will throw off your later computations, and for Group 2 locks, the decimal distinction isn't necessary.

If dialing AWR doesn't help clear up your True Center test, retry the entire process by dialing AWL.

Let's look at a couple of examples of what can happen when True Center isn't super clear. First, Figure 13-16 shows an attempt to find True Center after an initial 40 indication.

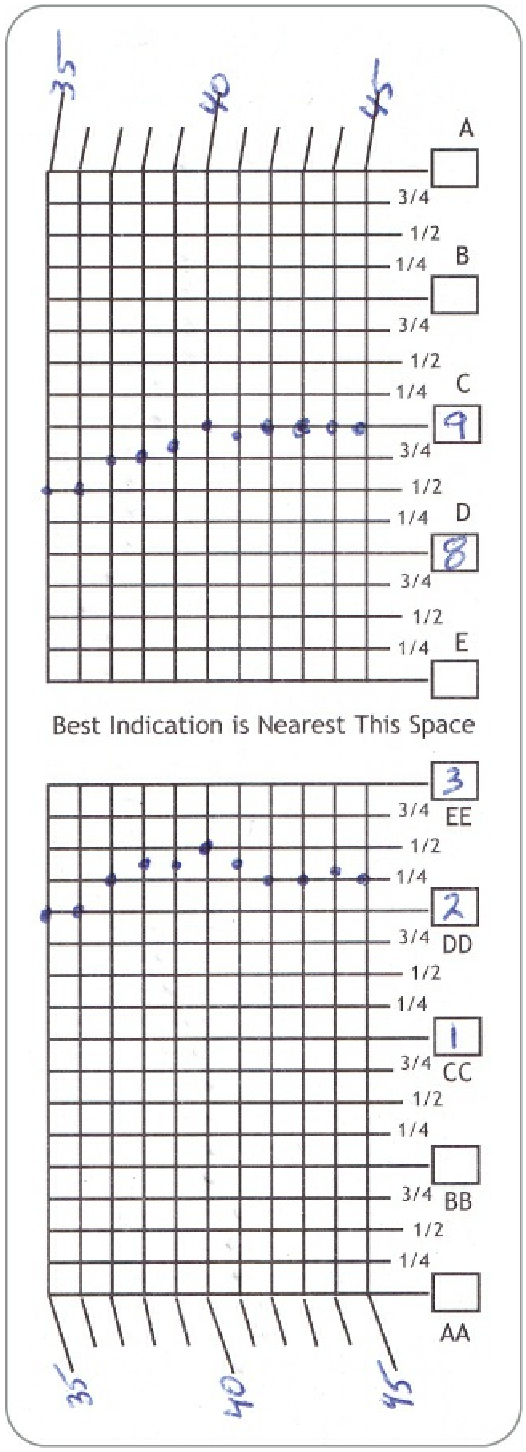


Figure 13-16: Attempting to find True Center after an initial indication of 40

A matching upward or downward slope for both contact points often indicates that the wheels are moving around the wheel post in an elliptical path. Because the pattern at the left side of both graphs matches, you should focus on the left contact point's high indication at 40.

In Figure 13-17, the initial indication is 20, but the right contact point shows little change, and the highest reading for the left contact point is 22.

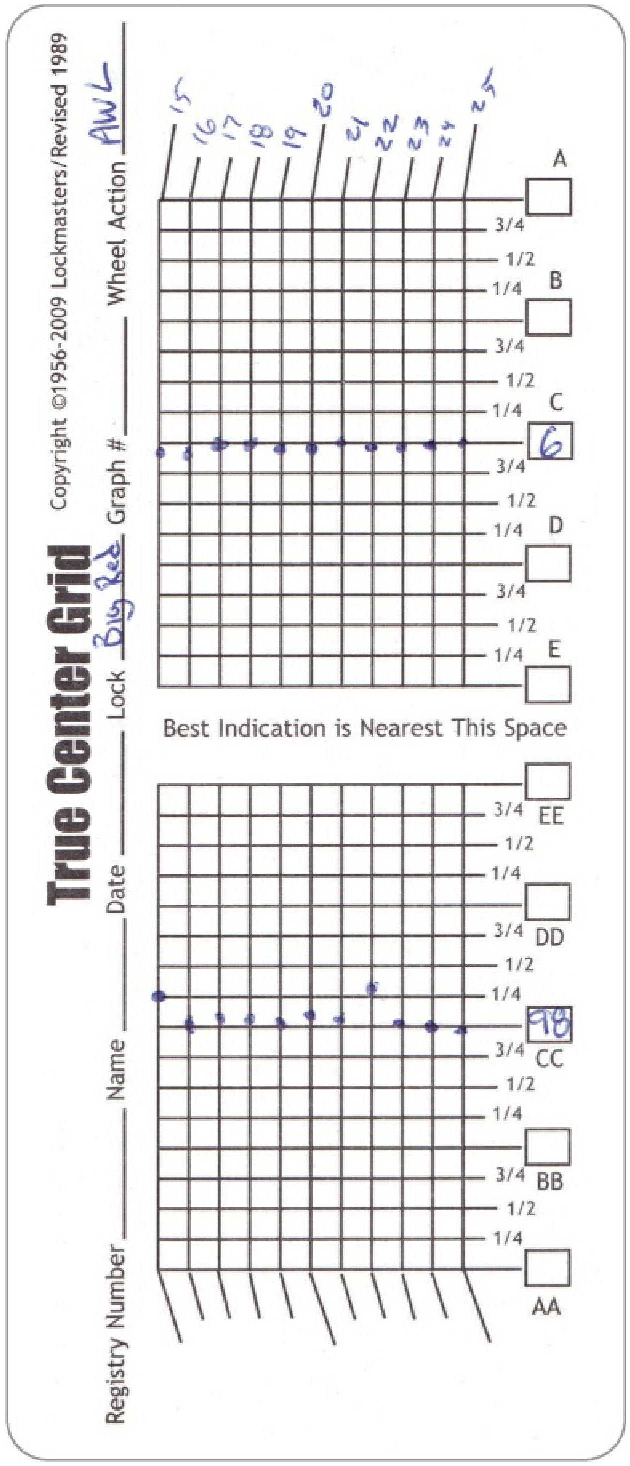


Figure 13-17: Attempting to find True Center after an initial indication of 20

While 15 and 22 are essentially equal indications, 22 is closer to the initial reading and thus more likely to be True Center. However, with this little action on both contact points, the best approach would be to run this again using the other direction—in this case, to take the same readings a second time running AWR.

Once you've identified True Center, you have one of the numbers in the combination. Now you need to determine which wheel is indicating that number, using a High Low test.

Running High Low Tests

You use different High Low tests depending on where you are in the testing sequence. The first test always checks for all three wheels because you don't know which one is indicating yet. After that, which test you run depends on the result from the first test.

During a High Low test, you try your True Center number on two wheels and purposely enter a wrong number (10 higher or 10 lower than True Center) on the other wheel, repeating this test for each wheel. In two of the tests, the fence will be able to drop into the gate, shifting the lever nose down, and in the other it won't, meaning the contact area will be significantly larger. So, instead of looking for the narrowest contact area, now you're looking for the widest, which indicates the wheel corresponding to the True Center number.

As you conduct your High Low tests, you'll fill in a worksheet like the one shown in Figure 13-18, generally starting with your True Center number and following the sequence. Each worksheet varies slightly depending on the wheel or wheels you're trying to find.

Use to determine if the #1, #2, or #3 wheel is indicating.

	↓ Start here fill in True Center (TC) ↓
True Center	**20**
HIGH Test (True Center +10)	30
LOW Test Number (TC -10)	10

High Test						
Test Combinations	#1 Wheel	#2 Wheel	#3 Wheel	Left Contact Reading	Right Contact Reading	Contact Area Width
Test Combo A	20 TC	20 TC	30 High Test	98.2	5.6	7.4
Test Combo B	20 TC	30 High Test	20 TC	98.1	5.6	7.5
Test Combo C	30 High Test	20 TC	20 TC	98.1	5.8	7.7

Low Test						
Test Combinations	#1 Wheel	#2 Wheel	#3 Wheel	Left Contact Reading	Right Contact Reading	Contact Area Width
Test Combo A	20 TC	20 TC	10 Low Test	98.2	5.5	7.3
Test Combo B	20 TC	10 Low Test	20 TC	98.2	5.6	7.4
Test Combo C	10 Low Test	20 TC	20 TC	98.2	5.7	7.5

How to dial the HIGH TEST and LOW test	
Test Combo A	RIGHT 4 times to TC___ (this parks #1 & #2) LEFT 2 times to Test Combo #___ (this tests #3 but leaves other two wheels parked) RIGHT to contact area. Record contact readings above.
Test Combo B	RIGHT 4 times to TC___ (this parks #1) LEFT 3 times Test Combo #___ (testing wheel #2) RIGHT 2 times to TC (this parks wheel #3) LEFT to contact area. Record contact readings above.
Test Combo C	LEFT 4 times to Test Combo #___ (tests wheel #1) RIGHT 3 time to TC___ (this parks wheels #2 & #3 LEFT to contact area. Record contact readings above.

The widest (largest) number in the Contact Area Width will be the wheel that is indicating.

Figure 13-18: A High Low test worksheet

This worksheet tests a True Center number of 20. The largest readings for High and Low were both during Test C, which indicates that the gate found at 20 belongs to wheel 1. Good thing that worked out, considering we know the combination is 20-40-60!

Here's some guidance about using the worksheets:

- **Accuracy counts.** Even the slightest deviation can overshadow the clues you're looking for (notice that in Figure 13-18, a mere 0.1 difference pointed the way). Subtract your left contact-point reading from your right contact-point reading to get your Contact Area Width. If your left contact point is left of 0, you can add 100 to your right contact to make the math easier. For example, if the left contact point is 98.2 and the right contact point is 5.6, just calculate 105.6 – 98.2 = 7.4.

- **Use the correct worksheet at the correct time.** If adding 10 or subtracting 10 puts you on or close to another known combination number, try a number more than 10 to clear that gate and get a test number. For example, adding or subtracting 13 to generate your test number would be allowable in this case.
- **If your test answers don't align, conduct your tests again.** If this happens, usually it means you weren't consistent in your contact-point readings. Dialing directions are at the bottom of the worksheet. Simply fill in the numbers as you go along and do the basic math.

You can print or copy the following blank High Low test worksheets to use as templates. Start with the following worksheet to determine if wheel 1, 2, or 3 is indicating.

	↓ Start here; fill in TC ↓
True Center (TC)	
HIGH Test Number (TC + 10)	
LOW Test Number (TC – 10)	

High Test						
Test Combinations	Wheel 1	Wheel 2	Wheel 3	Left Contact Reading	Right Contact Reading	Contact Area Width
Test Combo A	TC	TC	High Test			
Test Combo B	TC	High Test	TC			
Test Combo C	High Test	TC	TC			

Low Test						
Test Combinations	Wheel 1	Wheel 2	Wheel 3	Left Contact Reading	Right Contact Reading	Contact Area Width
Test Combo A	TC	TC	Low Test			
Test Combo B	TC	Low Test	TC			
Test Combo C	Low Test	TC	TC			

	How to dial the High Test and Low Test
Test Combo A	Right 4 times to TC_____ (this parks wheels 1 and 2). Left 2 times to Test Combo #_____ (this sets wheel 3). Right to contact area. Record contact readings above.
Test Combo B	Right 4 times to TC_____ (this parks wheel 1). Left 3 times Test Combo #_____ (this parks wheel 2). Right 2 times to TC (this parks wheel 3). Left to contact area. Record contact readings above.
Test Combo C	Left 4 times to Test Combo #_____ (this parks wheel 1). Right 3 times to TC_____ (this parks wheels 2 and 3). Left to contact area. Record contact readings above.

The widest (largest) number in the Contact Area Width will be the wheel that is indicating.

Use the following worksheet to determine if wheel 1 or 2 is indicating.

	↓ Start here; fill in wheel 3↓
Known Wheel 3 Number	
True Center (TC)	
HIGH Test Number (TC + 10)	
LOW Test Number (TC – 10)	

High Test						
Test Combinations	Wheel 1	Wheel 2	Wheel 3	Left Contact Reading	Right Contact Reading	Contact Area Width
Test Combo A	TC	High Test				
Test Combo B	High Test	TC				

Low Test						
Test Combinations	Wheel 1	Wheel 2	Wheel 3	Left Contact Reading	Right Contact Reading	Contact Area Width
Test Combo A	TC	Low Test	Known 3			
Test Combo B	Low Test	TC	Known 3			

	How to dial the High Test and Low Test
Test Combo A	Right 4 times to Test Combo #_____ (this tests wheel 1). Left 3 times to TC_____ (this parks wheel 2). Right 2 times to Known 3 (this parks wheel 3 under the fence). Left to contact area. Record contact readings above.
Test Combo B	Right 4 times to TC_____ (this parks wheel 1). Left 3 times Test Combo #_____ (testing wheel 2). Right 2 times to Known 3 (this parks wheel 3 under the fence, allowing us to read other wheels). Left to contact area. Record contact readings above.

The widest (largest) number in the Contact Area Width will be the wheel that is indicating.

Use the following worksheet to determine if wheel 2 or 3 is indicating.

	↓ Start here; use to fill in wheel 1 on chart ↓
Known Wheel 1 Number	
True Center (TC)	
HIGH Test Number (TC + 10)	
LOW Test Number (TC – 10)	

High Test						
Test Combinations	Wheel 1	Wheel 2	Wheel 3	Left Contact Reading	Right Contact Reading	Contact Area Width
Test Combo A	Known 1	TC	High Test			
Test Combo B	Known 1	High Test	TC			

Low Test						
Test Combinations	Wheel 1	Wheel 2	Wheel 3	Left Contact Reading	Right Contact Reading	Contact Area Width
Test Combo A	Known 1	TC	Low Test			
Test Combo B	Known 1	Low Test	TC			

	How to dial the High Test and Low Test
Test Combo A	Right 4 times to Known 1 (parks wheel 1 under fence, allowing us to read other wheels). Left 3 times to TC______ (wheel 2). Right 2 times to Test Combo #______ . Left to contact area. Record contact readings above.
Test Combo B	Right 4 times to Known 1 (parks wheel 1 under fence). Left 3 times to Test Combo #______ . Right 2 times to TC______ (wheel 3). Left to contact area. Record contact readings above.

The widest (largest) number in the Contact Area Width will be the wheel that is indicating.

Finding Your Second Number

You'll usually need to do more charting to find your second number. The exception is if your first chart found more than one number. Typically, you'll just test your best indication, but if you have two strong indications, then run the True Center and High Low tests for both. If you find two or even all three gate locations and know which wheels they belong to, you'll get a speedy opening!

In the previous example, we found wheel 1 first, which goes to show that you never know which wheel will indicate first. However, as noted previously, *usually* it's wheel 3.

> Wheel 3 indicates first so often that I usually just assume it and move forward without doing High Low tests until I'm proven wrong. Is that a waste of time when it turns out I'm wrong? Yes, but the odds are still in my favor—this approach works for me 75 to 90 percent of the time. That said, until you have the experience to be this cavalier, you should continue down the correct path and plot your second graph.
>
> —BANDEATOZ

A few changes for the second graph procedure are worth noting up front:

- You'll start graphing 2 or 2.5 above your first found number.
- The specific dialing procedure—parking certain wheels, isolating others, moving others back again—depends on which wheel indicated first. This can get confusing, but you can take shortcuts as you run the dial. You can print these out to keep them handy as you work.

NOTE

This is where owning a cutaway lock becomes indispensable, so you can see when each wheel will move. Understanding the why behind a particular dialing sequence will always pay dividends.

For these instructions, we'll start by assuming a known wheel 3 since that's the most common case. Still, try each scenario a few times before you graph. Get a feel for the steps. Watch the wheels and see the magic happen.

When wheel 3 indicated first (that is, you know the third number in the combination), use the following dialing sequence to find and graph your next indication:

1. Dial 4× left to 2.5 numbers higher than the known third number.
2. Dial 2× right to the known third number.
3. Dial left to the contact area.
4. Dial 2× left 2.5 numbers higher than the last stop in step 1.
5. Dial 2× right to the known third number.
6. Dial left to the contact area.
7. Continue around the dial in 2.5 increments, repeating steps 4 through 7.
8. Run the True Center test on your indication.

When you watch the wheels, you'll see that you're repeating a process of moving all three wheels forward, moving wheel 3 back under the fence, and recording the new contact-point readings with wheels 1 and 2 in new positions. Run a High Low test on the appropriate worksheet to determine whether it's wheel 1 or 2 that indicates.

When wheel 2 indicated first (that is, you know the second number in the combination), use the following dialing sequence to find and graph your next indication:

1. Dial 4× right to the known second number.
2. Dial 2× left to 2.5 numbers higher than the known second number.
3. Dial right to the contact area.
4. Dial 1× left to 2.5 numbers higher than the last stop in step 2.
5. Dial right to the contact area.
6. Continue around the dial in 2.5 increments, repeating these steps.
7. Run the True Center test on your indication.

Watching this time, you'll see you've parked wheel 2's gate under the fence and just moved wheel 3. You don't need to do the High Low test: your low indication will be wheel 3, because that's all you've moved.

When wheel 1 indicated first (that is, you know the first number in the combination), use the following dialing sequence to find and graph your next indication:

1. Dial 4× right to the known first number.
2. Dial 3× left to 2.5 numbers lower than the known first number.
3. Dial right to the contact area.
4. Dial 1× left to 2.5 numbers higher than the last stop in step 2.
5. Dial right to the contact area.
6. Continue around the dial in 2.5 increments, repeating these steps.
7. Run the True Center test on your indication.

Looking at the wheels now, you'll see that wheel 1 stays parked under the gate as you move wheels 2 and 3. Run a High Low test on the appropriate worksheet to determine whether wheel 2 or 3 indicates.

When you've completed this process successfully, you should have solved two out of the three numbers in your lock's combination. Now we'll look at how to solve the final number and open the lock.

Brute-Forcing to Find the Last Number

To find the last number, you could use one of the preceding dialing sequences and graph a third time, or you could simply *brute-force* the dial 40 to 50 times—meaning you'll use your two known numbers and try all the possibilities for the third number, working your way around the dial in increments of 2 or 2.5. The first process is precise, while the second usually leads to a faster opening and is our recommendation 99 percent of the time. The notable exception for brute forcing would be a lock that hadn't been communicating clearly throughout the previous steps. Sometimes you'll have to go the full graphing distance to get a clear indication for your last gate.

Let's assume you've found the 20 and 60 in your combination on wheels 1 and 3, respectively. At each try of the opening, jiggle the dial back and forth to hit the contact points several times at speed (the *vigorous oscillation* we mentioned earlier in the chapter) to encourage the lever nose to drop in further and the fence to hit the gates and, hopefully, self-align slightly. With a few dials and some luck, you should have your first open. Congratulations!

MANIPULATING LAGARD 3300 SAFE LOCKS

As Chapter 12 mentioned, on some LaGard 3300 locks, the wheels don't rotate so much as gyrate around the wheel post. As a result, the wheels might indicate irrelevant high and low points, often masking true gate positions and confounding novice manipulators. The good news is that you can steps take to mitigate this, and, as always, a cutaway lock will help you see exactly what's going on as you do.

Some LaGard 3300 wheels get pushed up and down depending on the direction of the spin for about half of the dial. You can use two easy tests to determine whether this is happening in your test lock. In general, wheel 3, when dialed to the right, moves up between 0 and 50 (technically, 55 to 0, given the turn direction), so you'll use the halfway point, 25, for your first test number. When dialed to the left, wheel 3 will generally move up from 50 to 99 (again, technically 45 to 99), so you'll use 75 for your second test number. Hence, these tests are called the LaGard 25 and 75 tests.

The LaGard 25 test

1. Dial 4× left to 25.
2. Dial 3× right to 25.
3. Dial 2× left to 25.
4. Dial right to the contact points and make note of them.

The LaGard 75 test

1. Dial 4× right to 75.
2. Dial 3× left to 75.
3. Dial 2× right to 75.
4. Dial left to the contact points and make note of them.

If the tests reveal little or no change in the distance between your contact points, your lock likely doesn't have the wheel gyration issue, and you can proceed with the regular manipulation processes outlined in this chapter. However, if the difference is a third of a number or more, you would likely benefit from either disassembling and reassembling your lock and rerunning the LaGard 25 and 75 tests to see if the results improve, giving the lock mount a light downward tap to try settling the wheels enough to improve the test results, or taking the steps described next.

Each dialing sequence for each wheel is divided into two steps, one to push the wheels up and the other to push them down.

Finding a gate on wheel 3 (running half of the dial)

1. Dial 4× left to 25.
2. Dial 3× right to 25.
3. Dial 2× left to 26.
4. Dial right to the contact points; then oscillate to settle the wheels.
5. Dial left to 45.
6. Dial right to the contact points; then measure and graph.
7. Dial left to 47 (that is, adding 2 to 45).
8. Dial right to the contact points; then measure and graph.
9. Dial left to 49 (adding 2 to 47).
10. Dial right to the contact points; then measure and graph.
11. Repeat these steps until you reach 5.

Finding a gate on wheel 3 (running the other half of the dial)

1. Dial 4× right to 75.
2. Dial 3× left to 75.
3. Dial 2× right to 74.
4. Dial left to the contact points; then oscillate to settle the wheels.
5. Dial right to 55.
6. Dial left to the contact points; then measure and graph.
7. Dial right to 53 (that is, subtracting 2 from 55).
8. Dial left to the contact points; then measure and graph.
9. Dial right to 51 (subtracting 2 from 53).
10. Repeat these steps until you reach 95.

This process should indicate your gate position on wheel 3. You'll use a similar dialing technique for wheel 2.

Finding a gate on wheel 2 (running half of the dial)

1. Dial 4× left to 25.
2. Dial 3× right to 5.
3. Dial 2× left to the known wheel 3 number.
4. Dial right to the contact points; then measure and graph.
5. Dial 2× right to 3 (subtracting 2 from 5).
6. Dial 2× left to the known wheel 3 number.
7. Dial right to the contact points; then measure and graph.
8. Continue 2× right to 1 (subtracting 2 from 3).
9. Dial 2× left to the known wheel 3 number.
10. Repeat these steps until you reach 45.

Finding a gate on wheel 2 (running the other half of the dial)

1. Dial 4× right to 75.
2. Dial 3× left to 95.
3. Dial 2× right to the known wheel 3 number.
4. Dial left to contact points; then measure and graph.
5. Continue dialing 2× left to 97 (adding 2 to 95).
6. Dial 2× right to the known wheel 3 number.
7. Dial left to the contact points; then measure and graph.
8. Continue dialing 2× left to 99 (adding 2 to 97).
9. Dial 2× right to the known wheel 3 number.
10. Repeat these steps until you reach 55.

Now simply use the brute-force method to determine the final number and open the lock.

Now all you need to do is practice the instructions outlined in this chapter until you can fully comprehend, visualize, and execute every step. Having a cutaway lock, graphing chart templates, and test worksheets handy is a good idea. You might not need to reference them every time you're manipulating a lock, but they can bail you out when you do need them.

Whenever you get confused during practice, simply look inside the lock to see where you went wrong and what the lock is really telling you. Don't be afraid to start over on a known combination to confirm that your steps are producing the results you expect. Knowing when you go wrong is easy if you already know the answer. This is your training time, and there's no reason to struggle unnecessarily.

Take one step at a time and master that step. If you spend all your time mastering your first graph and your first wheel, that's time well spent. Being able to accurately read contact points is just as important on your second wheel as it is on your first. And you don't have to memorize anything! Steps, dial directions, number of spins, where to park a wheel—these can all be referenced from a notebook or printout, even in a competition setting. Once you fully understand the process, your many notes and tests become an easy-to-follow checklist.

Summary

In this chapter, you've learned the end-to-end safe-manipulation process: finding and plotting detailed contact-point measurements on a graph, spotting a gate indication and testing to find the True Center, running High Low tests to determine which wheel that number corresponds to, and then using brute force to find the final number and open the safe! Now it's time to practice and practice some more. Stopping that dial where you want it, calibrating your eyes for that detailed reading, and getting some of the wheel-isolation techniques down pat all require repetition. Rest your eyes—and wrist!—when you need to. Safe locks are generally static. You can set the lock down and come back refreshed a few days later to pick up where you left off.

In the next chapter, we'll give you the rundown on safe-lock manipulation competitions, including suggestions for organizers and competitors, tips to improve your open times, and common competition rules.

14
SAFE-LOCK MANIPULATION COMPETITIONS

Once you've practiced and grown confident in your safe-lock manipulation skills, you might be interested in joining or even hosting a competitive event in your area. In this chapter, we'll provide suggestions and considerations for competition organizers and competitors, offer tips for both before and during the competition, and share example sets of rules from multiple continents to show how they vary across competition environments.

Safe-lock competitions generally fall into two major categories: either everyone starts manipulating at the same time or competitors can drift in during a set period and try their hand at getting an open. The TOOOL US LockFest manipulation contest is an example of the first category. The participants are all equipped with the same type of lock, which is mounted on the same type of mount and set to the same combination. The fastest three openings win.

But not every event can support this approach; for example, scheduling conflicts and the number of entrants can require multiple heats. Generally speaking, the estimated number of participants, equipment availability, room size and availability, and number of judges and staff determine the way the competition is organized.

Let's look at other considerations you'll need to weigh if you're planning to host your own event.

Considerations for Organizers

If you're running an event, it's *your* event. As long as you keep the competition friendly, fun, and enjoyable for the competitors, it should be considered successful. That said, some planning and work can make the event run smoother. This section offers suggestions, but you should choose what fits best for your competition.

Registration and Divisions

First, ask yourself these questions: Do people have to preregister? Are the registration process and the rules posted well in advance? Will you accommodate last-minute walk-ins and standbys? Will the event have divisions? If you choose to have divisions, you can choose from several possibilities:

Youth Include a separate category to recognize the youngest competitors.

Novice Use a modified lever that gives an initial wheel indication to assist new locksporters trying manipulation for the first time at your event (see "Modifying the Lever" on page 231). Maybe these participants just came from their very first class in a lockpick village.

Amateur Competitors in this division won't need the help of a modified lever, but they've never won. They have opened a lock in the past and should be able to open the lock within the allotted time.

Expert These are previous winners or professional safe technicians. They can always coax a lock open in under an hour.

Open In this division, all approved manipulation aids are allowed. (With the exception of fine-line stickers, most aids are prohibited in categories other than this group.) Consider permitting audio amplifiers, magnifying glasses, dial enlargement attachments, and other aids we've discussed in previous chapters.

Timing and Combination Setting

Randomly starting a search sequence directly next to a set combination number can give a competitor a huge time advantage. For example, if wheel 3 is set to a combination number of 51 and the competitor starts dialing on 50, they might find a gate on the second dial. You could offset this element of luck by having competitors open more than one lock and combining their open times.

If it is a "fastest open wins" type of competition, and people get their lock open early, can they get another lock and try to do better, or is it a one-and-done? Does the competitor's best time stand, or does another attempt always cancel out the previous times?

Some events, especially if they have a single start time, set all the locks to the same combination to try to keep the competition fair. Wandering eyes, notes in viewing range, or accidental audible mutterings could ruin this for other competitors. While limiting the variables in a head-to-head competition can make sense if you can account for these variables, maybe you'd prefer to set random combinations instead.

On a similar note, how are you generating your numbers? Most people will fall into easy traps if left to their own devices, and random doesn't end up being so random. Simple sequences such as 33-44-55 or High-Low-High or Low-High-Low patterns (avoiding the forbidden zone) often pop into people's minds and can feel predictable to experienced competitors. Consider using an online random-number generator for your combinations.

Do you want the first number that competitors set up to test—say, 0 or a number just outside the contact points or forbidden zone—to be a number in the combination? That might make for a fast opening because this is where a lot of folks will start their search. Choosing a number that ends in a 5 will likely also speed up the process, as manipulators will frequently run a dial in 2.5 increments on the 0s and 5s. Avoid using the same number twice in a single combination, as this may throw off their initial wheel readings—unless that's what you intend. Will the last number be within the manufacturer's published forbidden zone? (Hopefully not!)

Combination setting is an all-hands-on-deck, time-consuming task. You'll need to have a second person check every lock to make sure it operates correctly after the combination has been set. The lock should open when it's supposed to and not when it shouldn't. Also have someone check for contact points, as you would hate to hand a contestant a lock that truly isn't readable. Don't forget to check for a loose dial ring; index lines that move about can be frustrating.

Lock and Personnel Distribution

You also need to think about how you'll distribute the locks to contestants, and what to do if a problem occurs. Do you just hand any lock to a competitor, or can they choose one from a pile? Is the event using more than one brand of lock? What happens if someone has an issue with their assigned lock (such as a loose dial ring or stripped back-cover screws)? Can competitors exchange locks after they've started? If they're required to open more than one lock, do you require them to open a different brand the second time?

Make sure you have sufficient personnel available to supervise as well as handle any issues that arise. Several people are needed to watch competitors, run the clock(s), set new combinations, run the desk, answer spectator questions, post timings, and more. Plan accordingly.

The Competition Environment

Most competitors enjoy manipulating safe locks in silence. The fewer distractions, the better. A separate quiet room is great if you have the space, but that's often not the case—not to mention, others usually want to watch the magic happen. Positioning manipulators with their backs to the door will keep them from being distracted from their work every time someone enters. Rope off the competitors so a spectator doesn't wander too closely and throw off their mojo. Also consider placing the help desk out in a hall or less populated area.

Generally, manipulation aids (lasers, audio sensors, and the like) aren't allowed, but will you allow contestants to have their phones on and their earbuds in to listen to their favorite playlist? Will you provide the graphing paper, scratch paper, and a pen? What is your rule about bathroom breaks or leaving to take a phone call? Does the timer stop?

If the time expires or a competitor quits, can they find out the actual combination?

Everyone will want to know the final times. Post them inside and outside the competition room.

Plan an award ceremony and put it on the schedule. Rehearse your presentation. Be prepared for the possibility that the winner isn't present.

Considerations for Competitors

You have put in the work and are ready to jump into a competition, but you're in for a surprise if you think you can successfully try something new on game day or get a super-fast opening on your first try. In this section, we'll offer you tips to consider implementing and, more importantly, practicing, to get yourself competition ready.

Consistency and Speed

Consistency, both in your dialing and contact-point reading, is the key to success in this game of manipulation; it's what allows you to hear what the lock is telling you. Driving or spinning the dial harder and faster than you can accurately interpret is a recipe for disaster. While you may want to spin faster than usual, it's critical that you aren't slamming the lever nose into the cam gate—doing so will absolutely shift your readings. Keep your touch on the contact points consistent. Practice dialing quickly but with an emphasis on getting reliable contact-point connections and readings. A successful opening depends on it.

Use your pregame time to practice your dialing sequence over and over until your readings are smooth, fast, and accurate. Do this with locks that are both looser and tighter than you like. You never know what your assigned lock will be like, and you don't want to be thrown off your game just because the dialing isn't optimal.

Graphing Charts

Eventually, you'll be ready to taper off the lengthy graphing process as you learn to just read the right contact point and monitor it for changes. You might still have notes on the exact dialing sequence needed for isolating wheel 2 or the process for determining whether wheel 1 or 2 is indicating, but slowing down to graph that will chew up way too much valuable competition time.

But that doesn't mean you shouldn't be prepared to graph if needed. What if you get nervous and have to resort to the basics? The tried-and-true fundamentals won't let you down. Always keep some graph paper on hand—not as a crutch, but as a legitimate backup plan.

Simplified Dial Reading

Every dial differs slightly in the width of its index lines, and each has its own feel. Be consistent in the way you read it every time you face a particular lock. Here we'll show you an easy-to-remember dial-reading method that consists of only a handful of increments. It's a little more exact than quarter increments but nowhere near as detailed or time-consuming as tenths. It's a particularly useful system on S&G's chunkier index lines.

Let's use 50 as an example. Working around the dial left, or counterclockwise, you'll use these increments of sixths, using these visual clues to track your contact point readings: 50, 50 Overlap, 50 Aligned, 50 Middle, 50 Next Aligned, 50 Next Overlap, and 51.

In Figure 14-1, the opening index is exactly centered on the number's index line, so this is a reading of 50.

Figure 14-1: A perfectly aligned reading of 50

When the opening index overlaps the number's index line slightly, it's a 50 Overlap (Figure 14-2).

Figure 14-2: If any portion of the number index line is under the opening index, it counts as an overlap, so this is 50 Overlap.

Figure 14-3 shows an example of 50 Aligned: the left edge of the opening index is aligned with the right edge of the 50 index line.

Figure 14-3: Because the edges of the opening and number index align, this reading is considered 50 Aligned.

If the opening index is centered exactly between two number indexes, touching neither, it's a Middle reading (see Figure 14-4). With some locks, this might be a larger space, but this works great on most S&G locks.

Figure 14-4: The opening index appears between 50 and 51, so you'd call this 50 Middle.

In Figure 14-5, the opening index's right side is almost aligned with the number index's left side, so it would be considered 50 Next Aligned.

Figure 14-5: The opening index's right side is starting to align with 51's left side, so this is 50 Next Aligned.

Similarly, when the opening index overlaps the next number's index line at all, the reading is considered Next Overlap (Figure 14-6).

Figure 14-6: Here the index lines are slightly overlapping, which constitutes a reading of 50 Next Overlap.

Finally, because the opening index is exactly centered on the next number (51), Figure 14-7's reading is considered 51, and your subsequent readings will be relative to this number now instead of 50.

Figure 14-7: The opening index is centered on the next number, and the process starts again. This is 51.

If this sixths technique doesn't work for you, you might adopt quarters for S&G dials and tenths for LaGards, with their thin, crisp index lines. Regardless of the method you choose, *practice it*.

Pregame Decisions

You can often take shortcuts during a competition, but keep in mind that most are not risk free. If they fail, you can always fall back on the tried-and-true methods that have honed your skills.

First, be sure you know the rules. Will the organizers set the last combination number in a manufacturer's published forbidden zone? Use this knowledge so you don't waste time searching there when dealing with wheel 3. The forbidden zone is usually 0 through 20 on modern Group 2 locks but varies by brand.

You'll need to make several shortcut-related pregame decisions before you start looking for clues. You don't have to use any or all of the shortcuts presented here. You could build up to adding them as you improve your technique or forgo them altogether.

> While I call them all *pregame* decisions, truthfully I might change my mind depending on my interaction with the lock during my initial diagnostics. Say I've decided pregame to check only the right contact points. If my diagnostics show no concerns, I stick with that decision. If I find an issue, though—such as a dial that's so hard to spin it could easily mask contact-point readings—then I might have to change course by always using both the left and right contact points, lest I miss something.
>
> —BANDEATOZ

Will you spend time looking at both contact points or just one?

> Using just the right contact point not only reduces the time spent looking at contact points by 50 percent but also, and more importantly, leaves you looking at the contact point that consistently has the largest changes due to the lever nose contacting the cam gate. Even a little fence drop is more apparent on the right contact point than on the left.
>
> You'll also need to decide whether you'll run only wheel 3 or all wheels from the start. Each approach has pros and cons. Have a plan in advance and stick to it.

Which way will you dial the wheels to start: AWR or AWL?

> Dialing AWR will facilitate a direct dial into the right contact point, smoothing out your spinning sequence substantially (right spin to the increment, left spin into the right contact point; then right spin to the new increment, left into the right contact point again). You'll find a fast rhythm as you move all three wheels under the gate on your first spin around the dial. If you do an AWL and still just want to test the right contact point, you'll have to dial right a little past it, then left to make contact, and then left to your next increment. While still effective, that little backtrack can slow you down.

Will you be using increments of 2 or 2.5?

You've seen that using intervals of 2.5 is a proven method that gives indications just fine, and it's easy to remember since you're simply moving the dial halfway between the big index lines. Not only that, but it reduces your stops along the dial compared to increments of 2. Still, running the dial by 2s the first time around might settle some competition jitters, ensuring that you see what should be a solid indication.

Will you jump on the first indication or run the full dial?

While you could start finding True Center, parking wheels, and searching for another wheel's number after your first indication, our advice is to run the entire dial to get a good feel for the way the lock communicates. You can often pull more than one of the combination's numbers in that run. You'd also hate to have an anomaly in the wheel give you a false reading only to find the real gate signal loud and clear just a few numbers away.

Then again, you know what good gate indications looks like, so feel free to pounce on the first one if you're comfortable with it. Why keep examining that wheel for another umpteen numbers just to use your hard indication anyway? Be sure to make these decisions before you start; otherwise, you'll get hung up trying to figure out what to do in the moment.

If you spin all three wheels for your first run, will you assume it's wheel 3 that's indicating?

As mentioned in Chapter 13, in our experience 75 percent to 90 percent of all locks indicate first by third wheel, then second, then first. If you have to guess, run with wheel 3 as your first indicated gate. Again, also know your lock's forbidden zone. If you start the event assuming that wheel 3 will indicate first, you don't want to spend any time in that lock's 20-number forbidden zone. You could skip it when looking for indications—there's no sense looking for or dialing there for wheel 3's number if it won't mechanically work.

Game-Time Tips

Now imagine you're at the competition and just received your lock. The first thing you should do is run your diagnostics. Do all the wheels pick up? How freely does the dial spin? Is the dial ring loose? Are the contact points sharp? Evaluate the index lines. Are they thin or thick? Are they sloppily painted? Will any of this change your pregame decisions? Use this diagnostic time to get a feel for how well this lock talks to you.

We recommend using only the right contact points unless and until things go wrong. If they do, bring in the left contact points to bail you out. Check these in larger increments—5 or so—and only in the vicinity of any previous clues or indications.

If you're not getting any indications when dialing at your preplanned 2.5 increments, jump down to increments of 2. Are you still reading your contact points consistently? Sometimes a 0.4 can look like a 0.6 as your mind drifts.

When your lock supports it, oscillate over the drop-in area every time. Again, consistency is key. Sometimes you'll need an extra five seconds of solid oscillation to get a drop. Often this is time well spent, especially if you're just dialing for your last number.

Remember: breathe. Find your rhythm. A ham-fisted manipulator that spins the dial faster than a Formula 1 racecar, only to crash it into the lever nose and the drive cam, will likely suffer. You need gentle, consistent contact between them to see the fluctuations you're after.

Say you get a good number indication on a wheel during your first pass, but progress stalls. You've tested the number, and it indicates the expected third wheel. Using this information, you start parking wheels, but you still end up getting nowhere. In this case, you've probably indicated the incorrect wheel. Save yourself the time to retest and go ahead and run the indicating number as wheel 2 and see what happens. Often this will solve your dilemma.

If wheel 2 indicates first, park wheels 1 and 2 in the middle of wheel 3's forbidden zone, and when you run the dial (skipping the forbidden zone numbers), you can be positive it's wheel 3 indicating. That's a fast two out of three.

Now you've found two good numbers and are brute-force dialing for the third—but you've made an entire pass, and the lock didn't open. While you generally don't have to read the contact points for your last wheel's number, doing so could give you a clue if you've misidentified a previous wheel's number.

You've run the dial every which way, parked the wheels just so, and you have two numbers indicating. Brute forcing might very well work. If it doesn't, keep in mind that by jumping around the dial in 2.5-number increments, coupled with some unlucky oscillation, you might have missed that there are only two numbers in the combination! Sometimes two wheels do have the same number, or nearly the same number with the movable fly separation. Work these two numbers in the only three possible ways they can be positioned.

Competition Rules

There's no wrong way to hold a competition, but there is a wrong way to compete: by failing to follow the rules. Having competition rules clearly laid out will benefit both contestants and the organizers, and will go a long way toward preventing misunderstandings.

In this final section, we'll look at a couple of example sets of rules from various countries. Keep in mind that they're just that—examples—and won't fit all competition settings.

Example 1: The Czech Lockpicking Championship

The Czech Lockpicking Championship hosts a variety of events at its get-together. These easy-to-follow rules were used during its 2019 Safes–Mechanical Combination Locks competition (see *http://lockpicking.team/en/competitions/*).

Allowed tools

- Magnifying glass, removable tag with scale, mechanical arm to aid determining dial position
- Pen and paper

Prohibited tools

- Electronic devices and other devices that automate dial movement or measurements of the dial position are prohibited.

Requirements

- Arrive early (at least 15 minutes before the start of the competition).

Rules

- Group 2 combination locks will be provided by the organizers.
- The locks will be installed on stands simulating safe doors.
- The seats will be assigned randomly.
- The opening time limit is 60 minutes.
- The competition will have only one round, with all locks set to the same combination by an independent referee.
- The rules for this competition may still change depending on available time.

Additional info

- The maximum number of participants is 28 (in the order of registration).
- The lock is considered open when the locking bolt is fully retracted.
- When the contestants open the lock, they indicate this to the referee by saying "Open!" out loud and raising their hand. The referee then informs the contestant about their opening time, and the contestant writes down the time on the provided sheet.

Example 2: The Safe & Vault Technicians Association Competition

This example comes from an annual Safe & Vault Technicians Association competition held in the US.

CONTEST RULES FOR THE NOVICE AND EXPERT	
1. Locks will be chosen by a random drawing supervised by the contest	**CATEGORY SELECTION:** 1. New contestants will be allowed to

proctor. The locks provided will be the Big Red CDL-3-000, the LaGard 3330, and the Sargent & Greenleaf 6730.

2. Timing begins when the contestant first touches the dial.
3. Timing ends with retracting the lock bolt and manually stopping the stopwatch.
4. Contestants may compete five times during the contest. There is no waiting period between attempts; however, after any attempt, the contestant must go to the end of the line.
5. All lock openings must take place during the posted hours of the convention exhibits.
6. Contestants may not use any mechanical or electronic aids. The use of hairline indexes is allowed and will be provided upon request.
7. Any attempt to open a lock by means other than manipulation will result in immediate disqualification.
8. There will be a two-hour time limit on each manipulation attempt. If a contestant must leave the room during this period, they will be accompanied by an official monitor and the timing for that will continue while the contestant is out of the room.
9. If the exhibit floor closes during an opening attempt, that attempt will be counted as unsuccessful.
10. Rules' interpretations are left to the judgment of the contest proctor.

compete in either the Novice or Expert category.

2. Any Novice contestant that places twice in the top three opening times will be required to compete in the Expert category in all future contests.
3. Any Expert contestant that places in the top three opening times will be required to compete in the Expert category in all future contests.
4. Once a contestant begins manipulating a lock, the category cannot be changed during the contest.

NOVICE CATEGORY:

1. The contestant who opens a single lock in the shortest amount of time will be named the winner.
2. The posting of a subsequent slower time for an entry will negate any previous entry posting a faster time.

EXPERT CATEGORY:

1. Each contestant must consecutively open two locks from the contest, with each lock being of a different manufacturer.
2. There is a two-hour limit on each opening attempt, with the combined opening time of both locks constituting one entry.
3. An opening time cannot be improved upon within an attempted single entry.
4. The contestant with the lowest combined opening time for a single entry will be named the winner.
5. The posting of a subsequent slower time for an entry will negate any previous entry posting a faster time.

As you can see, no matter where they're being held or by whom, locksport events primarily want folks to dial fast, play fair, and have the flexibility they need to meet their circumstances.

Summary

You've practiced and have a game plan. Now get out there and take a risk. Enter a competition. Live a little; learn something about yourself; make friends and exchange some witty banter about going down in flames or succeeding like you knew you could. Better yet, set up a class, teach your friends your newfound skills, and then run your own event at your next conference, lockpick village, or meetup. *Dial smooth. Open fast*.

That concludes this part of the book. In Part V, we'll switch gears and cover the fundamentals of lever lockpicking, beginning with a brief discussion of the history of lever locks and the difference between single- and double-bitted versions.

PART V

LEVER LOCKPICKING

Unless you live in the UK, the Netherlands, India, or Australia, or have a keyed safe or safe deposit box, you've likely never interacted with lever locks. In this part of the book, we'll cover the fundamentals of their operation, walk you through how to open them, and give you tips on preparing for competitive lever lockpicking events.

Although the lever lock is the main security element on many British wooden front doors, it has often escaped attention within the locksport community because of its cost and overall scarcity. Another contributing factor is that it's difficult to make lever locks less secure in order to get started picking them without stopping them from working properly later; simply taking one apart is easy, but you'll have to think and work hard to modify and then pick a two-, three-, and then four-lever lock before attempting the lone five-lever lock you started with. Not only that, but the tools are a bit harder to get, and certainly more expensive than others you've seen.

> I've been a professional locksmith for over 18 years now, though I am almost entirely self-taught, and I found lever locks to be the one area that merited a long, expensive training course.
>
> —NIGEL

Fortunately, we'll be discussing ways around all of these issues throughout the next few chapters so that you can experience the thrill of opening this less common lock format. First, though, let's go over some history and basic concepts.

A Brief History of Lever Locks

You can often find secondhand basic lever locks with little security, as well as warded locks with even less, in reclamation yards and antique shops. This might be why there's a perception in much of Europe that lever locks are old-fashioned. They *are* old, but so are all major lock types.

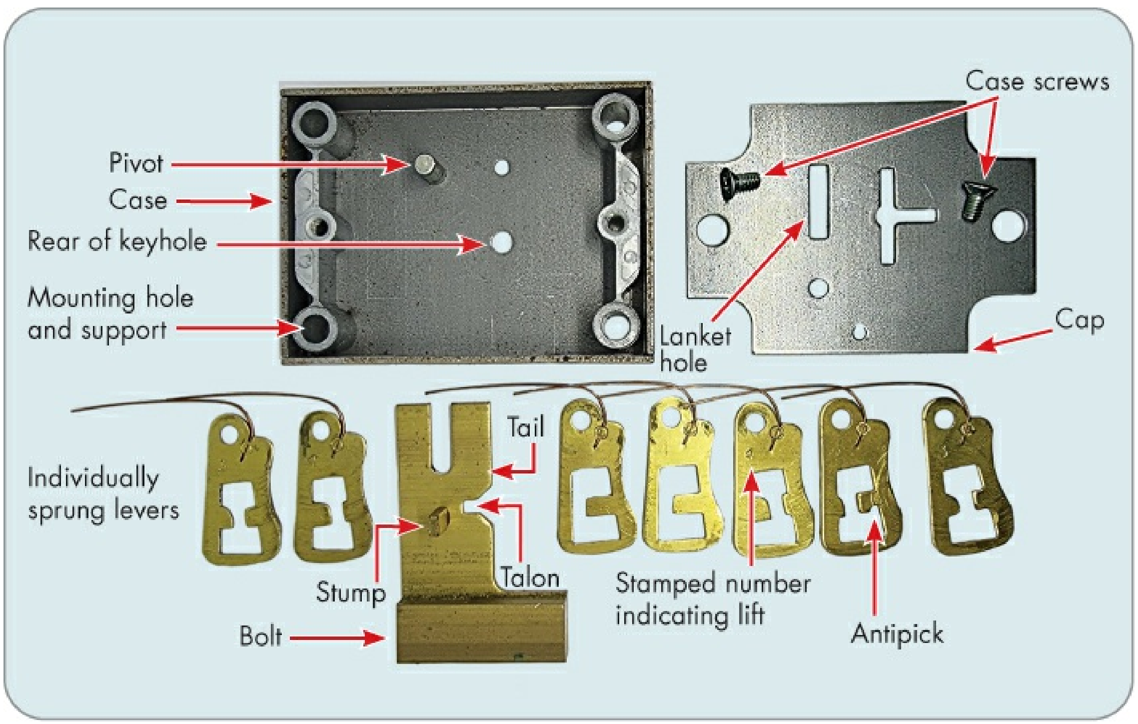
The most recent lock design to become popular, the ABLOY-style disc detainer, is "only" 120 years old. Pin tumblers have been around some 6,000 years—so lever locks, being only about 250 years old, are relatively young. That said, warded locks, which look similar and are essentially the precursor to lever locks before levers were identified as such, *do* go back a long way. *Wards* are simply fixed obstructions, such as bumps or protrusions, inside the lock, and they come in many forms.

> I love to collect warded locks and figure out their flaws and imperfections, as well as marvel at how such wonderful, intricate things designed to resist attack have lasted for, in some cases, hundreds of years of daily use.
>
> —NIGEL

We'll discuss warded locks in more detail in the next chapter. For now, it suffices to say that once the more secure lever lock was invented, many manufacturers swapped production from warded locks and came up with their own (sometimes outrageous) designs for lever locks, often to get around patents.

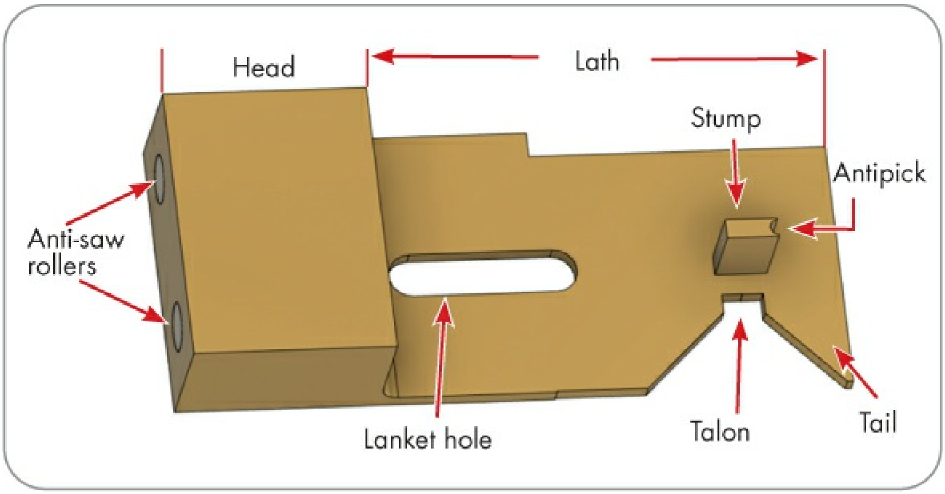
Components of a Lever Lock

The following figure shows the parts of a typical, fairly cheap, seven-lever, single-sided safe lock. Let's break this down and take a look at how these components work.



The Bolt

As with the safe lock just shown, and those combination safe locks discussed in Part IV, the moving locking mechanism in lever locks is called a *bolt*.



Each lever in the lock has a notch or gate (like those you saw on safe-lock wheels), and the levers in the lock pivot, slide, or rotate—or some combination thereof—to block the movement of the bolt. When you turn the key, its bitting lifts each lever to the correct position at the precise moment to allow the *stump*, a metal protrusion on the bolt, to align with the lever gates and retract the bolt.

In some designs, the stump is part of the lever (in single-lever locks) or even the lock case itself, but generally it's part of the bolt and the same depth as the bolt head. Sometimes the stump will have *antipick notches* (or just *antipicks* for short) that interact with the levers as an added security measure. The V-shaped *talon* is where the key or a *curtain*—a rotating ward that blocks off the keyway to thwart picking attempts—pushes to *throw* the bolt. A lock with multiple throws—that is, requiring multiple turns of the key—will have multiple talons to match.

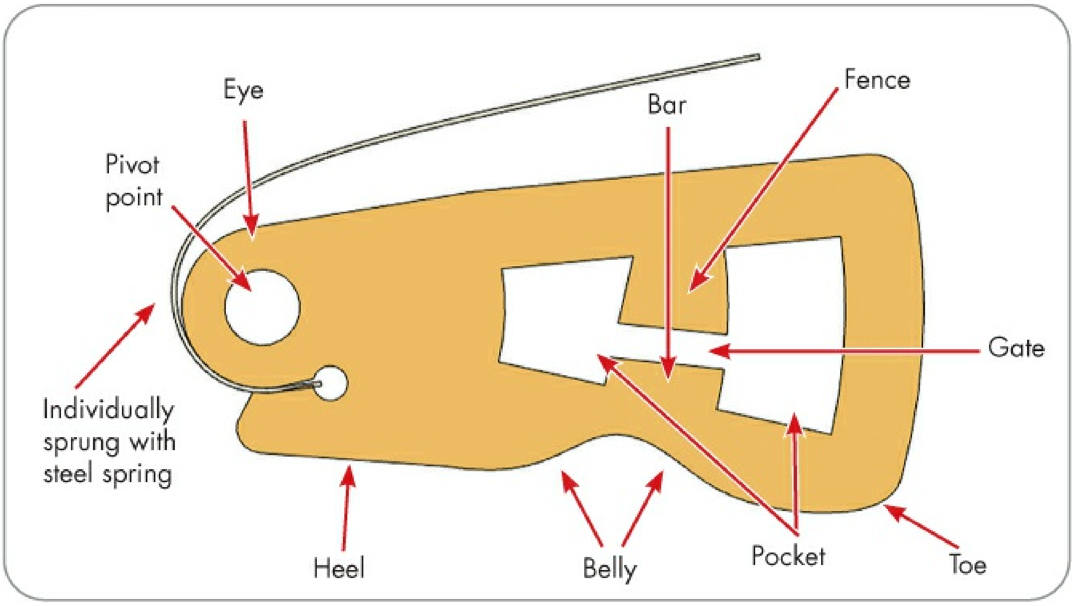
The *lanket hole* is there to limit the sliding travel of the bolt, and is either in the bolt per the preceding diagram, or the bolt stump stops on the case, per the first photo. The bolt must not come out the front of the lock case! The *lath* is the thinned section of the bolt.

Bolts are commonly made of steel these days, but they can still be found made entirely of brass, which is far easier to work with by hand, a big advantage for early lock manufacturers across the heart of England. Small locks for cupboards and the like are frequently still just brass, as are many older safe locks. The self-lubricating nature of brass means that while it is strong enough to resist force, it cuts and machines nicely, which is useful for making complex parts—and the bolt is almost always the most complex part of a lever lock.

Of course, ease of cutting isn't an advantage for a door lock, so most security-rated locks add *anti-saw rollers*, a set of loosely secured steel rollers in the bolt head, which will spin freely under a hacksaw blade (or similar) to thwart cutting attempts. Many locks have two anti-saw rollers, as shown in this design.

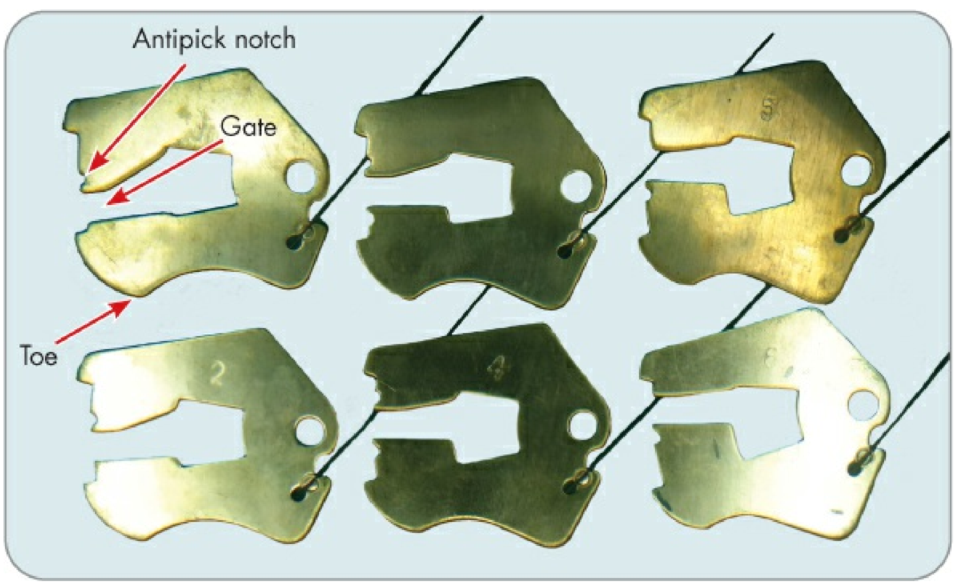
The Levers or Detainers

As for the levers themselves, many variations exist. Every lock model has different levers, but this one from a three-lever Legge is a good illustration of the common parts.

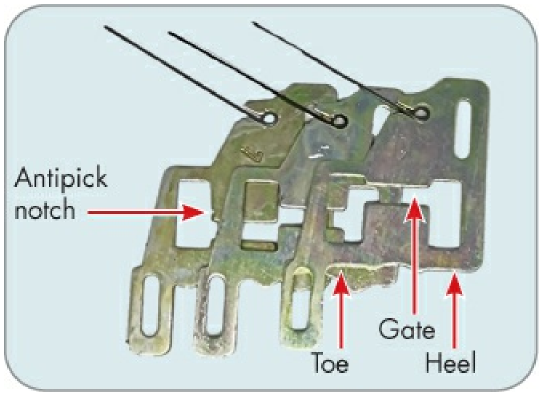


You can clearly see the gate in the *pocket* where the bolt stump aligns to open the lock, as well as the *pivot point* where the lever is lifted by the key. The *belly* is the area where the key interacts, flanked by the *toe* and *heel* in the front and back of the lever, respectively. The toe is on the bolt side, and the heel is to the rear.

Another type of lever, commonly known as a *detainer* (as we'll discuss in Chapter 15), doesn't have a fully enclosed pocket but instead has open gates. These detainers are from a UAP ICL (now MAX6MUM) six-lever lock, and the lift height is stamped on each.



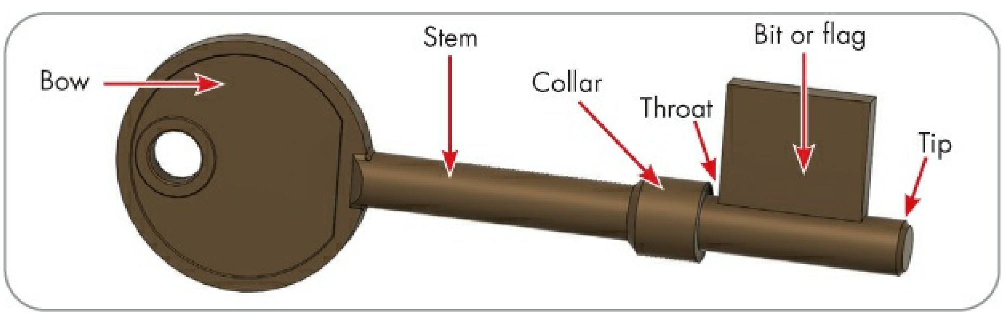
Another variation is the sliding lever, shown here from Legge.



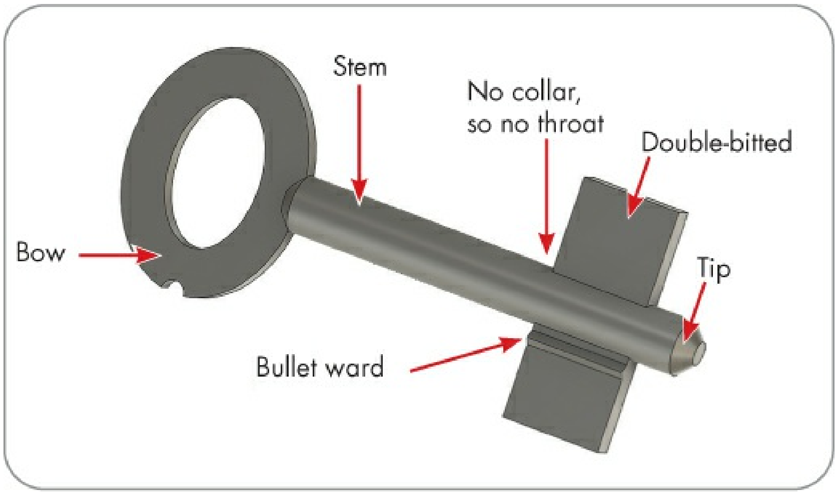
In the unusually shaped S&G eight-lever 6804 safe lock illustrated here, see if you can discern the same features you've seen in the previously shown levers.

The Keys

Lever lock keys are either single-bitted or double-bitted; a *flag*, sometimes known as a *bit*, is the part of the key that interacts with the levers. In this typical single-bitted blank, the *collar* stops the key against the near side of the lock case, at the correct depth from either side to prevent it from going all the way through the lock. The *throat* width matches and clears the case's thickness, allowing precise alignment under the levers from either side.



In this typical double-bitted blank, a *case notch* in the bow works with a case ward (an obstruction in the lock case, not pictured) and the *bullet ward* (the triangular section on one flag) to prevent the key from being inserted upside down or too deeply, stopping against the far side of the lock case. We'll talk more about the many types of wards in Chapter 15.



NOTE

Single-bitted and *double-bitted might be considered misnomers. Technically, a* flag *is the uncut part of the key attached to the stem, and a* bit *is a cut in the flag (and, as you've seen in earlier chapters, the full pattern of cuts is the key's* bitting*). Thus, a double-bitted key could have much more than two bits, but it will always have only two flags. Once a flag is cut, it's referred to as a* beard. *For simplicity's sake, we'll use the term* flag *for the protrusions from the key's stem and* bit *for the cuts in the flag.*

Notice that the stem on both of the keys shown here is solid, meaning these are *pin keys*. Some lever locks use *pipe keys*, which instead have hollow stems. We'll discuss pipe keys further in Chapter 15.

Lever Lock Categories

Lever locks are grouped in many ways; in fact, you'll rapidly notice that there are nearly as many possible groupings, and locks that don't quite fit into them, as locks themselves. To prevent confusion in the chapters that follow, here we'll define a few of the more common categories you'll encounter.

A *sash lock* incorporates a latch mechanism to hold the door shut without locking it, whereas a *deadlock* has only the locking bolt thrown by the key. Some locks combine both actions into a single mechanism, and others use the latch mechanism as a lock if the key is used. For example, some sash locks have no handle, so the key must be used to open the door. Generally, though, a sash lock has handles, and a deadlock doesn't.

A *rim lock* refers to a lock screwed to the face of the door, and a *mortise lock* fits into a pocket mortised out of the door. Again, some locks are a bit of both, but most clearly fall into one category or the other. Still others are also fitted with an interchangeable cylinder, as you've seen in some of the locks from earlier in the book. However, generally, the term *mortise lock* refers to a lever mortise lock, and a *night latch* refers to a key-operated cylinder-and-rim-lock combination.

With the bolt thrown, the rim lock shown next is also a sash lock. You can also see a modern, five-lever deadlock below it, mortised into the edge of the door, to provide insurance cover according to the specifications of the British Standard.

Finally, you might hear references to a *Chubb lock*, which is a colloquial term for a lever lock (either a sash lock or a deadlock), taken from the Chubb manufacturer's characteristic design and key shape. Meanwhile, a *Yale lock* refers to the latch-bolt-style rim cylinders that you saw in Chapter 2.

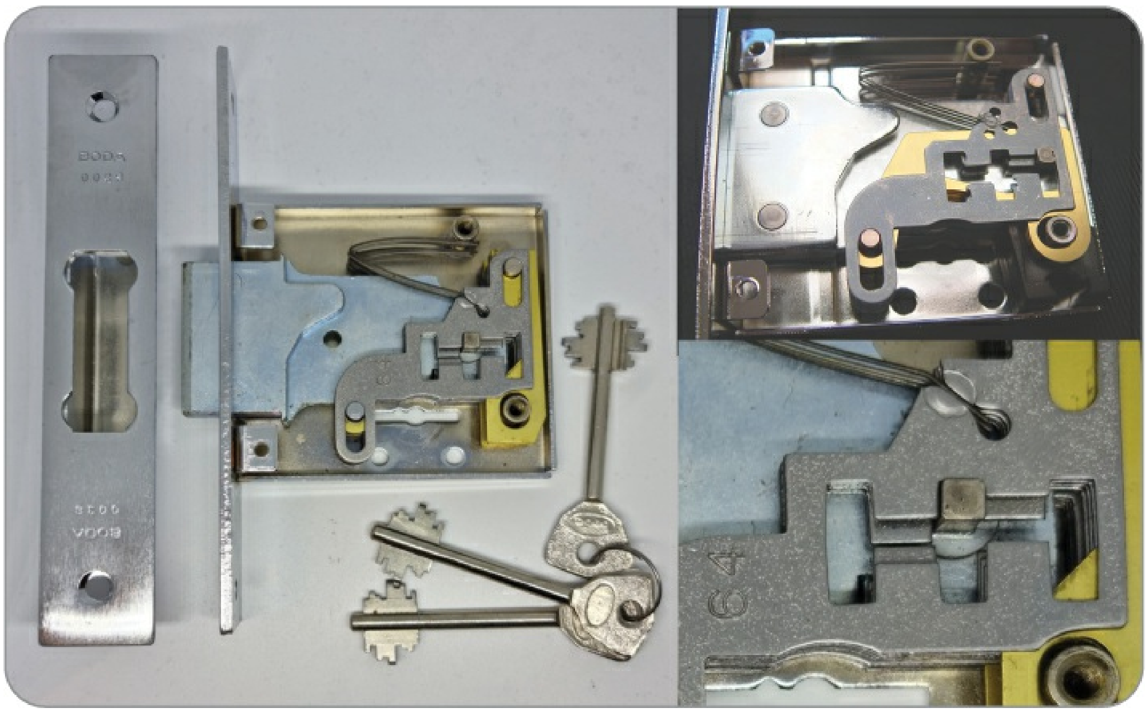
Modern lever designs have settled into two main camps: single-bitted, curtained locks and double-bitted, noncurtained locks. In the UK, insurance policies require that a lock meets the British Standard and includes at least two antimanipulation devices, so the inclusion of antipick features and curtains has become customary. The use of the curtain almost dictates the use of a single-bitted key for reasons we'll go into later, so all current British Standard lever locks have a curtain and a single-bitted key. One example is this T. Morgan & Sons non-insurance-rated, five-lever, curtained deadlock.

Double-bitted, noncurtained locks are found in Spain, Italy, and many other southern

European countries, marketed as *multithrow multipoint-locking systems*, and also in Finland, where ASSA ABLOY produces the more traditional BODA lever locks, like the ones shown here.

NOTE

Multiple throws refers to turning the key more than once (commonly twice), while multiple points refers to a lock having bolts in more than one position, not just where the lock is.



In the older version of this double-throw BODA 429 lock at left, the key would be turned 180° (meaning the bolt is thrown once) at this point, and the levers check the key bitting twice, for a full unlock. The stump extends on both sides of the bolt, with four levers on each side. In the close-up at the bottom right, you can clearly see the stump located between the two sets of gates. The newer version of the lock (top right, the model 428) has square gate antipicks, as well as a matching antipick notch on the stump, both of which are features designed to trick lockpickers into thinking the stump is properly aligned with the lever gates. All three photos show the small triangular ward cutout that stops the key against the rear of the case. Notice that the simple ward makes the new blank key and the old blank different. This is the only difference between the same-age models 428 and 429.

We'll go over how to work around such measures, and much more, in the coming chapters. Let's get started by looking at the tools you'll be working with—first and most importantly, the locks and keys themselves.

15
LEVER LOCKPICKING TOOLS

Lever lockpicking tools can present challenges for locksporters. They're often tailored to specific locks, difficult to find, and costlier than other locksport gear. As a result, and fortunately for us, competition hosts tend to supply both the locks and the tools for opening them. But while this chapter could easily have been the shortest in the book, it's important that you understand the tools you might encounter at events, as well as the mechanisms in lever locks that make picking possible.

The first and most important piece of equipment is, of course, the lock itself. We'll discuss types of warded locks and lever locks, including their keys and other components, and then turn our attention to the specific tools you'll use to pick them open.

Single-Acting Warded Locks

The earliest warded locks in the UK, still found on old churches and the like, used only one lever, meaning if the lever was moved too far out of the way, it would never block again. To "pick" such a lock, you simply hit or lift that lever a little or a lot until you can withdraw the bolt—it can't be lifted too far. The wards on the inside of the lock match the holes and cutouts on the key.

This design had several issues, the first of which was the relatively limited complexity of the key. In a warded lock, material is removed from the key to match the wards in the lock, as shown in Figure 15-1.

Figure 15-1: A single-bitted pin key for a warded lock

In the single-bitted key shown here, one half of the flag throws the bolt, and the other moves the single lever. You can see that the bitting closely matches the wards, but that's not required. The lock can't tell if too much material has been removed from the key (only if too little has, or in the wrong place). Therefore, to open such a lock, you could simply *skeletonize* the key—cut away much more material—being sure enough metal remains that the key doesn't bend or break (see Figure 15-2).

Figure 15-2: A skeleton key

Figure 15-3 shows a basic pick skeletonized from a flat steel plate. The skeletonization means the tool will work against many warded locks with this style of warding, if the sizes match closely enough. Warded locks tended to be really large to allow for more key variation and higher security. Sets of similar skeleton or *tryout* keys are commercially available.

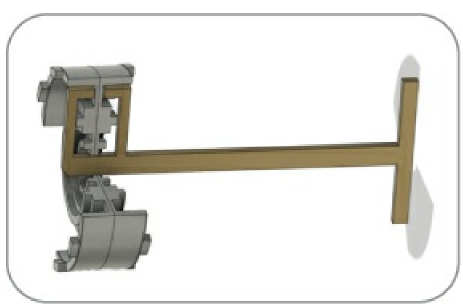


Figure 15-3: A flat, steel picking tool

Another, more flexible option for opening this style of warded lock is to use a pair of wires—one to lift the lever and the other to retract the bolt. Which wire performs which task depends on which side of the door you're on. Figure 15-4 shows the required wire pattern overlaid in blue.

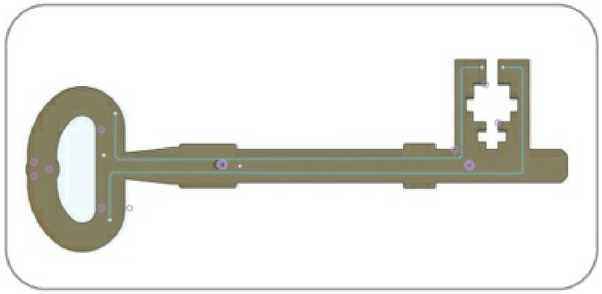


Figure 15-4: Bending two wires to the shapes shown here would also allow you to pick a basic warded lock.

Types of Wards

Wards, or fixed obstructions, have been around since the invention of locks. They may consist of one or more pins, flags, or plates—or whatever else the designer comes up with! The most common type you'll see in a double-sided lock is a *bridge ward*, fixed to the middle of the lock case, as shown in Figure 15-3, and the sash lock in Figure 15-5.

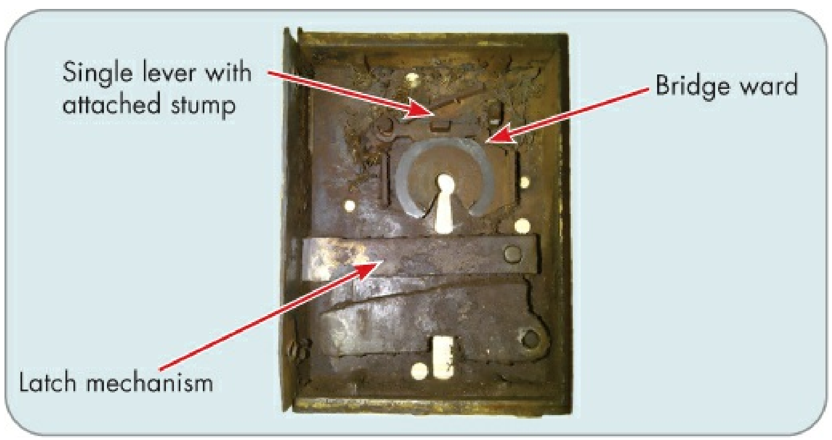


Figure 15-5: An antique bridge-warded sash lock still in use at a stately British home

This is an unusual, early, bridge-warded rim sash lock with weighted (gravity) latching. Notice that the latch is below the bolt and keyhole, and the case was clearly designed to be screwed to the edge and rear of a door.

You can see on the bridge ward where the circular arc of the key has worn away the rust on the inside of the lock case. Note also that the single-acting lever has an attached stump, and the lever's pivot point shows wear, resulting from hundreds of thousands of uses over hundreds of years.

Other types of wards include the following:

The keyhole

The keyhole itself is a ward. The extent to which it hinders access depends on its size and shape, of course. The keyhole is often also used to *stop* the key via the collar or tip.

French warded locks from the 15th to 18th centuries took this to extremes, including complex and beautiful keyholes. An extended keyhole is called a *nozzle* (see Figure 15-6).

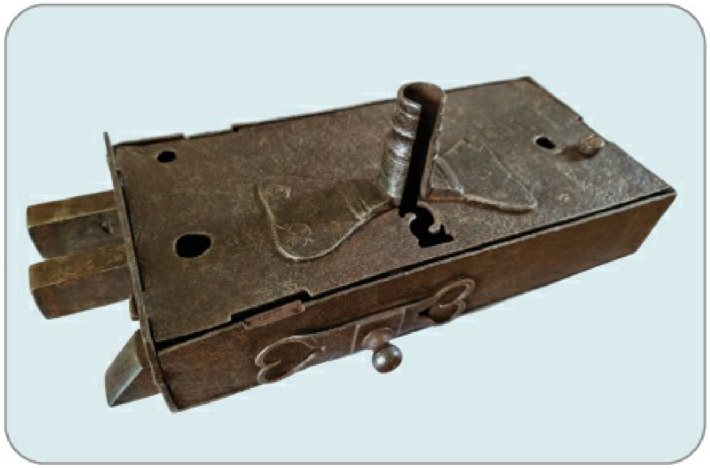


Figure 15-6: A nozzle keyhole

Bullet ward

This is a triangular or other protrusion along the key in the direction of the insertion, as shown earlier on page 286. It's visible from the outside of the lock, usually as a notch or tooth in the keyhole outline, as in Figure 15-6. A bullet ward is often used in lieu of an expensive collar to prevent the key from passing through a double-sided lock, and to increase the number of key *differs* (the unique keys possible for a given lock). It offers the lowest level of security, though, as it can be easily bent or removed from either key or lock housing. Bullet wards are used in a few modern lever locks for blank restriction, and they form the keyway profile in nearly all pin tumbler locks.

Case (or sash) ward

This is simply a ward on the inside face(s) of the lock case, on either or both sides. Case wards are concealed from view and hard to reach to attack. Higher-security locks use inset brass "bushings" that were turned on a lathe and surround the key, offering better warding against wires and skeleton keys. Cheaper and older door locks rarely have case wards on both sides of the lock, and are often simply stamped and formed into pegs or teeth from the bent material of the case itself. This leaves far more free space for picking tools.

Hook ward

Similar to case wards, these mostly appear on single-sided warded locks, such as a padlock or furniture lock. The corresponding ward cuts are usually just on the end of the key, and turn the key ward cuts into a hook shape to match.

Drill pin

These large metal pins are often used on single-sided locks to ward the keyhole, frustrating efforts to use the wrong key or a wire. Further, for some locks they're used for master keying. By using a long, fat pin on one lock, and a shorter, thinner pin on another, you could differentiate two pipe keys that otherwise look identical. The servant key could have a shallower and narrower hole, which would be blocked by the longer pin in one lock, and the master key would have a deeper, wider hole, allowing it to fully enter both locks.

> This is a very effective technique. From personal experience I can say that drilling deep, thin-walled holes into cast keys is nerve-racking, even with modern equipment. Three hundred years ago, few people could have done it. And, of course, undoing such a change would be impossible, and proof of guilt after the fact.
>
> —NIGEL

Mastering/moving ward

You might see this on a double-throw lock, which has an additional ward on the bolt that moves with the turn of the key. The idea is that a servant key would operate only the first throw of the bolt, and the master key would operate both throws. The second throw moves a ward on the bolt forward to block the servant key's operation.

Curtain

As noted previously, a curtain is a moving ward that blocks the keyway. When the proper key is inserted and turned, the curtain rotates with it, allowing access to the levers.

CURTAINS

The *curtain-and-barrel*, usually just called a *curtain*, is the most common ward in modern locks. The *barrel* is a collar that holds the working end of the key, and the curtain is connected to it, blocking off the keyway to prevent picking tools from accessing the levers. When the key is inserted and turned, the curtain rotates as well, taking up free space for picking tools and limiting the key's movement. A curtain acts as a great defense against *J wires*, the main form of attack on a warded lock, and also restricts the movement of skeleton keys in the keyway.

However, curtains are rare in warded locks, having been invented much later than lever locks. The first curtained locks appeared in 1830, but it wasn't until 1852 that Chubb Locks patented them as a defense against the picking tools that locksmith Alfred C. Hobbs had successfully used against its flagship Chubb Detector (at the same 1851 Great Exhibition where he defeated the Bramah lock, as mentioned in Chapter 1). As a result, many lever detector locks were retrofitted with curtains.

Most curtains also incorporate a bolt thrower. This has many advantages, the main one being that it strengthens the action of the lock because the entire key, rather than just one or two bits, is now turning the curtain to drive the bolt.

Here you can see two curtains from British Standard lever locks. On the left is a cast brass, semiconcealed curtain, which becomes visible only when it is turned in the keyway, from a Generation 1 ERA Fortress. On the right is a Chubb 114 curtain.

You'll need very different tools for curtained locks than for noncurtained locks, though the locking mechanisms and principles are similar for both.

The finest wards were expensive and time-consuming to make, as were the matching keys, and regardless of the warding, a single lever wasn't terribly secure. Impressioning was a big risk. The clever engineers of the time sometimes added one or more single-acting levers, but even these could simply be lifted right out the way by any tool longer than the keyway—similar to comb overlifting in Chapter 6. Thankfully, English locksmith Robert Barron came up with a more secure solution.

Double-Acting Lever Locks

Barron's invention of the *double-acting lever lock* in 1778 changed the shape of security forever, inspiring Linus Yale Jr. some 80 years later to augment his father's original design with the same double-acting mechanism and turning Yale into a household name worldwide. Now, you could no longer lift the *tumbler*, as Barron called it, as high as you needed to open the lock; it had to be lifted to the correct place. Suddenly, reaching the moving parts to open a lock required skill, rather than just a tool that would fit. Let's look at examples of these locks and the components you might encounter while working with them.

While you can still buy cheaply made stamped, warded, and one-lever locks to this day, they are shadows of their former selves. Modern five-lever (and upward), double-acting lever locks are much more secure, self-contained units that feature high mechanical strength and few weaknesses.

The bolt in lever locks travels along one axis, typically sliding in and out limited by the lanket hole, and so can't (or shouldn't be able to) leave the case. The levers stop the bolt from moving by physically blocking its travel unless they're lifted to the correct height to allow the stump to clear the lever gates. In traditional levers, the gates are contained completely within the lever body.

In a variation on this design, the gate is open on the end for the bolt to slide through. Though these are commonly known as *detainers*, a true detainer such as the Chubb 110 has at least one notch cut out of the front edge, which makes the lock able to be master-keyed securely. Patents and trademarks for these designs have come and gone over more than 250 years, and the terms *lever* and *detainer* are often used interchangeably. Figure 15-7 shows examples of each.

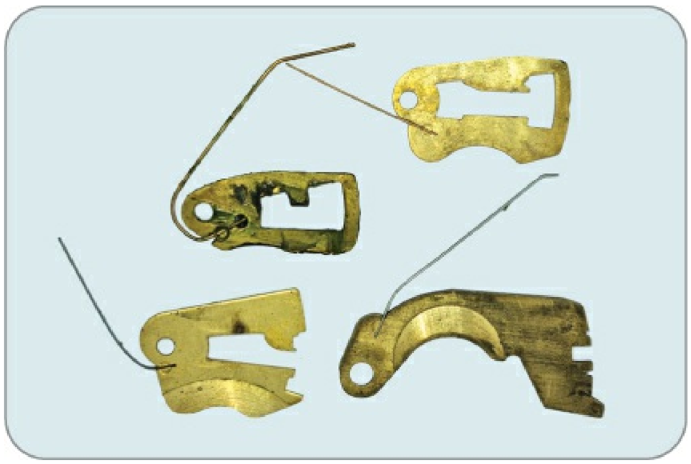


Figure 15-7: Clockwise from bottom right: a Chubb 110 detainer, an ICL/MAX6MUM detainer, a lever from a random three-lever lock, and an unused lever from a prototype lock

The key, with or without the aid of a curtain, lifts the levers, aligns the gates, and drives the bolt through the aligned gap as it turns farther. It's a simple but effective mechanism, and lever locks commonly have just two or three moving parts beyond the levers (see Figure 15-8, and the image on page 282).

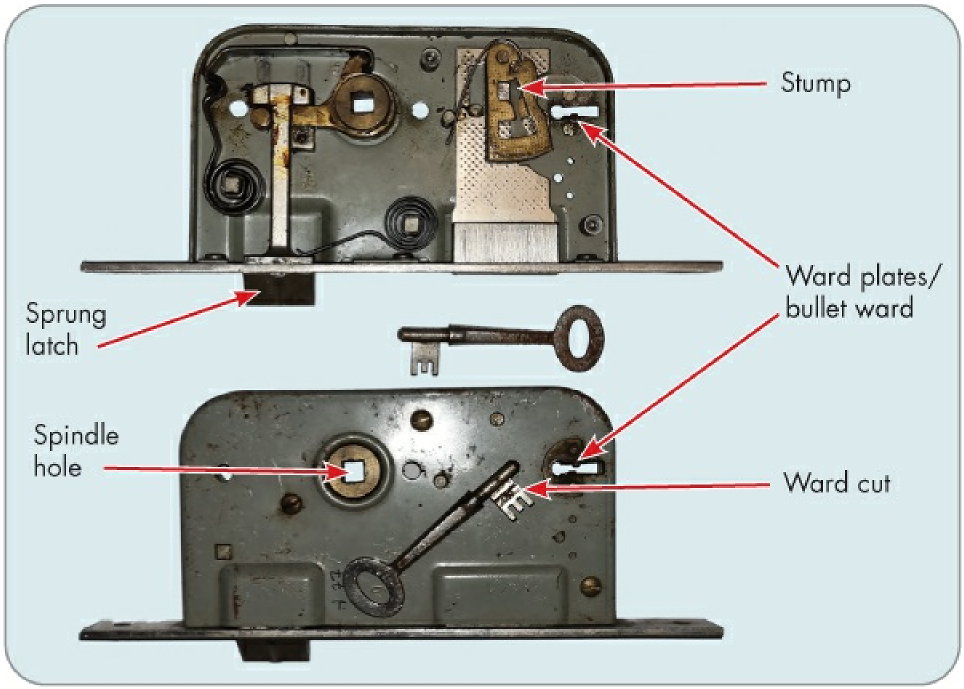


Figure 15-8: A Dutch three-lever sash lock from LIPS. Notice the ward plates, which are riveted to the keyhole and so can be easily changed at the factory, and the matching bullet ward in the key.

In the five-lever lock shown in Figure 15-9, the curtain is turned clockwise to the position at which it starts to try to drive the bolt to the right. The curtain spring keeps the curtain from turning for reasons other than the key's rotation, such as the door slamming. Behind the visible lever, you can see a brass, friction-reducing spacer; there's one between each steel lever. The levers in this lock slide vertically on two stumps.

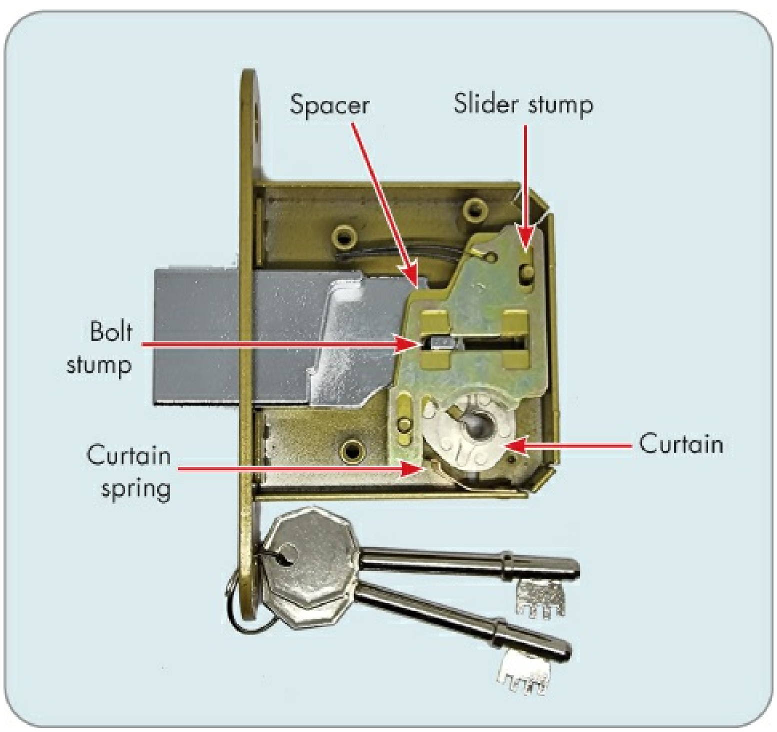


Figure 15-9: An Asec British Standard five-lever deadlock

Lever locks at the opposite end of the simplicity scale look like a fine wristwatch inside. Figure 15-10 shows a high-end safe lock designed such that you can immediately code in any suitable key without disassembling the lock. Coupled with a spring-loaded blocker to make manipulation harder, this makes this lock more complex than most lever locks.

The spring-loaded blocker, attached to the rear of the bolt head, means that any tension prevents further movement of the levers, or, at minimum, gives false feedback to the picker. The white plastic spacers between each lever not only ensure smooth operation but also make some high-end attacks, such as optical decoding, more difficult by filling the space between the levers and the other gaps (which also makes it harder to maneuver lockpicking tools).

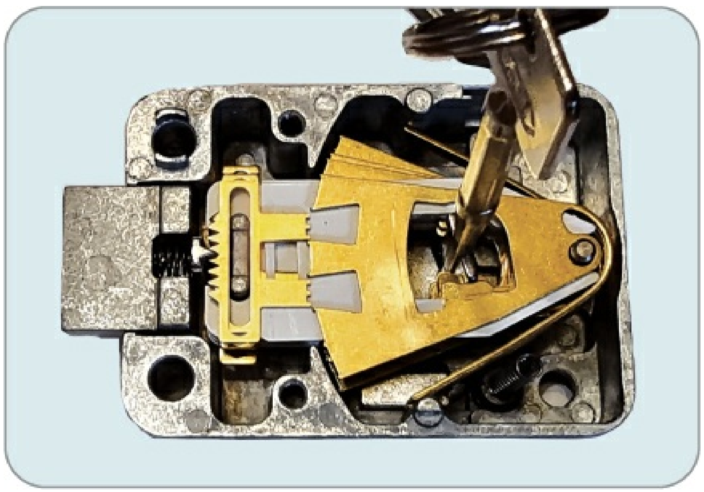


Figure 15-10: A high-end safe lock, the S&G/FAS 6890

Another noteworthy design is the rather complex ERA Vectis, a multipoint door lock, shown in Figure 15-11. It contains 5 tiny levers as well as 14 (!) case screws and all the moving parts to operate the 3 locking bolts.

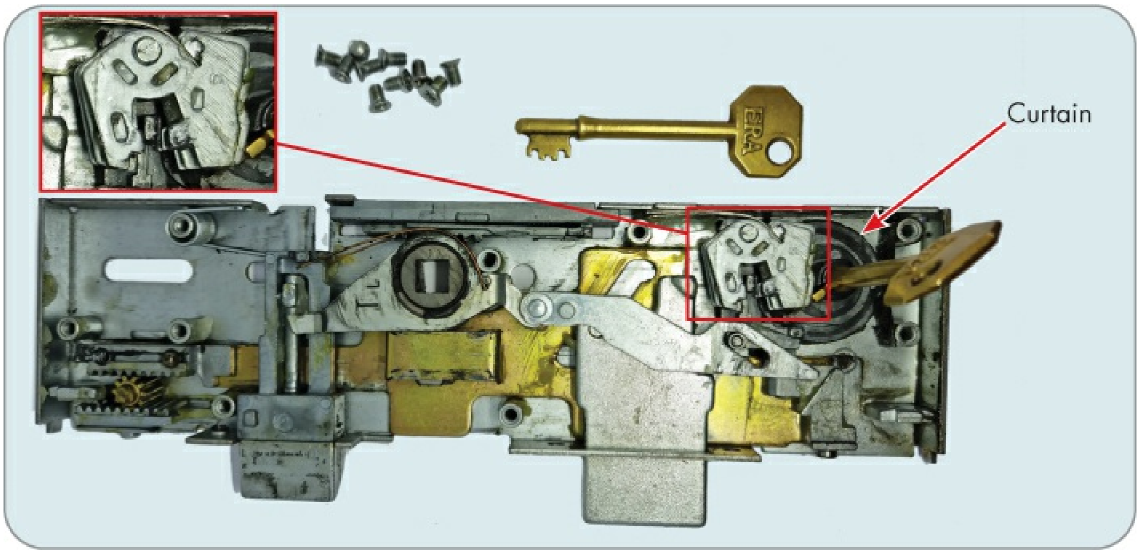


Figure 15-11: In this ERA Vectis multipoint lever lock gearbox, the key is partly turned in the curtain, and the stump has mostly cleared the aligned gates of the lever pack. Unusually for a door lock, the stump is not a part of the bolt, and the bolt is a constant thickness, so it has no lath.

Now let's move outside the lock to take a closer look at how lever lock keys operate.

Lever Lock Keys

Lever lock keys look like warded keys, but they contain far more information. Let's look again at a warded key (Figure 15-12).


Figure 15-12: A single-sided pipe key with a complex ward structure

This is a pipe key, which has a hollow stem like a pipe to fit over the drill pin in the lock, in contrast to the solid-stemmed pin keys you saw earlier. The key's thin and complex ward cuts mean that, despite the key likely being quite large and cast from bronze, iron, or steel, it will be prone to failure due to metal fatigue, being dropped, lint caught up in the wards, and imperfections or weaknesses in the casting. Creating a second key, even with access to the first and to the lock, would be a taxing job. Further, because it lacks a second, mirrored flag, this key can work from only one side. However, it contains very little secret information.

Now take a look at the lever lock key in Figure 15-13, which tells us more.

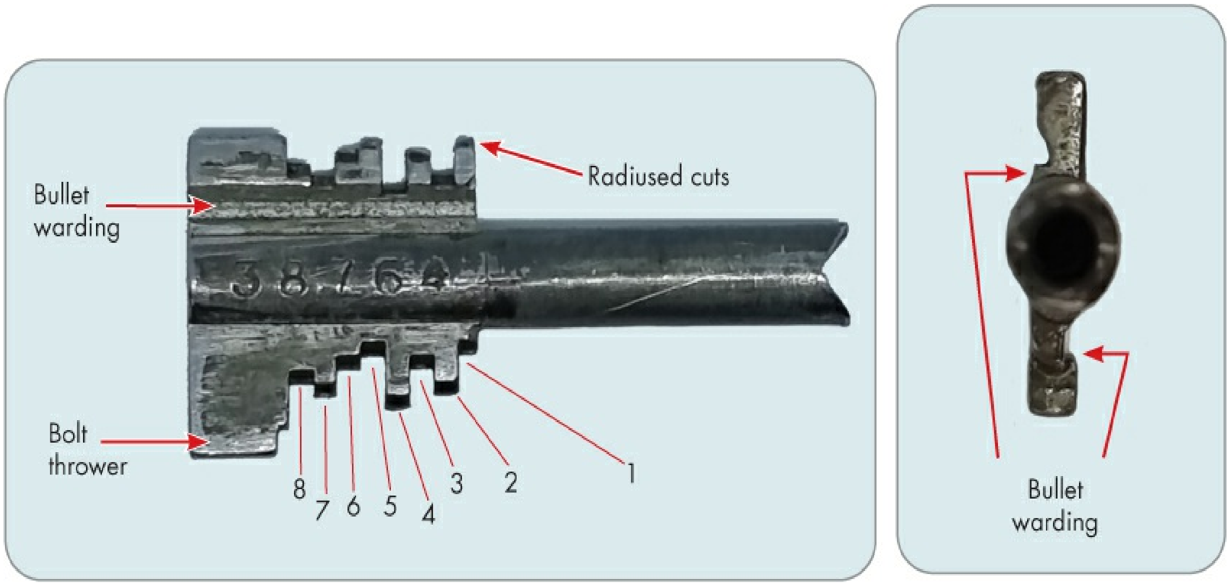


Figure 15-13: A Rosengrens ABN changeable safe-lock key

This is a double-bitted pipe key that drops over a drill pin and can work from only one side of the lock. The key has eight bits and a large bolt thrower at the tip end. The V end interfaces with a long stem to reach through the safe door.

Zooming in on the flag, you can see multiple cuts (in this case, eight) of various heights, much like a cylinder key. However, they're not smoothly linked together, but instead cut as distinct steps with the top surface *radiused*. Because these keys arrive at their test point via rotation, not linearly, there's no MACS as you see in a pin tumbler. The presence of a tallest bit has no effect on the adjacent bit, which could be the same height, the lowest in the sequence, or anything in between. This key contains far more secret information than the warded key, even without the stamped reference number.

NOTE

Lever locks don't really have a MACS in the same way as a cylinder lock. Most lever locks allow a maximum cut next to a minimum cut, because the key rotates into the levers on a well-defined arc, and a large step between them makes the lock harder to open via most "illegal" methods. That said, general guidelines do exist. Most manufacturers allow no more than three levers of the same cut in a five-lever lock, for example. Some locks also have warding that interferes with the cuts available on the key—removing, say, cut depths 6 and 7 from the possibilities—which actually reduces the security of the lock.

What's most important to consider when picking any lock that can be used from both sides is the patterning of the key and the levers. We'll discuss this more shortly, but it suffices to say that if you get the patterning wrong, the key will work from only one side. Another consideration is that on some noncurtained locks, the key requires a bolt thrower of the correct dimensions and location in order to operate the lock, so having all the levers at the correct lifts but with a nonfunctional tensioner that is too long or short means no open.

The double-sidedness of a key affects picking. Consider the bit pattern of the single-bitted key shown in Figure 15-14. Each letter corresponds to a specific cut depth, and the A cut/lever is always closest to the bolt.

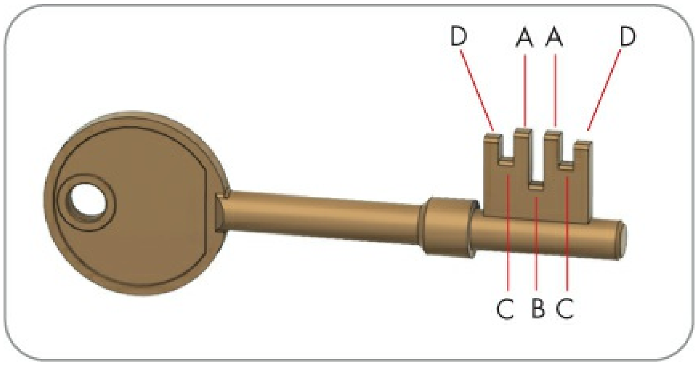


Figure 15-14: A seven-cut key, patterned across the bitting as (DC)ABACD (aka ABA)

In this key, the two A cuts are the same depth and must be lifted to the same height to lift the corresponding levers. From one side of the door, the cuts ABACD will interact with the five levers, and from the other side, DCABA. The other two DC cuts either directly drive the bolt or help drive the curtain. Although it's hard to tell here, note that the top of each cut is rounded slightly to match the arc of the key.

Figure 15-15 shows every legal cut for this key.

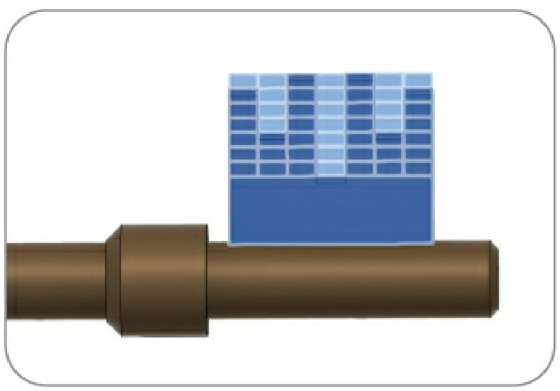


Figure 15-15: Every legal cut on this seven-cut key

As you can see, the ABA symmetry must be maintained for the key to work from both sides of the lock. Figure 15-16 shows another example, this time with a nine-cut key.

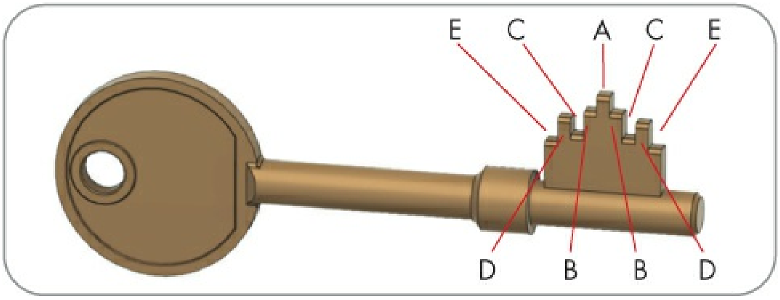


Figure 15-16: A nine-cut key with the (EDCB)ABCDE (aka ABC) pattern

On double-bitted keys, the principle is the same, but the mirror pattern and constant overall bit length means that a low lift becomes a high lift on the second throw, and so on (see Figure 15-17). Further, the sum of each opposite cut-depth pair equals the sum of each other pair, so a 1 opposite a 6 would equal 7, in the same way a 5 opposite a 2 would equal 7.

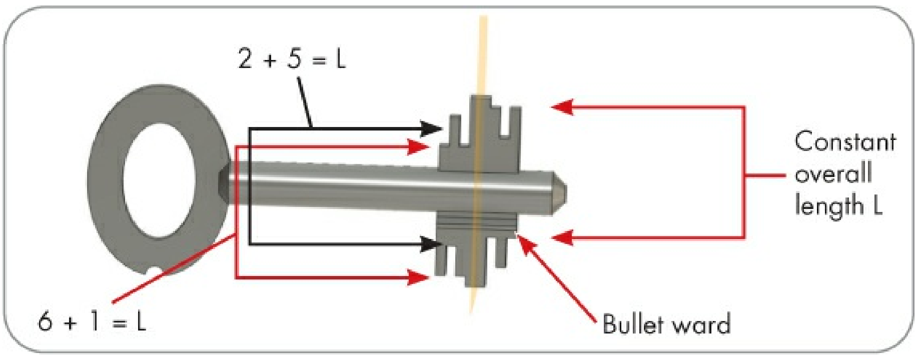


Figure 15-17: This double-bitted key has a symmetrical central plane and can be inserted only one way up because of the bullet ward and corresponding case ward (tactile indication indentation on the bow).

On some double-bitted locks—always the ones with wide flags on the keys—the centrally located bolt has nothing on one side. You'll find no levers there because that side isn't operated at all, as it uses the other cuts on the key from the other side of the lock.

Figure 15-18 compares the bitting on the two flags.

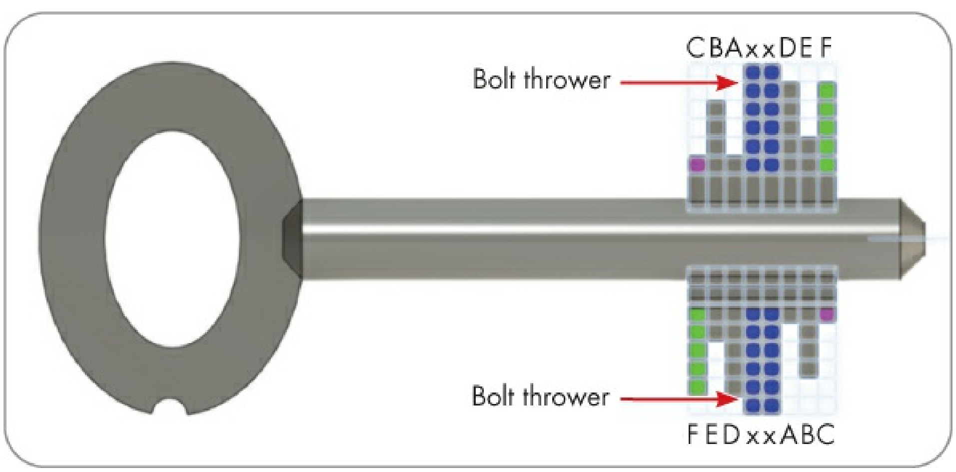


Figure 15-18: The key drives the bolt directly off the two central bits rather than off the opposite side of the key. The "top" bitting pattern is CBAxxDEF, and the "bottom" bitting pattern is the reverse, FEDxxABC.

NOTE

Here, the central two "bits," which are actually the bolt thrower, are shown one cut higher than usual for clarity.

Of course, not all locks have double-bitted keys with a constant length *L* between opposite bits, just as they don't always have the symmetrical bitting that allows them to work from both sides. Plenty of lever locks don't have either of those features. But knowing about them will reduce your workload.

Lever Lock Precision and Tolerances

As with anything physical and mechanical, lever locks have effective limits on precision and tolerances based on mechanical strength and materials science. For example, a lever could have 1,000 possible "true" gate cuts, but because of mechanical limits, that wouldn't add any further security to the lock; a certain portion of them (say, 100) would still align with the true gate under use. Too small a change would allow the wrong key to work, and too large would mean fewer possible keys. In other words, they're not "differs" if a key cut to a higher or lower lift still opens the lock. Also, the levers can't be made any thicker, as generally a lock needs at least five for there to be enough differs for effective key security. Made thinner, they would not have enough strength.

Similarly, requirements exist for the stump. It must be robust and thick enough to withstand efforts to force it into place. Obtaining a British Standard certification has two requirements: that changing any bit on the key by one cut depth stops the lock from working, and that the end of the locking bolt can take a literal ton of force (1,000 kg) *without* stopping the lock from working. Thus, you can see why the stump has to be fairly thick and solid; and, since it commonly rides directly on the levers, they too should be fairly solid in door locks—typically between 1.4 mm and 1.6 mm thick. Picking isn't the most common attack for lever door locks; it's much more likely that someone will use a tool to try forcing the bolt back. Hence, zero-lift levers are rarely seen.

Safe owners, on the other hand, aren't quite so worried about a swift kick or a large screwdriver on the bolt, so safe locks have lower pure-force standards. This is also why many higher-end lever locks (such as the Urban Alps Stealth Key lock) have levers that don't need to be disturbed at all (*zero lift*) for the stump to enter the true gate—something you wouldn't ever see on a standard door lock. Because picking is more of a concern on a safe, levers that result in an immediate, inescapable false set when moved are more useful for safes.

NOTE

With only three cuts, one of which is a zero lift, and 14 levers, the Stealth Key lock has, on average 4 or 5 levers (14 / 3 = ~4.5) that are already at the correct position before picking even commences.

Currently, the number of possible lifts on a lever in a British Standard–certified lever lock ranges from five to nine. The (2004 and later) Securefast has just five, across five levers, on a nine-cut key with bitting in the ABC pattern (EDCB*ABCDE*). This means the cuts for the key follow no discernible pattern; no lever will tell you what another lever might be. At the other end, the Chubb 110 has five detainers with nine possible lifts, again on a nine-cut key. This gives 5^5 possible keys for the Securefast, or 3,125 differs. Even given that it's not permissible to have two adjacent identical lifts or more than three identical lifts across the five levers, this result is still far above the 1,000 differ minimum required by the British Standard. The Chubb 110 has over 59,000 (9^5) differs. As noted previously, the testing rules also ensure that a key that is just one cut higher or lower, on a single bit, can't open the lock.

Now you can see why you don't really want zero-lift levers in a five-lever door lock, especially if it is patterned ABA.

If you're from a computer background, you might be thinking that a key space of just 1,000 is terribly small. Those of you familiar with high-security cylinder locks probably know of manufacturers with claims of billions of keys available. So why can a lever lock with only 1,001 differs be called *high security* or *insurance grade*? The reason is that key space isn't what really matters, but rather, the time to generate and test a key.

A computer attack against a password can perhaps test tens of millions of electronic keys a second, but how fast could you take a mechanical key, insert it, try it, take it out, and repeat? Even with a helper and lots of practice, you couldn't likely get through more than one per second. Assuming you went flat out with everything ready, and that on average you'll find the right key at the halfway point, that's 500 keys. This is almost 10 minutes, which is longer than the time the lock is expected to resist attack. (Where you would generate so many keys at the correct gauge and how you would carry them is another matter altogether.)

Note that smaller lever locks, such as those found on cupboards, may have only a few lifts and one or few levers, often mixed with a ward or drill pin in the middle of the keyway. A few higher-security locks have other wards, but increased key space is usually preferred over the fixed limits of a ward. The drill pin is the notable exception to that rule, as it also prevents a great many other nondestructive entry (NDE) attacks, besides hampering picking.

Hobbs Picks

Alfred C. Hobbs was a prolific lockpicker who became famous in 1851 when he used several tools to open both the Chubb Detector and the Bramah challenge locks. The tools he used are not perfectly known. However, what is known is that he used a 2-in-1 type tool for the Chubb, and a tensioner and separate crochet hook-like pick for the Bramah.

A *2-in-1* is a sort of catchall term for a picking device that has both the picking arm and tensioning arm in one, as seen in Figures 15-19 and 15-20. In the UK, this is the accepted term, while in Europe it is called a *Hobbs hook*. Confusingly, in the UK, a *Hobbs pick* is a 2-in-1 with a tip designed to fit over a drill pin, for a pipe-key lock—that is, it is still a 2-in-1, but to highlight the most vital difference—whether it will even start to fit into the lock or not—we use this slightly different terminology. Even worse, some people refer to any pick for a pipe key lock as a *Hobbs pick*, even if it is a cut-down key and separate picking wire, as per Figure 15-26.

Lever Lockpicks and J Wires

Unlike nearly every other lock type, a hook won't get you far with a lever lock. We've seen almost every type of lock picked with a hook, but never a curtained lever lock. Likewise, even the easiest lever lock can't realistically be opened with a manual pick gun. Instead, we use either wires or manufactured tools such as those shown in Figure 15-19.

Figure 15-19: Seven-gauge 2-in-1 picks used to open non-curtained, pin-type locks with all levers on one side of the bolt

In 2-in-1 picks, the picking arm and tension arms are the same, enabling use from either side of a lock. In a double-bitted lock, you can use one to easily push a lever downward as well as upward (see Figure 15-20).

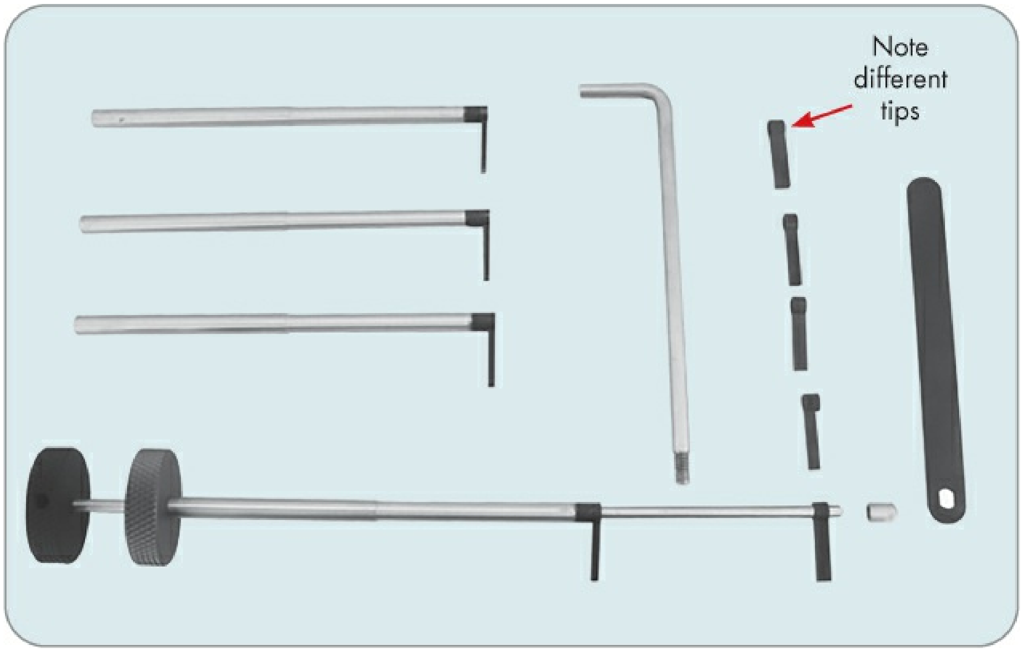


Figure 15-20: Examples of 2-in-1 picks

A 2-in-1 will deal with a lock like the three-lever UNION shown in Figure 15-21 just fine, as it has no curtain.

Figure 15-21: Using a 2-in-1 to pick a three-lever UNION lock

However, these tools require laborious filing to size, and tuning them to fit a specific safe lock with a single lever spring requires even more work. (Note the six slightly different tips in Figure 15-19!) They're also expensive and, without the customizations mentioned, mostly work on only a single model of lock from a single manufacturer. Reasons like these are why you'll almost always be provided with the appropriate tools at lever lockpicking competitions.

For curtained locks, the tools are a little more flexible because the tensioner can often remain the same, so only the wire must be changed. Figure 15-22 shows some example tools from Chris Belcher.

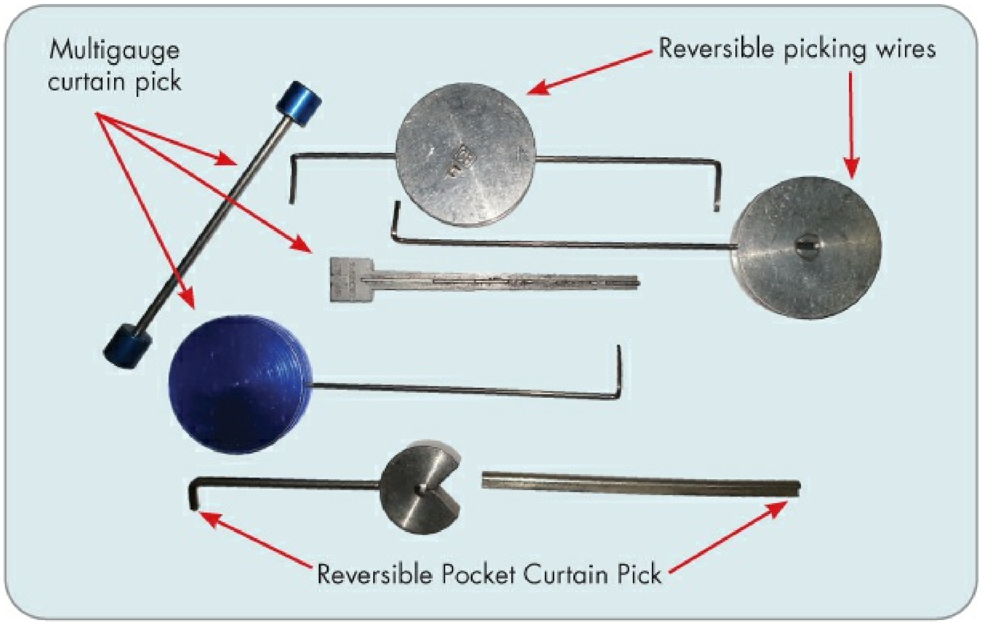


Figure 15-22: Chris Belcher's Reversible Pocket Curtain Pick (RPCP) and Multigauge curtain pick, as well as picking wires basically made of 1.6 mm piano wire

Figure 15-23 shows two other types of picking tools: a sophisticated custom offering and a basic J wire.

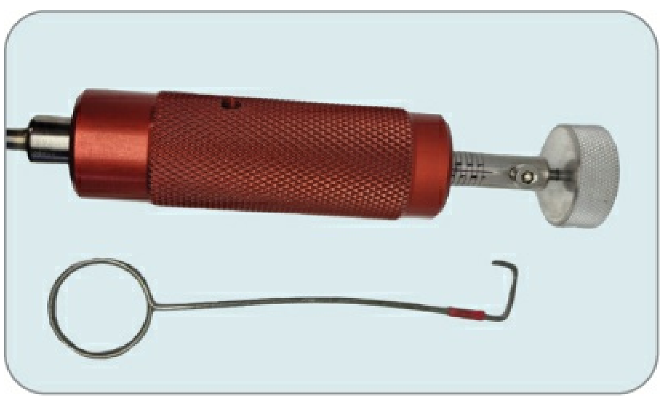


Figure 15-23: Both of these tools started off straight: the handle to a custom-made pick for the Mauer 71111 President lock, complete with engraved spacing markings for each lever, by Jason Jones at https://www.kelocks.co.uk *(top), and a J wire (bottom).*

In operation, the J wire is to a lever lock essentially what the bump key (crossed with a rake) is to a pin tumbler lock. It's simply a shaped bit of wire for hitting the underside (toe, belly, or heel) of all the levers at once, in the hope that the lock has no antipick protections and that the levers will self-set into the gates with enough tension (see Figure 15-24).

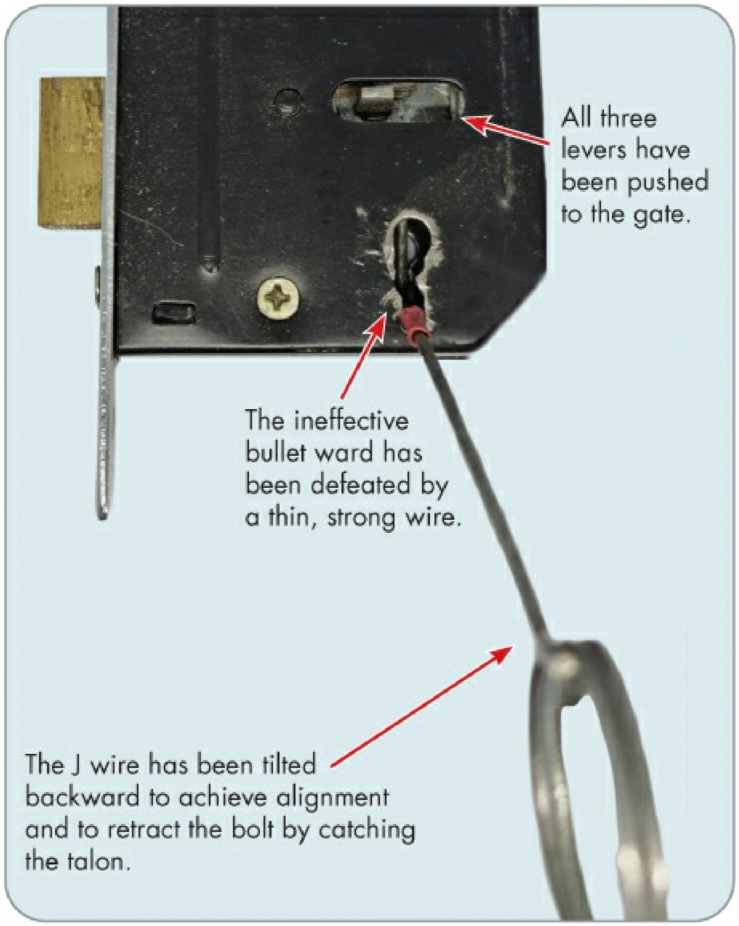


Figure 15-24: The J wire is analogous to the rake and can be used with or without a tensioner.

However, also like a rake or bump key, a J wire teaches you almost nothing about the lock and what's happening inside it—not to mention, nearly every lever lock for centuries now has included antipicks, a drill pin, a curtain, or a combination thereof!

LEVER LOCKPICKING VS. PIN TUMBLER LOCKPICKING

Depending on the exact lock, lever lockpicking tools vary to a far greater degree than those for pin tumbler locks. You'll need to create or adapt a wire for a lever lock far more often than you will with cylinders. As long as you can get your hook through the wards of a keyway, it will open the pin tumbler lock (though you might occasionally need a slightly deeper hook for trickier bittings). However, with a lever lock, if the tensioner is too short, you'll be able to pick the lock but not open it fully. If the tensioner is too long, you won't be able to open the lock at all, because it will jam the bolt. Likewise, if the picking wire is too long, it might not fit in the keyway, and if it's too short or the wrong shape, you may not be able to lift the levers high enough—which also means you won't get the lock open. The good news is that once you've tuned your wires for size, they'll open every bitting of that lock.

Lever lockpicking is similar to pin tumbler lockpicking in that it still follows the binding element order principle: we move only the binding tumbler, unless we have prior knowledge (*tumbler* refers to any pin stack, lever, detainer, disc, wafer, or other locking element).

You'll be using a tensioner and a pick, just as with pin tumbler locks. Sometimes they're combined into one tool, or for some lower-security locks, you might use a key analog known as a *jiggler*. Jigglers aren't really suitable for competitions, though, and the locks are a bit too easy if the entire room knows that "key 14 on the ring" is the one that works!

Practice Locks

Some lever locks have multiple lever packs, and others are master keyed. Over the years, dozens of variations have arisen in keyway size, drill pins, warding, and more, adding up to thousands of possibilities. So, our tool buying advice? Don't, unless you really want to. And even then, make sure you have both the exact lock and picking tool for any competition you want to enter.

Don't just start buying super-expensive tools for lever locks! They mostly work only on a single model of lock from a single manufacturer (for example, the Mauer pick in Figure 15-23 costs hundreds of dollars and will work only on the Mauer 7111*x*). You could make your own if you're handy, but you'll rarely get to use your own tools in a lever lockpicking competition, even if you could ensure that you have the correct one.

> I know of only one lever lock competition where the locks and tools aren't supplied: the Master Locksmiths Association (MLA) Western Region contest. Since that competition includes random locks of all types and qualities, you'd be foolish to attack the Chubb 110 five-detainer lock when you could rake open a Euro profile cylinder or shim a padlock instead for the same number of points. And while to open the Chubb in three minutes would be a notable feat, it wouldn't win you the contest. Lever locks generally can't be opened at speed; you can rake open a cheap cylinder far faster than you could even get a curtain pick into a lock.
>
> By the way, my top score in that contest was 17 points, at that time a clear lead, but it was beaten the next day by the winner, Mete Hilmi, a talented locksmith from Cardiff, Wales, with 18 points. Yes, that's 18 random locks opened in 3 minutes.
>
> —NIGEL

That said, you can pick up a couple of pieces of random equipment in order to practice. First, you need to source a double-bitted lock. The locks used for the LockCon competitions have so far always been double-bitted locks with a single mainspring. Safe deposit and door locks have been used, though the exact models are kept secret to prevent people from buying them and learning how to best beat them.

Annoyingly, these locks tend to be quite expensive, rare, or very hard to pick—and sometimes all three. The best practice lock for the average person is the one shown in Figure 15-25, which is cheap and from China.

Figure 15-25: A cheap, double-bitted safe lock from China. Note the drill pin in the center of the keyway.

This lock cost less than $15 (£10) and is of low quality. One of the two keys wouldn't actually *chamber* (fit fully) onto the drill pin. However, the other one did work, and they looked about the same. The bad key was fashioned into the homemade Hobbs pick shown in Figure 15-26.

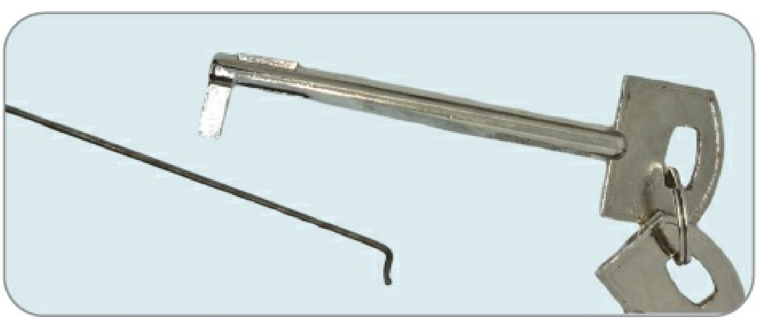


Figure 15-26: A homemade Hobbs pick (cut-down key and wire) for the Chinese safe lock shown in Figure 15-25

If you can find and afford them, we strongly recommend you order at least *two* of whatever lock you choose (noted lockpicker Deviant Ollam suggests four), but you'll still be able to practice if you have only one. The key bitting for the two can be different; the more variety, the better. Go for a five-lever or higher, nonsafe (as in *not for a safe*, not *dangerous*!) lock of the style used in the competition you want to enter. When you buy or make a tool, it will fit both locks, and you can practice on either. One great thing about lever locks is that you can't "brick" (render unusable and unfixable) them when they're not installed in a door, since you can almost always remove the cap without the key (or even with the key stuck in it), so you always have an escape route.

To make your lock easier to pick, you can swap the levers around or replace them with a few washers to keep the levers aligned. Better still, you can sacrifice a few levers (hence buying multiple identical locks) and file away a few of the false gates, file back the bar or fence to affect the binding order, or make the true gate larger. To make it harder to pick, you can file serrations, notches, or square gates in the appropriate locations on your levers. You could also convert one lock into a cutaway so that you can see the stump and the levers, or remove the cap and replace it with clear Plexiglas. Keep in mind that many of these modifications are irreversible, which is part of the reason you want at least two locks of the same make, model, and age.

Lever Lock Disassembly and Reassembly

If you want to look inside your lock, you're in luck—almost all lever locks are easy to disassemble. Usually, one to six screws hold the cap onto the lock. Some locks are a clamshell design, but most have a simpler flat plate. Just undo the screws and lift off the cap, and the innards are revealed. Simple!

One notable exception is the Mauer 7111*x* series, which has a sliding metal cap secured by a little twisted tab (Figure 15-27). You'll need to carefully pry that tab up to then slide the cap backward, and then lift it off. (The odds are high you'll run into one of these locks, as it's currently the most common lever safe lock in the world.)

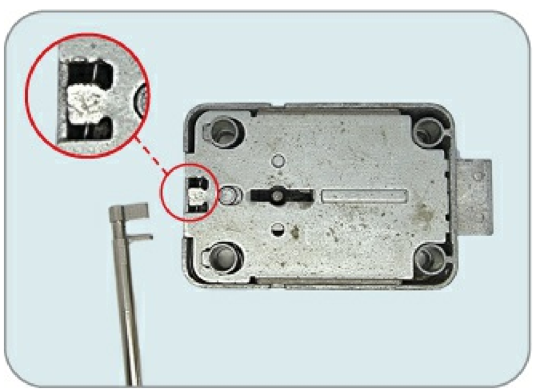


Figure: 15-27: The Mauer President 71111 features the highlighted tab. Also shown is the tip of the custom picking tool for this lock, as shown earlier in Figure 15-23.

One word of caution: on sash locks (recall these are locks with a built-in latch mechanism), the powerful handle-return springs can sometimes jump out of alignment. This isn't a problem for picking, since it doesn't affect the actual locking part(s), but it can be annoying when you want to put the lock back together again. During reassembly, you can use a spindle to align and hold parts in place as you replace the cap.

Reassembly is generally easy. Just ensure that the lever springs are all in the right place and the curtain is aligned to let you put in the key (you may find putting the key in from the back of the lock helps); then slide the cap back on. If the cap doesn't sit flush, don't simply tighten the screws—figure out what's blocking it.

A subtle failure on some curtained locks is that you must push the curtain alignment spring into place, with the cap loosely on, via the hole in the face of the case below the bolt. You'll need a long, thin wire to do this. Another potentially frustrating issue is that the lever spring on the top lever won't stay neatly in place; try using a bit of thin plastic, a shim, or a pin tumbler pick to hold it in place; then align the cap, carefully slide the tool out of the way until the cap clicks into place, and then replace the screws.

Summary

In this chapter, you've taken a tour of warded and lever locks, including various kinds of wards, keys, and antipick mechanisms, and learned about the tools you'll be using in practice and competition settings to open them. In the next chapter, you'll start putting this new knowledge to use as you learn the step-by-step process of lever lockpicking.

16
LEVER LOCKPICKING STEP-BY-STEP

In this chapter, we'll walk you through picking a double-acting lever lock. We'll cover tensioning and picking, troubleshooting, and the various locks you might encounter in competitions. You'll also learn some tips on how best to practice so that you're competition ready.

Lever Lockpicking Overview

Picking lever locks, which works similarly to picking the other lock types you've explored, is possible for the same reason: manufacturing tolerances. When the lock is made, the levers are stamped out from multiple tools to give the variations of lift, so the levers aren't *exactly* the same size, and the stump can't be perfectly aligned. When you tension the lock, the longest lever will be caught by the stump first. This will keep the bolt from traveling farther back and hold the lever in place. When you move that one binding lever, the next binds up, and so on, until, with any luck, the lock opens.

Currently, only LockCon has an annual lever lock championship, so we'll be examining the technique for picking the locks used there: noncurtained and with a single mainspring controlling the levers. However, the process is mostly the same for curtained and individually sprung locks. The general steps for using a 2-in-1 or Hobbs pick are as follows:

1. Tension the lock bolt by turning the rear handle of your tensioner to the open direction, which is usually clockwise.
2. Release the tension but hold the pick in position, and use the picking arm to locate the lever pack. You'll usually know the number of levers in the lock before you start, but make sure you can find each. They're movable and typically found in either rotational direction.
3. Apply the tension again, and tentatively probe each lever to determine its state and locate the binding one.
4. Move the binding lever until it no longer binds. Generally, you'll nudge it upward only

a millimeter or so—a tiny movement.

5. Repeat this process until the lock opens.

This process should sound familiar by now. Let's look at each step in more detail.

Tension the Lock Bolt

Tension is the metaphorical key to opening any lock by picking; specifically, it is the balance of tensioner rotational force to drive the bolt back and the resulting holding force applied to the levers. The concept is similar to pin tumbler lockpicking: if you don't apply enough tension, nothing will bind, the lock will keep resetting, and you'll never open it. If you apply too much tension, everything will jam up so that you won't be able to manipulate the working parts. With the right amount of tension, however, one lever should bind up enough that you notice it and can hold it in place while moving the picking tool to another location.

To summarize, you're aiming for the balance that allows you to both nudge the levers into position and probe them to get feedback. Nudge, don't fire, the levers—if they bind too hard, you'll lose control over them.

When using a 2-in-1, always keep it perpendicular to the lock case. If you don't, at a minimum you'll get false readings from the lock case, and the picking tip will hit multiple levers—and at the extreme, you'll bend or break the tool.

Locate the Lever Pack

Competition locks, so far, have always had only one lever pack, and figuring out its location comes with experience. The lever pack can be anywhere, but generally it's next to the bolt, inside the keyway. What you're feeling for is the solid contact of the bolt and the springy or "clattering" movement of the levers.

If you hear *lock facing to the left* or just *left facing*, it means the bolt is facing to the left, with the levers above the keyway and in front of the bolt, as shown in the photos throughout this section. Keep in mind that if the bolt is *right facing*, the levers are now behind the bolt. In that case, you'd reverse your tools: using the picking tool to tension in the opposite rotation, and using the tensioner to pick.

> Usually, the side with the bolt facing left is easier. I'm not entirely sure why; the bolt lath making the levers a few millimeters farther away surely has a negligible effect. Possibly it's because most people practice that more frequently. On all lever padlocks I know of, you also pick as if the bolt were facing left, because internally it is. Likewise on 95 percent of safe locks, although they can be mounted such that the bolt points vertically as well (a few old ones out there, I suspect, are also right facing). You can reverse any double-sided lock for the challenge of picking "right facing" if you wish.
>
> Just yesterday, I faced a five-lever lock I identified as a Henderson. I don't recall ever seeing one outside the books before. Though fairly responsive, the

lock would go only so far from the "outside"—that is, with the bolt facing to the right. Yes, it was a little worn, but it was also very "gritty" and very hard to turn back the curtain to reset the lock. After almost an hour, I gave up and walked to the other side of the door to try it "left facing." Just a couple of minutes later, it gave up the fight.

—NIGEL

Probe the Levers to Determine Their State

Even if you already know the number of levers in your lock, counting them is good practice. Nearly all British Standard curtained lever locks have five levers. Make sure you have free and full movement under the lever pack; that is, ensure you can get from the front of the lock case to the back, reaching every lever, as some locks deliberately have very low levers to hinder you.

If you can't, then either something is wrong or you need to lift each lever a little to get clearance for the picking tool. You won't need to do this with the 2-in-1/Hobbs-type picks, as they rotate like a key. As long as you rotate these picks back far enough toward the keyhole, you'll clear the lever pack and/or bolt and can move freely back up under the lever of your choice.

With the picking tip, check whether the lever bellies (their curved bottom edges) are all the same. If not, odds are high that a lever with a longer belly requires a higher lift, and one with a shorter belly requires a lower lift, or vice versa—there's information there, and you just have to determine which way around it is! (In many high-security-rated locks, all the bellies are identical to prevent you from using this trick. Indeed, some standards insist on it.)

Levers have four possible states:

Unbound The lever moves freely, under gravity or spring pressure.

Binding The lever binds against the stump.

Gated (aka *true gated*) The lever is located in a true gate; that is, it's positioned such that the stump can clear its gate (see Figure 16-1).

False gated The lever is located in a false gate; that is, it's positioned such that the stump is caught in a false gate, and the lever can no longer move freely.

The false gated state is a subset of the gated state. Likewise, binding has varying degrees. The more heavily bound a lever is, the harder it is to move with your picking tool, but it's also less likely to be disturbed by other levers, gravity, or springs.

Figure 16-1: The topmost lever in this UNION StrongBOLT is in the true gate, while the levers behind are as yet undisturbed.

To determine the state of a lever, you probe it with a wire or other picking tool. Nudge the lever to see whether it moves freely and returns under spring pressure (where applicable —if the tool you're using takes off the spring pressure, this won't apply until you reset the lock). Also check whether the lever returns loosely under gravity or returns when driven in the opposite direction. A bound lever, like a bound pin, won't move freely.

If the lever is tightly bound, excessive pressure from the stump means you won't be able to move it easily either. When you apply sufficient picking force to overcome the binding force, the energy stored in the natural spring of the picking tool will "fire" the lever upward, like a rubber band flicked across the room. This often pushes the lever past the gate to its maximum height, but there's no way to know whether you have then *overlifted* it (gone too far and blocked the stump). If you have, it's game over; you can never deliberately reset a chosen lever on a single-bitted key lock.

NOTE

Double-bitted locks are somewhat easier to pick because you can reverse the picking tool direction on most of them to drive the lever back downward if it's too high. However, this will probably move other levers too, as the only thing keeping them in position, if they're unbound, is friction with the adjacent lever(s).

Move the Binding Lever

As always, remember the element binding order principle: move only the binding lever. Nudge it upward until it stops binding and "jiggles" or "slaps" against the stump. When you tap the lever, it should move freely a small distance, just between the top and bottom of the gate, trapped by the stump.

At this point, you might be in a true gate or a false gate, or the angle of the lever might be such that it simply stopped binding. (Some locks, such as the UNION ones with reversed levers—the pivot point is on the bolt side—require tiny, repeated lifts, as they bind, then stop binding when lifted slightly. See Figure 15-21.) When released, the lever drops back to almost exactly where it started, and the bolt moves imperceptibly. Lift the next binding lever, and the bolt moves imperceptibly again, and that lever also returns almost to its original position.

Repeat the Process to Open the Lock

You repeat the preceding step until one of the levers gates and you get a little bolt movement. Keep at the other levers, and in short order, another one will end up in a gate. Eventually, your final lever will bind heavily because of the massive tension you've been using to get even a slight movement, and you'll fire that lever straight past the gate—now you've been warned!—and fail to open the lock.

Keep in mind that as you progress through the levers, the pressure binding each unset lever increases (the pressure that before was spread across, say, four levers, is now all on a single lever). Therefore, you'll have, for example, a fivefold increase on a good five-lever lock in which all the levers bind at around the same time. The moral of the story: keep it light when you can. Nudge the final lever into position gently!

Congratulations—you've opened a lever lock! In a competition setting, you now call out "Open!" and beam with pride as your time is read out and recorded for posterity. Of course, if it's a multithrow lock, you have perhaps three more throws before you're truly finished with the round, but don't let that detract from the satisfaction of having opened the first one!

Troubleshooting

Sometimes a lever is just not binding. You can increase the tension, but only within limits, because breaking the tool is a really bad idea—not only will it be expensive to replace, but in a competition it will get you disqualified. In this section, we'll look at better techniques and work-arounds for when you get stuck.

Pack Compression

If you can't get any of the levers to stay where you want them, you can "cheat" on some locks by *compressing the pack*: pulling the entire pack of levers together, pinching them with the tensioner, and effectively jamming them against the lock case and their neighboring levers. If you compress them too hard, the entire pack could move as one, or just the target lever and the adjacent one(s). If you pull too gently, the entire pack, or individual levers, could drop and reset when you reduce the tension.

As with the more usual tensioning method, this technique requires a proper balance. Not only that, but it doesn't work the same on all locks. In some locks with stamped steel levers and no spacers, like the StrongBOLT shown in Figure 16-1, compressing the pack can cause the levers to move into the empty spaces between them or to bind into the space where two stamped bumps meet, locking the levers together. Compressing the pack for center bolt locks with levers on either side produces different results as well.

A true gate is generally larger than a false gate. Therefore, when compressing the pack, you might be able to feel out the locations of the false and true gates, based on the feedback such as a lever slapping or a lack of resistance from a lever rubbing on the stump, even if you can't get the levers to stay quite where you want just yet. Mentally note these gate locations for later in the picking process.

On single-spring locks with double-bitted keys, there's simply no way to move just a single lever reliably, even without pack compression. These levers are very light and free to pivot, so they'll shift whenever a neighbor is disturbed. Fortunately, you can always push the lever up or down in a double-bitted lock, so record or remember your positions, and then dial them back to where they should be, and you'll be one step closer to your open.

Finally, note that tilting your tensioner will have much the same effect as compressing the pack. This is fine if you're doing it intentionally, but if you aren't, then you'll be making the task more difficult for yourself, as the feedback you get will be altered. Remember to keep your picking tools in the correct place—perpendicular to the lock.

Antipicks

So far, we've just assumed that the lever has only a true gate, but that's generally not the case with higher-security lever or detainer locks. Broadly speaking, antipicks have two categories: ones that you can escape from, and ones that you can't. V notches and similar machined indents are examples of the former, and square false gates are examples of the latter.

V Notches and Machined Indents

A *V notch* is a shallow *V* cut into the front edge of a lever. When the lever is in a false gated state, the stump will hit the lever's front edge and then move back slightly into the V, and the lever will stop binding. As you find other binding levers and set them, this one will start binding again as the stump moves farther into the V, slowing you down. When you lift this early binding lever higher, the V notch will force the stump, bolt, and tensioner backward, probably releasing some unknown other levers at the same time. Annoying! This is, of course, the role of an antipick: to frustrate the lockpicker and slow them down.

The good news is that, just as with a spool pin, you can drop the tension a little, increase the lifting force, and pop the lever past the V notch, often without dropping too much. As you push on the falsely set lever, it will push back against your tension, indicating in the same way as a pin tumbler spool.

Figure 16-2 shows a detainer with two V notches. It takes great skill to balance the tension and the picking forces, and not fire the detainer past the true gate, to where it may well drop into the higher false gate.

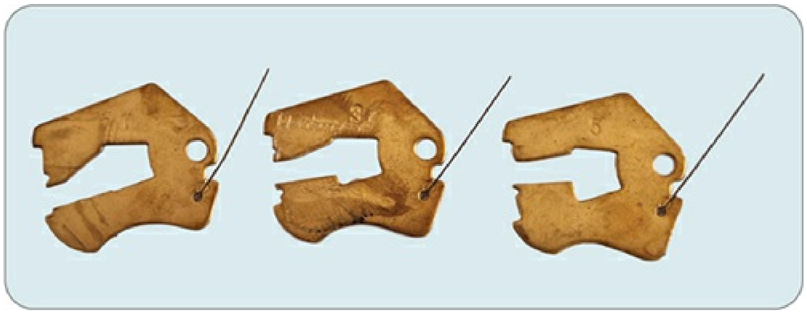


Figure 16-2: A UAP Tradelocks MAX6MUM six-lever British Standard lock detainer with V notches

As always, you can tell whether a gate is a true gate only after you're in it. As the stump moves back, the movement of the levers in false gates will become more limited or bind solidly, while the behavior of true gated levers won't change. For better locks, you'll need to develop a mental picture of the interior to determine which levers need to be lifted higher or lower to be correctly set.

Square False Gates

The *square gate* antipick is often extremely obvious. You'll slam into it as you nudge a lever that's binding well, the tensioner will turn, and for a brief moment you might even be celebrating. But no—you're in a squared-off trap. No amount of pressure on the picking wire, nor reduced tension on the tensioner, will cause any counter-rotation.

Once you're fully into a square false gate, you can't skip past it, and you'll have to remember where you were in the lock while you reset it and try again. The next time you lift that lever, you'll have to lift it higher than you lifted it before to go right past the false gate and reach the true gate, or at least bind somewhere above it.

Quite often, you'll find that the picking order is the same, and you're back at the point of tripping into the square false gate. At this point, you need to drop off as much tension as you can, and try to rapidly skip that lever up to the true gate. It may help to try to compress the lever pack (by pulling the tensioner back toward you) as you do this, to slow or stall the other levers dropping back to rest. Just don't throw it too high, or you might well be stuck again.

Review the photos of the various levers throughout this section, including the detainers in Figure 16-3, and contrast the antipicks.

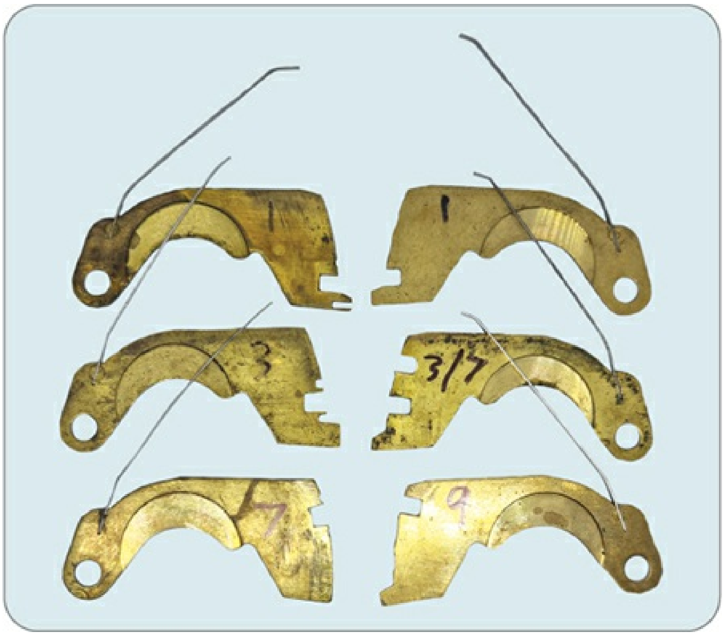


Figure 16-3: Chubb 110 detainers, clockwise from bottom left: 1960s number 7 lift with no extra toe added to prevent overlifting attacks; number 3 lift from the '80s with deeper false gates; number 1 lift from the '70s; new number 1 lift with lightly scalloped front edge; a mastered detainer with gates at the 3 and 7 lifts and scalloped front edge; new number 9 lift with scalloped front edge.

Note in Figure 16-3 that all the older detainers in the left column have distinct antipick notches above and below; you can spot the predictable pattern of the antipick notches always exactly one lift away, a fact that was often exploited when NDE opening was required. The newer style (righthand column) removed this weakness: note that the toe, bellies, and even the pivot points are all identical, defeating all simple decoding attacks.

CHUBB DETAINER LOCKS

Not all locks are created equal. Some have far higher tolerances than others (they're manufactured to a higher standard and generally have fewer vulnerabilities for lockpickers to exploit); Chubb (now UNION C-series) locks are generally at the higher end. Additionally, Chubb engineers were experts in the game of lock manipulation and added a few features to hinder lockpicking efforts.

They created the detainer lock: instead of the gate being an H-shaped pocket in the lever, it's a notch cut into the front of the lever that the stump slides into. This provided more key space, as a tiny difference in key lift could turn into a very large travel distance due to the amplification of the movement. The change also put the useful drill point well away from the keyhole, behind the edge of the door frame. Anyone simply using a drill through the keyhole of a lever lock was already going to be disappointed, but now anyone doing the same with a hole saw would be too! An additional advantage of the detainer is that it allows master keying; note the lever in Figure 16-3 marked 3/7, featuring two true gates. The disadvantages include the higher precision required for the key, and the additional complexity of the checking mechanism.

The genuine Detainer pack is actually made after the key, with the gates milled to match the precut keys at the factory.

The Chubb 110 is considered generally too hard to straight pick, so the extra defense of the square gates shown in Figure 16-3 wasn't really required. However, the fact that they were easy to decode using a more advanced tool made them suboptimal, so the more complex, "scalloped" front-edge pattern was introduced. The frustration of having to do a full reset when you encountered one of the square gates was replaced by the uncertainties the scalloped edges introduced.

Decoding the Lock

As with picking any other lock, opening a lever lock relies on getting feedback from the locking elements—the levers—to determine their state. Going through all the possible lifts for five levers can be time-consuming. Knowing the tricks that manufacturers use to resist attacks can help you *decode*, or learn the configuration of, the lock.

The turn of a key, as well as each bit on the key, traces a circle (see Figure 16-4). The belly of a pivoted lever forms a semicircle. At the point the key is tested, the curved paths (or *arcs*) of the bit and its corresponding lever must overlap in the correct place to maintain a true gate throughout the travel of the bolt and key. Otherwise, the bolt stump jams into the levers, causing wear, or, if the paths diverge and force the lever upward into the stump, the lock jams solid, partway open, until the key is turned back.

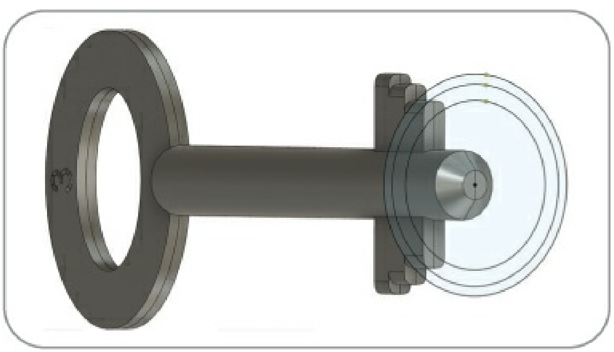


Figure 16-4: Each bit of a different height draws a different-size circle. The arc of a lever must match this arc; otherwise, the lever will ride up and down and jam itself against the stump.

The longer the throw of the bolt, the harder it is to maintain a true gate. In other words, the farther the stump has to travel into or through the lever, the longer those arcs have to stay overlapped.

Lower-security locks avoid this difficulty in a couple of ways. They either change the curve of the belly to match the curve of the key so that they overlap within the lock's tolerance long enough for the stump to travel through the gate, or they simply make the gates wider. (Remember that the stump has to be thick enough to stop force attacks and strong enough to avoid bending under load should someone press on the end of the bolt or try forcing a wrong key, so the gates are generally already quite large to match.)

A better solution, as noted earlier, is to make all the bellies identical. This leaves a lockpicker with no way to see or probe for the bellies to decode the key. However, this is technically really hard (see Figure 16-5); of the curtained locks, only some safe locks and the previously mentioned Chubb 110 series detainer door locks have identical bellies, toe, and heel.

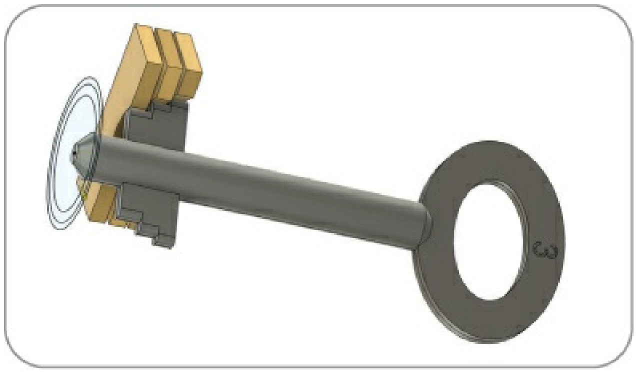


Figure 16-5: This lock couldn't have near-identical bellies unless the gates were curved, but regardless, simply lifting the toe or heel of all the levers together, perhaps with a J wire, would open it!

The third belly-modifying option is a combination of the first two: grouping the lever bellies. That is, 1 and 2 (Group X) will have the same bellies, as will 3, 4, and 5 (Group Y) and 6, 7, and 8 (Group Z). This still allows decoding, but it isn't perfect information anymore; done correctly, there are still lots of keys to try.

A picker, of course, can easily use this information to their benefit by decoding with the wire and then lifting straight to the area of interest. In the case of an ABACD lock, you'd go, perhaps, high, medium, high, medium, low with your lifts, rather than picking purely with feedback, which could help you avoid antipicks and mapping out the lock by feel.

In Figure 16-6, notice the bellies and toes of the levers with antipicks above the true gate, and compare them to those with antipicks below the true gate. A grouping emerges, with those stamped 1 through 4 in one group, and 5 through 8 in the other (not all are pictured).

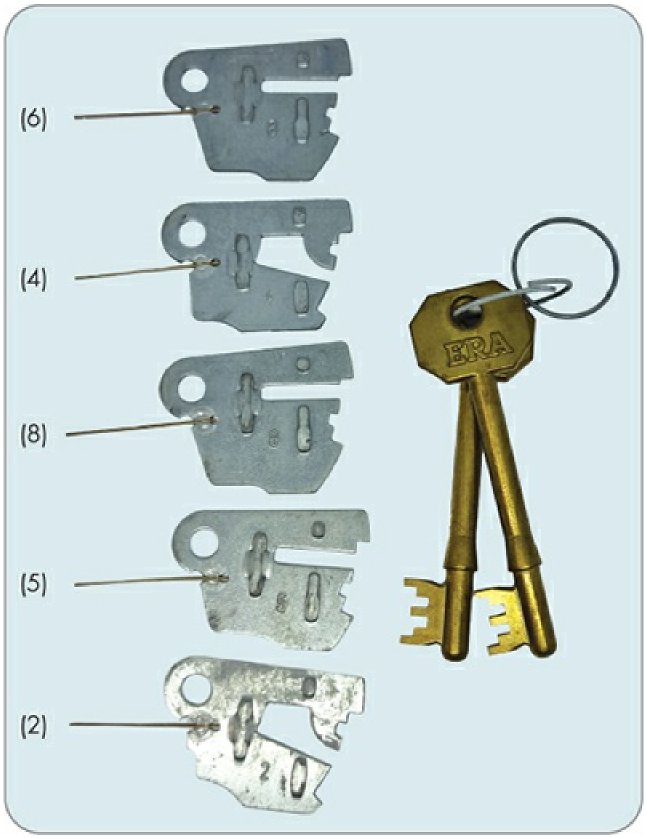


Figure 16-6: The ERA Invincible, now a few decades out of production

Now consider the Ratner Safes lock shown in Figure 16-7. You can see how the lever bellies betray the lift; the low lift has a smaller radius than the high. To increase the picking difficulty and available key differs, the front edge of the lever gate is narrow, while the back is widened to prevent jamming.


Figure 16-7: This Ratner Safes lock is the very model of simplicity; shown here are the two halves of the case, the bolt, five levers, and four screws to hold it together. Image courtesy of autom8on (@a8n_pub), © 2021 by Stephen Wilson.

Manufacturers also use other tricks. They can cut away the fronts and backs of the levers to defeat this simple way of decoding, making it harder to find out. See the Asec/Legge with vertically sliding levers, shown in Figure 16-8; and the Mauer 76000 series and the S&G FAS 69x0 series are other examples. Manufacturers might also restrict the rotation of the curtain to prevent easy access to the levers, leaving the fronts of the levers all the same, with the only variation being at a steep angle through the curtain (examples include the UNION StrongBOLT and ERA Fortress). In that case, the lock's levers can sometimes then be decoded from the heel.

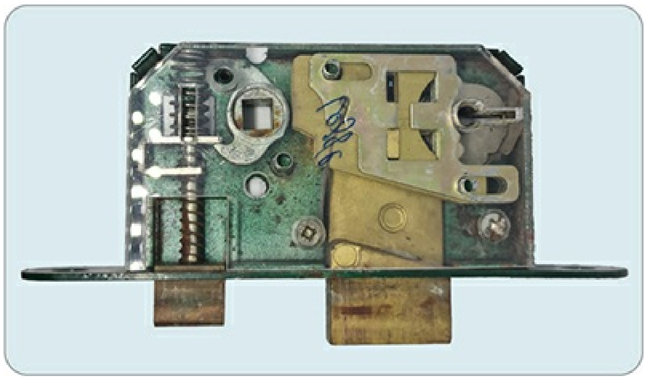


Figure 16-8: A Legge sash lock with vertically sliding levers

Looking closely at this Legge lock in Figure 16-9, you can see the reduced contact lever bellies that slide vertically. A wire picking tool of a standard length will miss the details required to decode, making the task harder. Early models had full-width bellies and were easily read with a wire.

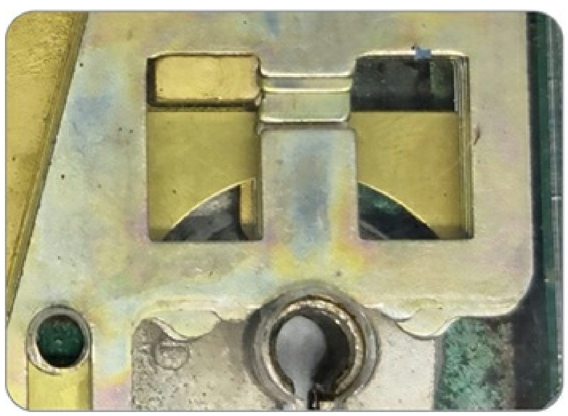


Figure 16-9: Detail of the levers, with the spacers removed and arranged to show the various belly radii as well as possible

Also notice the subtle antipicks. The main issue with picking these locks is the tendency of the wire to get trapped by the front edge of the cutaway lever toe as it rotates.

OTHER TYPES OF DECODING

Other decoding methods, including *optical* (use of a camera, endoscope, or tiny mirror on a stick), *wire* (poking one or more wires in and gauging rotations), or alternate impressioning techniques (using plasticine or putty to impression the key) may or may not be allowed in competition settings. You'll have to ask and should expect a no. You can often decode the toe or heel of the levers by using the same double-bend picking wire or 2-in-1 tool you use for the actual picking. You'll need to practice this on a few target locks beforehand if you want exact results.

However, simply knowing that the first lever is a high lift because the pick rotates much farther before it hits the lever—as compared to the second lever you test, which has barely any rotation—gives you a big clue before you even start picking. You'll need to know your lock in advance, though; as explained earlier, some are the reverse orientation, and others have identical bellies throughout.

For something more like the Master Locksmiths Association (MLA) exam or an "open" contest, decoding kits and endoscopes are likely fine, as they are equipment the locksmith owns already, and the goal is to open the lock neatly, not to get the best time. Many other decoding techniques can be used, but we've already strayed far enough from the subject of this chapter!

Summary

In this chapter, you've learned about the hands-on lever lockpicking process. Hopefully, you've seen that once you have some experience under your belt, the process isn't as daunting as it might have seemed initially. Getting ahold of the locks and hardware will likely be your biggest challenge (your first ports of call should be friendly locksmiths or thrift and antique stores for locks, and hobby shops for piano wire).

Just reading up on lever lock theory has already put you ahead of most of the competition. Speaking of which, in the next chapter, we'll show you ways to prepare for lever lock events and what you can expect in a competition setting.

17
LEVER LOCKPICKING COMPETITIONS

In this chapter, we'll cover the general setup of a lever lockpicking competition, tools and locks you can expect to see there, and advice for preparing to win. We'll give you tips for both running and competing in a lever lock competition, as well as some helpful dos and don'ts.

The Competition Setup

Because of the cost of the tools and availability of the locks, competitions rarely have enough for everyone who wants to take part. The only fair way around this is a qualifier round using, for example, a single, easy lever lock with a short time limit. The fastest openings get through to the next rounds, which are head-to-head in the usual way. Generally, a certain number of preliminary rounds occur with four competitors each, and then a larger final round.

The time limit, explained beforehand, is between five and nine minutes per lock. At the end of each time period, the locks are reset, and the entire field moves round-robin-style until all the contestants have picked all the locks. More contestants usually means less time per round.

The lock will already be mounted in a vise. Usually, the tools will also already be in place, and you won't be able to see the operating parts of the lock. You likely won't be allowed to touch the tools until the time starts, so always check beforehand to see whether a qualifier round or test period is scheduled.

You'll probably be standing, with the pick at waist level. It is both easier and faster to simply walk from lock to lock, leaving the setup in place. The pace can be quite fast; in 2019, the LockCon lever picking contest was a mere five minutes a round, on locks with four throws. Granted, you're not running the 100-meter sprint in under 10 seconds, but not partying all night before the competition might help you maintain your stamina.

You'll be told how many times you must pick the lock; the most is four, and the least is one. Sometimes the lock will move a full rotation with each pick, and sometimes a half rotation. It can take as many as five half rotations, or as few as one, to complete the open.

Scoring is based on the number of openings, with the most openings winning the round. If a tie occurs for the highest number of openings, the fastest time wins.

As noted previously, lever lock competitions are fairly rare, with LockCon in the Netherlands (where Walter is competing in Figure 17-1) being the main one. For information about other contests, consult the groups listed in Chapter 1.

Figure 17-1: Walter competing at LockCon 2014

Competition Tools

As we've noted in previous chapters, the competition's organizers almost always provide the locks and the picking tools. (Make sure you ask, though!) The noncurtain lock pick will be a 2-in-1, and the curtain pick will be a wire picking arm and a separate tensioner of some form. A mounting block and vise will also be provided.

NOTE

You can pick a small lever lock in-hand with a wire pick and a tensioner by holding the tensioner in position in the lock, but that approach is far harder than with the lock mounted, and it can't be done in competition or if the lock bolt faces the other way. Doing so with a 2-in-1 is impossible, unless you have three hands—hence, the necessity of a vise and block.

If you want pen and paper, or a personal timing device, however, you'll need to bring those yourself.

Competition Locks

As you no doubt know by now, practice is the most important part of competition prep. However, specific practice on the specific lock isn't possible unless you know which lock type, brand, and model will be used, which is unlikely. Location will help give you a clue, so in this section we'll review some locks you'll encounter in European and UK competitions.

First, however, let's briefly talk about locks you *won't* find there. Some lever locks are unsuitable for competition. The Chubb 114, for instance, would be a terrible choice (see the 3G114 in Figure 17-2).

When the Chubb 114 is new (unpicked), it's extremely easy to pick. However, its knife-edged brass stump wears easily, and its levers rapidly take up the small amount of play from the manufacturing imperfections. Therefore, it quickly becomes much harder to pick, especially if it's been subjected to lots of tension. Once "bedded in" with this wear, this lock can be nearly impossible to pick. This would obviously favor the first competitors, even if the same lock were used in each round (as is typically the case).

Figure 17-2: A Chubb 3G114 with an antipick notch on the rear of the stump

Figure 17-3 shows levers for the 114. The antipicks work together to hinder picking and help defeat impressioning attacks by lifting the lever slightly away from the key. Note that the lever marked B (bottom middle) has no antipicks. Each lock has an A, B, or C lever without antipicks to ensure smooth operation under all circumstances, just as with many pin tumbler locks.

Figure 17-3: Chubb 114 levers

Locks used in competition should have steel stumps with rounded edges, and preferably steel levers.

DETECTOR MECHANISMS AND ANTIPRESSURE DEVICES

Detector mechanisms and antipressure devices are just a couple of the often creative and advanced ways that lock designers have invented to prevent picking and other attacks. Chubb created the Detector, for example, hundreds of years ago after an English naval dock was robbed via lockpicking. When the wrong key or a picking tool is used and lifts the trigger lever(s) too high, the Detector jams in the locked state, indicating that it's been tampered with. The only way to reset it and reallow normal locking is to turn a correct key the *wrong* way. Antipressure devices are designed to frustrate picking by, for example, jamming all the levers if the lock bolt is tensioned.

You won't meet any of these in any contest, however, mainly because opening them in a few minutes without lots of preparation is far too hard. Fifty contestants with no open wouldn't be much fun!

European Competition Locks

In mainland European competitions, the double-bitted lever lock is most common. Often mounted on the back side of a door as a rim lock, with the resultant very long keys, these locks often also throw bolt work worthy of a safe: in three directions, requiring multiple turns of the key to open. Two complete rotations of the key will throw the bolt work four times, giving a high level of resistance to physical force, and the levers have four sets of gates that engage at different times.

The good news is that these locks are fairly easy to pick if you have the dedicated tool for them. The bad news is that you don't own that tool, and the bolt is 100 mm away through a small keyhole.

Unlike single-bitted locks, double-bitted locks often have only a single lever spring to reset the lock. The BODA shown in Figure 17-4 works like a single-bitted lock, apart from the double-throw-in-one-turn operation, and you can't push the levers back down.

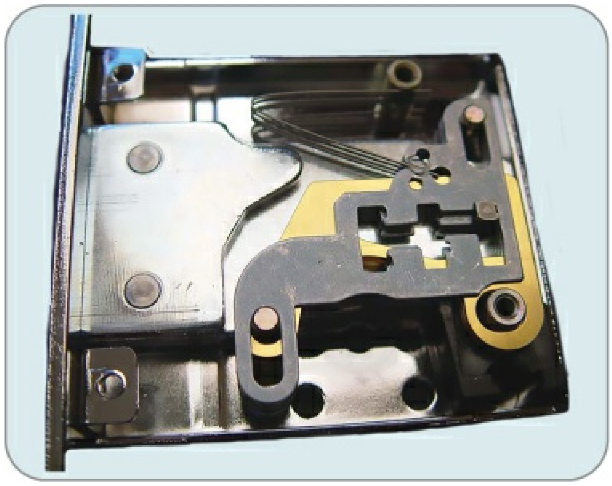


Figure 17-4: The BODA (Finland) 42x double-bitted, eight-lever lock

You can see the single lever spring in the Mauer 71111 in Figure 17-5. In these locks, you use the lower half of the key to prevent the levers from lifting too high. The main difference in picking them is that, if you overlift, you can simply push the overlifted lever back down by pushing against the bottom of the lever.

Figure 17-5: The Mauer 71111

Notice that the Mauer 71111's lever is lightly trapped in a true gate and can't move up or down (although a picking arm on a Hobbs pick could push it up or down freely). The antipicks are fairly aggressive, but you can skip them if you reduce the tension enough, and the lack of individual springs means that the whole lock won't likely reset.

The other difference from single-bitted locks is that because of the absence of individual springs, in double-bitted locks the friction between adjacent levers tends to move them a little as you move their neighbors. You'll frequently have to push the nonbinding levers back down, as they freely lift with the binding lever. You also need less force to move them, and they may or may not fall under gravity.

UK Competition Locks

UK lever locks are almost exclusively single-bitted keys and curtained locks on doors, but we also have hundreds of years of safe locks, containers, and padlocks, so you're more likely to run into a variety in a competition. The locks could be noncurtained locks running from two to seven levers, with a huge difficulty range, or they could be curtained lever locks running from three to seven levers (though usually five).

Though you can pick a curtained lock in exactly the same way as a noncurtained one, you'll find the kit required differs significantly. Gone is the beautifully lathe-turned, precision-fitted 2-in-1 tool; instead, you'll use bits of bent wire and maybe a cut-down key! You might even see something like precision-bent wires and CNC wire EDM tensioners.

Don't worry, though: the wire will lift the levers just as effectively, and the tension will work just the same too. Getting the hang of the different tooling styles will probably take you a while. Remember that any curtained door lock is a single throw, and the levers will be individually sprung (the only exception is the APECS LX5).

The locks you'll most likely encounter are the UNION StrongBOLT and the ERA Fortress 2. For all practical purposes in picking, these locks are identical, and they are the most common British Standard lever locks around.

> If you really want to know, the UNION has eight key cut depths, and the ERA has seven. That's the only noteworthy difference when you're using a wire curtain pick. In my opinion, the StrongBOLT is generally a slightly harder pick.
>
> —NIGEL

Improving Your Odds of an Open

Now we'll talk about a few other steps you can take to improve your chances of getting an open when you're in a competition setting.

Controlling Your Nerves

Keep your cool in the competition and under test. The adrenaline surge will numb your sense of feeling in your fingers, so you'll be tempted to use more force than necessary. You'll feel as if time slows down and yet somehow passes faster. Of course you want to win, but don't let the moment get to you—that's how you end up breaking things or failing to open your lock.

Practice under pressure helps you get used to this; with a few competitions under your belt, you'll find your nerves will calm down. (Then again, once you have a reputation for opening, you might get stressed for the *opposite* reason, so don't put too much pressure on yourself, either!)

Practice on a variety of locks so you're not flummoxed by an unfamiliar one in the moment. Similarly, figure out which technique works best for you to open fast. Do you hyperfocus on the noises coming from the levers? Do you count the taps and track the movement of the picking arm through the lever pack? Are you holding the tensioner effectively to get the best feedback from the tiny movements as the bolt shifts? Remember that competitions tend to be noisy!

Getting Intel on the Lock

So far, LockCon has yet to reveal the locks that will be or have been used in its competitions (the organizers obscure the brand and model on the locks they use). This is because the cost of swapping those locks for another type would be too high. In the MLA lever opening test, you have to tell the examiner what the lock is (multiple British Standard five-lever locks are assigned randomly, and the locksmith has to identify their lock via the keyhole, then open it, right-facing, within one hour). Since the organizers are unlikely to give much away, ask yourself what information you already have about the lock. What can you learn from the outside?

When you have a lot of time with a lock, you can try multiple methods of opening. In a competition, you want to get to the right method as quickly as possible. Let's look at how to accomplish this.

Holding the Lock

Bolt pushing (applying direct pressure on the end of the lock bolt to bind the levers) isn't allowed and probably wouldn't give you enough feedback on any decent lock, anyway. Most competitions have the *keep* (strike plate) screwed over the bolt, or some other defense, to prevent this. Plus, a curtained lock could end up out of sequence—meaning that the curtain is at the wrong rotation to drive the bolt—requiring the lock to be disassembled prior to the next round.

Examining the Lock

As mentioned, the competition organizers deliberately obscure the lock's model or even the brand to avoid revealing significant information about the lock's peculiarities. Still, you can look at the keyhole to determine whether it's a single- or double-bitted lock. You can also check whether a curtain is present. A curtain won't really make that big of a difference for the picking process, but you won't be surprised to see a wire pick instead of a 2-in-1 or Hobbs tool.

Feeling the Lock

The organizers won't permit you to fiddle with the locks and picks beforehand—that's cheating! But what can you learn when you're allowed to touch the lock?

First, does the tool turn smoothly or does it need maintenance? The two parts of the picking tool must move separately and without binding or grinding, both forward and backward under the levers, and in rotation. Don't confuse this with hitting the levers! Organizers usually check the tools between rounds, but if something seems wrong, speak up. Also say something if the pick simply spins freely—if a part has snapped off, you need to mention it right away.

Next, find the location of the levers, and, more importantly, the bolt. It's usually at the far side of the lock, but can also be in the middle of the lever pack, or at the front if the lock is facing the other way (bolt facing right). Nearly all current lever locks (bolt facing left) have the levers sitting either on both sides of the bolt or in front, nearest to you and the lock cap. The tool will be able to reach all the levers by design, even if they're on both sides of the bolt, but you must ensure that you apply the tension *to the bolt*, not a random lever.

After the competition starts, if you know the number of levers, you'll be able to count them once to confirm. If you don't know, you'll have to find them and count them, probably twice or until you get the same result twice. Then check the spring pressure:

- On locks with a single main spring, you'll feel the spring as you tension the lock, and the levers will then "float" freely. You'll be able to push them up and down with the picking tool with almost no force.
- On locks with individually sprung levers, you'll always feel the spring pressure trying to return the lever to rest, unless it binds and doesn't return, or gets caught in a (false or true) gate.

Typically, levers are above the keyhole, but they can also be to the side (see Figure 17-6). When you have differently curved lever bellies, you'll hit the bottom of some levers early, and others later. On some locks, this is a basis for decoding, but you'll need free movement underneath the lever pack. Either your tool must allow this or you'll be using a wire curtain pick, not a 2-in-1, which can be "scooped" under the bellies at certain angles. This takes practice to avoid disturbing the levers or overlifting them, possibly over the true gate height.

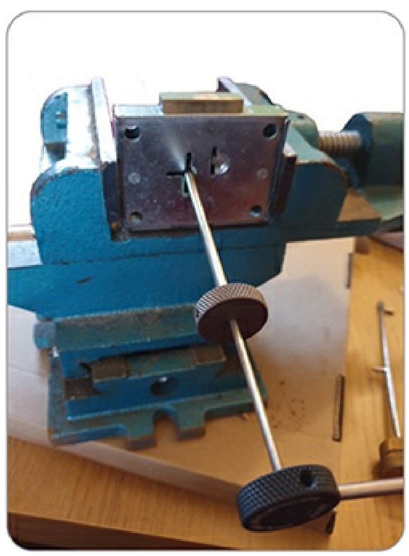


Figure 17-6: A seven-lever safe lock with a three-way keyhole that allows mounting with the bolt facing up (as shown here), left, or downward. When the lock is positioned like this, the lever pack will be found on the right of, rather than above, the keyhole.

Finally, what about antipick protections? The lock might not have any, or they might be disabled by the pick. You'll need to figure this out as soon as possible and keep a mental note. Your picking tool will avoid a curtain or wards for you, and a mainspring that resets the levers will be disabled by the tensioner. (At the high end, the lock could have antipressure stumps and detector mechanisms, but you won't see those in a regular lock and certainly not in competition.) Also keep in mind that you can drive a double-bitted lever back downward if it's lifted too high.

Asking About the Lock

You'll be briefed about the lock by the organizers. Unlike for the pin tumbler lockpicking competitions described in Chapter 8, asking others for intel about lever lockpicking is tricky. It's poor form to ask what's going on inside the lock rather than figuring it out for yourself, mainly because knowing that a certain lever should be immediately lifted high gives you a mighty advantage over someone who has to fight through the antipicks to get there. Also, *tryout keys*—keys that approximate true keys, which you simply try until the lock opens—might be perfectly legal, so if someone tells you that key 12 of the set opens the lock, you're going to be in faster than anyone else!

We suggest keeping any specifics of the lock internals to yourself until after the competition is over. When in doubt, check with the competition organizers for how much discussion about the locks is allowed.

Competition Dos and Don'ts

Now we'll go over a few final dos and don'ts to improve your odds of success. First, remember to hold the picking tool perpendicular to the lock case (see Figure 17-7). Accidentally tilting the tool up, down, left, or right is easy during the excitement of competition, but doing so will make your life more difficult, as it will compress the pack in an uncontrolled manner.

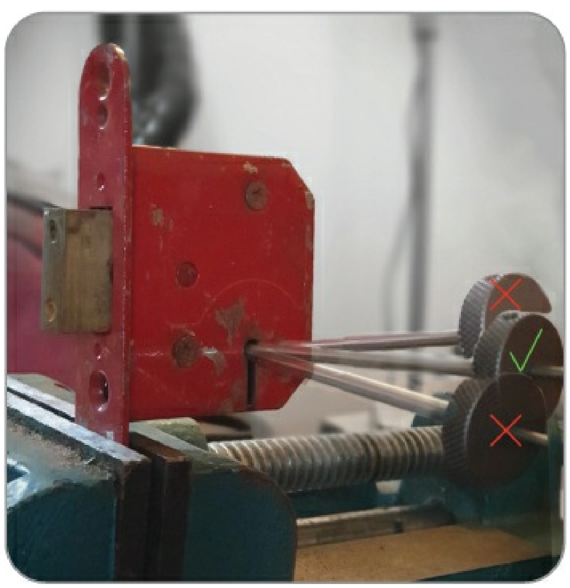


Figure 17-7: Keep your picking tool square to the lock face. If you compress the pack, take care to pull the tensioner straight outward, not tilting it, as the picking arm will hit multiple levers if you do.

Approach the lock with care. Test what the lock feels like inside; then draw your conclusions about the way it works. You'll be able to see the keyway, and that will reveal whether the key is single- or double-bitted. You already know that most single-bitted locks are individually sprung levers, and most double-bitted locks use a single mainspring. Confirm this when you find the lever pack(s).

Keep your cool, and don't be tense or cramped or use too much force. This advice holds true in any lockpicking setting.

Changing tension to go from clockwise to counterclockwise or vice versa, or changing sides of the lock, won't be an option. However, changing tools might be allowed, depending on whether you have another tool available. If you aren't using your own tools, though, you'll have to stick with the one the competition has provided. Have confidence in the tool!

NOTE

For example, if you're feeling desperate in the last few seconds, you could swap to a J wire on a single-bitted lock—but even with the tool right there, you'd better have at least 45 seconds to allow enough time to swap. Odds are good that changing tools won't be allowed, though.

You might consider differences in approach for the final round(s) as opposed to the first round(s), given that you have a more difficult lock and more time. However, as a rule of thumb, stick with what's been working! Bind and nudge, bind and nudge. Figure out where the antipicks are, reset and lift higher, and then bind and nudge, bind and nudge . . . If you can skip through the antipicks, remember how you did it in the earlier rounds—drop the tension off, keep light pressure on the target lever, pop it up and past the false gate, and repeat until open!

If you get completely stuck, you can always reset the lock, taking it back to a known state. Make certain to reset the lock fully, though. For some locks with square antipicks, completely releasing the tension won't reset the lock from an antipick, and in the extreme, you may need to drive the bolt back to fully locked to reset it. Likewise, with a single mainspring lock, you may need to turn the tension back a fair way to fully reset the lever pack.

Keep in mind that you might need to turn the lock more than once to open it. You *absolutely cannot* spin the picking tool to "flip" the lock around, as you can with a plug spinner on a pin tumbler lock. The design of the levers is such that they're already blocking the stump's next movement as they allow the first one. You'll bend or break something and get thrown out. Instead, you'll need to pick the lock again.

Recall and apply what you learned in Chapter 16. Remember that for many double-bitted locks, the key is symmetrical, meaning the low lifts and the high lifts are reversed, so this would be your best place to start when picking the second throw. This isn't the case for the best multithrow, double-bitted locks, where the two sets of bittings are independent.

Even the best double-throw locks, however, must have the same first and third, then second and fourth, lever alignments, so the first high/low combination will work the same on the third turn, and so on.

Running Your Own Lever Lockpicking Competition

If you decide to run your own competition, be prepared for budget shock. The typical equipment will set you back a few hundred dollars (or pounds) per competitor. You'll need an extra set of lock tools as well as a spare of everything else. Therefore, four competitors will need five lockpicking sets.

You'll need a selection of locks of various difficulties. Some will be too easy and others too hard, and you'll want to keep track of this as the rounds progress so that you can, perhaps, remove the easy locks from the final round. You might also want to throw in a lock that no one beat in the semifinals as a potent test of skill differentiation. Don't go overboard with this idea, though—having no openings in the final will likely be boring and frustrating! Aim for the easier end of the range. You need to have some openings within the timescale you set.

Let's look at a couple of LockCon competition setups to see what kind of equipment and cost might be involved.

2014 LockCon

The 2014 LockCon competition run by Jord Knaap used lower-end secondhand locks, though unmodified. These were the identical make and model from several manufacturing years by a safe company that used the lock on an internal compartment. These had four levers, and the build quality appeared to vary little over the decades. These locks were simply held in a vise, with the bolts visible, and the competitors were forbidden from touching the lock itself (see Figure 17-8).

However, it's incredibly unlikely that anyone other than a dedicated safe technician would ever have the opportunity to collect 16 or 20 locks of the same make and model for a contest. Knaap, being a skilled machinist and toolmaker, made the picks himself.

Figure 17-8: LockCon 2014 competition lock

2019 LockCon

The 2019 LockCon lever lockpicking competition was organized and sponsored by Ivo Poletto, founder and owner of Parmakey in Italy. The Italian team running the competition used an Italian-made, double-bitted, four-throw safe lock (that is, two complete turns move the bolt four times) with an *electronically indicating* bolt position switch added, meaning that a light on each lock showed the bolt's current position (see Figure 17-9). The first pick would turn the lock 180°, the second 360°, the third 540°, and the final the full 720°, and each turn would be tracked by the lights, which allowed the judges and audience to see each competitor's progress and the timekeepers to record accurate times.

The lock make and model still hasn't been revealed, as the organizers want to use the locks again in future competitions and don't want to give a tactical advantage to anyone who might buy and study those specific locks. The locks used were modified to make them more easily pickable (some levers or antipick features may have been removed), and, being relatively high-end, they didn't observe the usual "high becomes low on the next throw" pattern, meaning they're like two separate locks from a picking perspective.

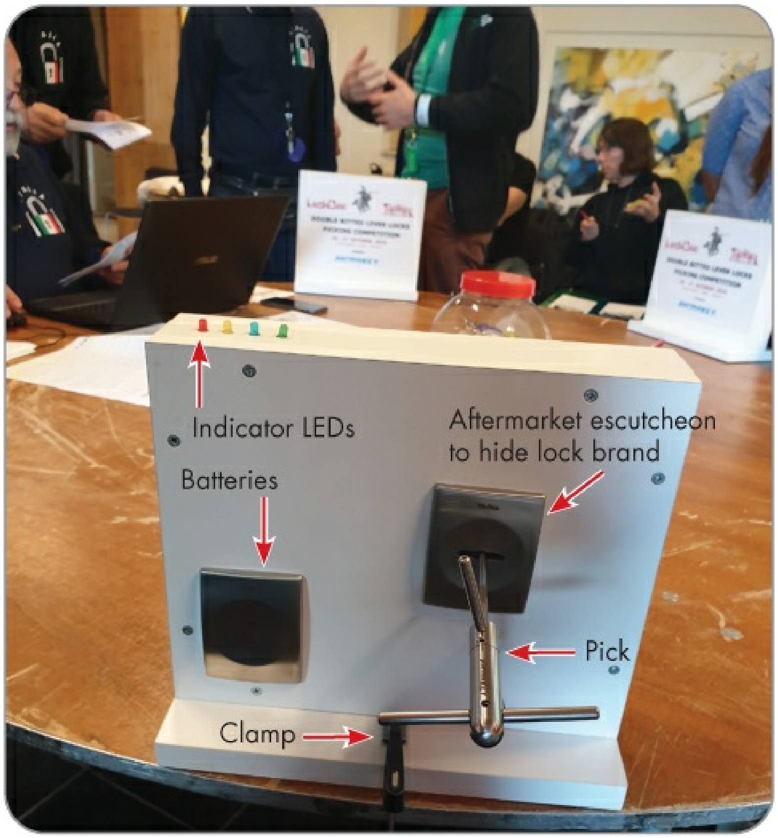


Figure 17-9: LockCon 2019 competition lock

These custom, identical competition rigs were clearly not cheap! The locks themselves are over $60 (€50) each. The tools were custom-made to suit the lock and cost more than double that. Parmakey made 10 picking tools and brought 10 locks, and the electronic mounting block obscured the entire lock. (Seeing a round trio of bolts or the faceplate, for instance, would give an advantage to anyone familiar with the lock.)

2022 LockCon

Nigel ran a small lever lockpicking contest at the 2022 event, using a single-throw, curtained, five-lever Kibb deadlock (see Figure 17-10). Four of the locks were modified such that the bolt couldn't be fully retracted, instead hitting a microswitch, which in turn stopped the electronic timer. This prevented issues with the lock ever needing to be reset with a key. Ten sets of curtain-picking tools were supplied too.

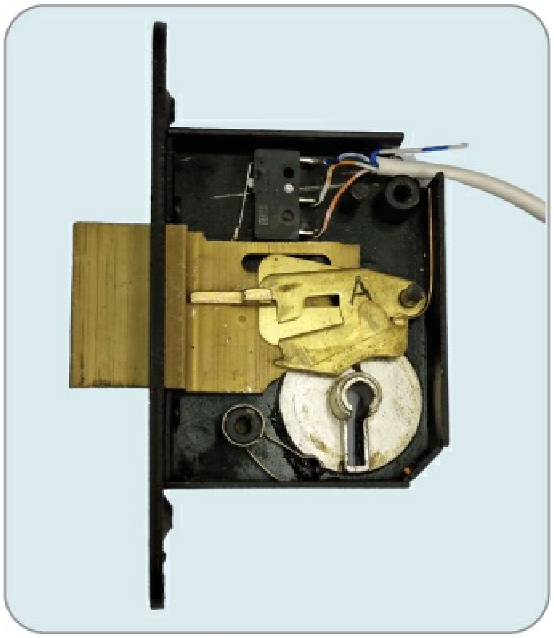


Figure 17-10: The single-throw, curtained, five-lever Kibb deadlock used at LockCon 2022

You can see some typical lever modifications in Figure 17-11. The top lever is unmodified, with square gate antipicks. The antipicks in Lever A have been filed almost completely away, meaning this lever binds very late in the picking order and is easily set correctly. Filing away the bottom edge of the square gate in Lever B meant that lifting the lever out of the antipick was far easier than having to do a full reset. One lever was also completely gutted into nothing more than a fancy spacing washer, which the stump would never touch unless the lever was lifted far, far too high.

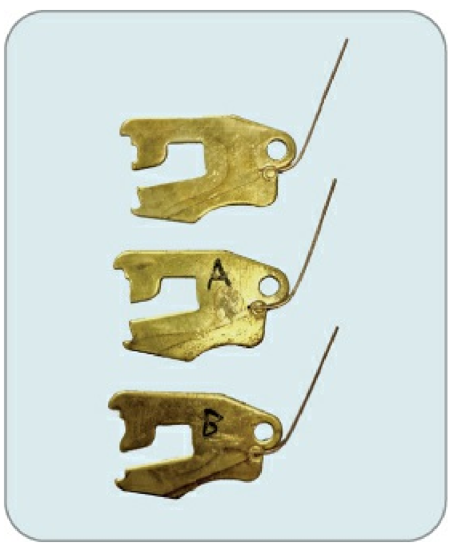


Figure 17-11: The lever modifications

Figure 17-12 shows the system in use. The heavy vise holds the lock in place securely. The red and black wires provide power for the timer, while the white wire goes inside the lock case to the microswitch. The curtain pick is one of Nigel's own design.

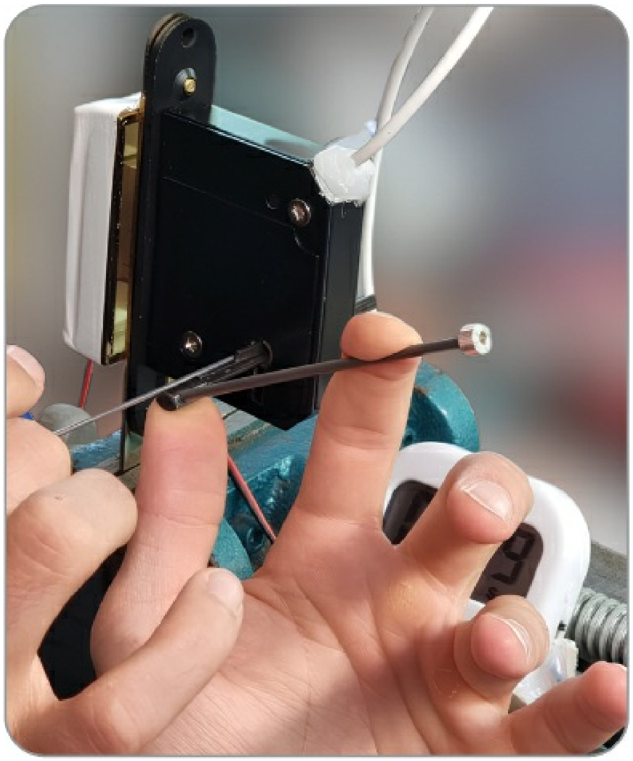


Figure 17-12: Picking the modified Kibb deadlock at LockCon 2022

NOTE

A neat trick from the MLA exam is to screw the keep directly to the face of the block holding the lock. This prevents someone from gaining access to the bolt or identifying the lock by peering at the faceplate. In Figure 17-12, the keep is bolted directly to the lock, and the remaining gap is then covered with tape.

The plan for this event was to swap in another set of unmodified levers for the top four players as a grand finale. However, despite the levers being modified, gates widened, and antipicks removed, the effectively four-lever "qualifier" lock turned out to be far too hard, with very few people opening it within 10 minutes even after multiple attempts.

Other Hosting Considerations

As you can see, running one of these contests is a big ask. The investment of time and money is pretty high. The lowest price for tooling would be around the $87 (£70) mark, and while the locks might be relatively cheap, they would require modifications to ensure opening in a seven-minute round. For example, you'll need a quick way to reset multithrow locks if they've only been thrown incompletely. You'll also need to have the standard key modified to work in this scenario that the lock was surely designed to prevent; this modification will be easier with some models than others.

All lever locks should be new or fairly new, and you'll need to make sure they've been serviced and made as similar as possible. Add in a vise and probably a block custom-made to hold the lock, and you'll be easily above $125 (£100) per station.

Summary

The tips and processes outlined here should give you a definite edge over your fellow competitors. Try to get some generic lever locks and picks and then practice some actual picking, and we'll see you on the podium soon!

Should you choose to run your own events, at least now you're aware of the potential scale of the undertaking. But don't let that put you off. If you get creative, you might be able to find ways around the challenges. And if you do run an event, we hope you'll send us an invite!

A
OTHER LOCKSPORT GAMES

Congratulations, you've now learned all the techniques needed to tackle the main competitions at locksport events around the world! In this appendix, we'll discuss a few locksport games that are frequently played at conferences or run by locksport organizations, but aren't part of the main competition. We'll cover the timed head-to-head challenge; a locksport spin on tic-tac-toe; escape challenges; bike lock decoding; and "The Room," a spy-themed contest. We'll end by taking a look at Reddit's belt system, one way to challenge yourself and earn public accolades from the online locksport community.

Timed Head-to-Head Challenge

One competition that appears frequently at conferences like ShmooCon, DEF CON, and various BSides events is the timed *head-to-head deadbolt picking challenge* (Figure A-1). Competitors are seated at wooden stands, each containing a pin tumbler deadbolt lock. Each deadbolt is the same brand, and all the locks are keyed alike (pinned the same). Each stand contains a built-in switch that's continually depressed by the bolt until the lock is picked. Those switches are wired to a circuit board or small computer, often an Arduino or Raspberry Pi, which is connected to a timer display that shows the opening time when the switch is triggered.

Figure A-1: Head-to-head timed challenge at an InfoSec conference

When the game organizer says go, competitors pick their lock as fast as they can. Sometimes the fastest person to open in each group is dubbed the winner, though more often every competitor's time is recorded over the course of a day, and the best times win a prize.

At least four stand designs are used in the US: two created by Dosman (@dossman33) of the Fraternal Order Of Lock Sport (FOOLS) club in Indiana (Figure A-2), one used by TOOOL US at large conferences (Figure A-3), and one created by Matt and his friend and fellow hacker volty for use at events around Seattle. Three of these designs are functionally the same for competitors, though one of Dosman's also includes rumble motors to make the locks shake, increasing the difficulty. This stand is called the Rumble Challenge.

Figure A-2: One of Dosman's nonrumbling stands at ShmooCon

Figure A-3: One of the TOOOL US stands

Timed Challenge Tips

At first glance, the timed challenge may seem pretty easy: you need to pick just one lock, and usually it's not even a high-security model. However, several factors make this challenge unique.

First is the stand itself. Having the lock mounted to a board can be a surprising twist for locksporters who typically hold their locks or mount them in a vise at an angle that suits them. Since picking in this position might feel awkward to you, consider practicing on a lock mounted on a vertical surface before entering this competition. You might also want to ask the judge if you're allowed to move the stand before you start; placing it on your lap might be more comfortable.

Second, unlike most locksport picking competitions, in this event it matters which direction you turn the plug. Unlocking the deadbolt requires retracting the bolt, meaning the plug needs to rotate away from the bolt. Whether this means you need to turn the plug clockwise or counterclockwise depends on which way the lock is mounted. For the stand in Figure A-2, you'd need to turn the plug counterclockwise to open it. Many contestants miss this detail and waste valuable time picking the lock in the wrong direction.

Third, rules about placing tension wrenches in the lock before you start picking can vary from event to event. Positioning the wrench ahead of time can save you valuable seconds, so be sure to ask the judge before the round starts whether this is allowed. If it isn't, ask if you can at least test various turning tools first to see which fits best.

Fourth, going head-to-head with other people can be intimidating, especially when a timer is running. Try to focus on the lockpicking, not on the timer or on anyone else's progress. Also try to ignore any spectators, as this type of contest is quite visual and can sometimes draw a crowd. If you're easily distracted by other people, consider trying to find a lull in the crowd sometime during the event and play then. In lockpick villages at large events, lunch breaks and breaks between talks are usually busy times and best avoided by those who suffer under pressure.

Finally, check the rules for do-overs. Some competitions allow you to retry the contest only a set number of times, if at all. Others may take your best time during the event, or they might average all of your times. Based on the rules, decide whether you're likely to improve your time by trying the contest more than once. However, be considerate of other competitors and the judges' time. Even if retries aren't limited, having one contestant keep trying the contest continually throughout an event can be annoying, especially if judges are overseeing multiple events.

DIY Set Instructions

Building a timer set of your own can be time-consuming, but it's reasonably easy. Matt published the code needed to run the timer on a Raspberry Pi on GitHub at *https://github.com/mburrough/locktimer*, so building a set is mainly a woodworking project. Here we'll list the materials to build four stands, but feel free to adjust up or down depending on your needs. Since this design uses US-style deadbolt locks, we're also specifying the materials in imperial units. Materials in metric equivalents should work just as well. If you're looking to build only one set for home practice, just quarter the material quantities.

- Four double-sided deadbolts that are keyed alike
- Four feet of 2"×4" lumber
- Seven feet of 2"×6" lumber
- Raspberry Pi, model 3 or higher (with power cable and microSD card)
- USB mouse and keyboard
- HDMI cable
- MicroSD card reader
- Four micro switches, like those used in arcade games, one per lock (for example, the Micro Switch with Roller Lever at *https://www.adafruit.com/product/819*)
- A monitor or TV with HDMI input, large enough for everyone competing to be able to see
- Paint (spray paint works well)
- Eight 6" screws
- Twelve 3" screws
- Sixteen 0.75" screws with truss (broad) heads
- Eight 0.5" screws for attaching the micro switches
- Five Ethernet cables (the fifth cable will be stripped for wire to solder to the switches)
- Eight Ethernet/RJ45 keystone jacks
- Four surface-mount keystone outlet boxes (like the Surface Mount Box 2 port at *https://www.monoprice.com/product?p_id=7089*)
- Solder
- Sixteen stick-on rubber feet
- An outlet box
- A four-keystone jack outlet faceplate
- Four pieces of clear acrylic, cut to approximately 4"×6"

In addition to those parts, you'll also need several tools:

- Drill
- Drill bits
- Saw
- Screwdriver bit for drill
- Soldering iron
- Wire cutter/stripper
- Door lock installation kit (sold at hardware stores; includes two hole saws and a plastic template to aid in drilling)
- Sandpaper
- A woodworking router and bits

Making the Stands

Follow these steps to assemble the stands:

1. Cut the 2"×6" board into four 12" lengths and four 9" lengths, and cut the 2"×4" board into four 12" lengths. The longer 2"×6" pieces will act as the door to which you'll mount the deadbolt. The 2"×4" pieces will be the door frame where the bolt of the lock enters. Finally, the shorter 2"×6" pieces will serve as the base for your stands.
2. Drill one large hole through the 12" portion of the 2"×6" to mount the lock. The center of the deadbolt should be about 4.5" down from the top of the board. Use the template included in the door lock installation kit to drill a smaller hole into the side of the 2"×6" for the bolt to pass through.
3. Once the holes are drilled, follow the instructions that come with the deadbolt to install the lock. Make sure all your holes are aligned and the lock is working properly. Note that doors are slightly thicker than 2"×6" lumber, so you may need to adjust the tightness of the screws if the lock isn't working smoothly. Extend (lock) the bolt by using the key.
4. Next, line up the 2"×4" with the 2"×6". Note where the bolt will need to enter the 2"×4" and how deep it will go, and trace this onto the 2"×4" with a pencil. Also position one of the micro switches on the 2"×4" to determine where it will be depressed when the bolt is engaged, and trace it as well.
5. Using a woodworking router, notch out a pocket on the 2"×4" big enough for the bolt to fully extend, with room for the switch to sit in the pocket as well (see Figure A-4). The section under the bolt may need to be deeper than that under the switch so that the switch's arm can hit the center of the bolt.

Figure A-4: A batch of stands with holes drilled for the locks, and pockets cut for the bolts and switches

NOTE

At this point, you could remove the lock from the 2"×6" and sand and paint all the wood parts. However, we prefer to build the entire stand first to make sure everything works, and then disassemble it and paint it at the end.

6. Realign the 2"×4" and the 2"×6" pieces and confirm that the lock still functions. If so,

drill two pilot holes through the edge of the 2"×4", one near the top and one near the bottom, and then use 6" screws to connect the two boards (see Figure A-5 for an example from a completed stand).

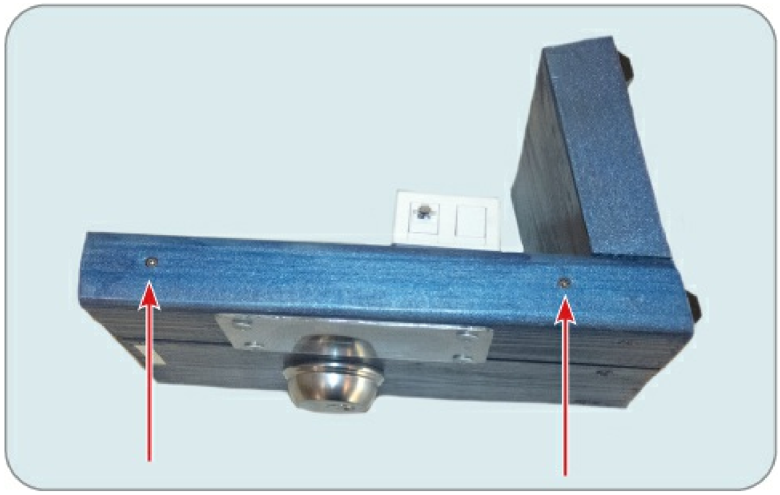


Figure A-5: Two 6" screws securing the 2"×4" board to the 2"×6" board on a completed stand

7. Determine where in the pocket the switch will need to sit, and drill two pilot holes for mounting the switch. Also drill one hole below the micro switch completely through the 2"×4" for the switch's wires.
8. Cut one of the Ethernet cables into 6" lengths. Remove the individual wires from the cable's jacket. Strip 0.75" of insulation from one end of two of the wires. With your soldering iron, solder two wires to the switch's terminals. If the switch has three terminals, use the normally closed (NC) and common (com) terminals.
9. Once the solder is cool, place the switch in the pocket and push the cables through the hole to the back of the stand. Screw in the switch and confirm that the bolt still fully extends and that the switch is depressed by the bolt.

On the back of the stand, install the keystone box over the area where the wires are protruding. The RJ45 keystone jack should come with a punch-down tool; use that to punch the wires into any two of the jack's eight positions. (The example shown in Figure A-6 uses orange and white-orange, but it doesn't matter which you use as long as you're consistent.) Trim any excess wire. Snap the jack into the keystone box and close the box.

Figure A-6: The back side of a completed stand with an open keystone box (left) and a close-up of wires feeding into the RJ45 jack

10. Drill a hole in each corner of one of the acrylic pieces. To avoid cracking the acrylic, don't drill closer than half an inch from the edge, and if possible, use a drill bit meant for acrylic (we recommend the ones from TAP Plastics at *https://www.tapplastics.com*). Using the truss head screws, screw the acrylic over the pocket in the 2"×4" (see Figure A-7). This will allow contestants to see the bolt but not to touch the switch or wires.
11. Finally, drill two pilot holes three-quarters of an inch from the bottom in the front of the 2"×6" and another on the bottom of the 2"×4". Be careful to avoid hitting the 6" screw connecting the boards. Using these pilot holes, attach the 9-inch 2"×6" with 3" screws, as shown in Figure A-7.

Figure A-7: A finished stand

You should now have one fully completed stand that can stand on its own. If everything seems right, repeat the entire process three more times. If you haven't painted them already, now you can disassemble them, sand any rough edges, paint them, and let them dry. Once they're dry, reassemble them and attach the rubber feet to the bottom.

Setting Up the Raspberry Pi

After building the stands, you need to wire up the Raspberry Pi. Using more scrap Cat5 cable, punch two 8" wires into each of the four remaining RJ45 jacks. Be sure to use the same positions on the jacks that you chose to use on the stands. Run these wires through a hole on the outlet box, snap the jacks in the four-keystone wall plate, and screw the plate to the box with its included screws.

Make sure the Pi is unplugged; then solder one wire from each jack to a ground pin position on the Pi. For the jack you want to use with the first stand, solder the remaining wire to GPIO 4 on the Pi. Solder the remaining wire for stand 2 to GPIO 17, stand 3 to GPIO 27, and stand 4 to GPIO 22.

Plug one end of each Ethernet cable into the jack on each stand, and the other end into one of the jacks now connected to the Pi. Connect a USB keyboard and mouse to the Pi, and use the HDMI port to connect the monitor.

On a computer, install the Raspberry Pi OS on your Pi's SD card by following the directions at *https://www.raspberrypi.org/software/*. Place the SD card into the Pi, boot it up, and log in. Next you need to download the locktimer program. Connect the Pi to the internet, and then open a terminal window and enter the following:

```
sudo pip install guizero
git clone https://github.com/mburrough/locktimer/
cd locktimer
python timer.py
```

This installs guizero, a Python library used by locktimer, followed by locktimer itself. Then you move into the locktimer directory to run it.

You should now see the locktimer interface. If the program doesn't fit on the screen, run `timer-720.py` in the last step instead.

Running a Competition

Now it's time to set up a competition! First, make sure that all the locks are locked and the stands are plugged in to the Pi. Click the **Reset + Go** button to start the timers. You should see four individual positions with the status LOCKED, as well as a larger overall timer. As soon as one of the locks opens, the time for that seat will replace the word LOCKED, but the timer will continue running for the other seats. Once all the locks are open, the overall timer will also stop.

NOTE

The timer code is written for a four-stand setup with four players. You'll need to edit the code if you want to have more or fewer stands.

If at any time you want to stop the timer, click **Stop**. Clicking Reset + Go will reset all timers back to 0 and start them over.

Be sure to have a key handy to reset the locks so that you don't have to pick them again just to lock them. Consider using double-sided deadbolts, rather than single-sided bolts with a thumb turn on the back, to help prevent cheating.

PicTacToe

Another head-to-head lockpicking competition is *PicTacToe*™ (see Figure A-8), created by FoxPick. In this locksport take on tic-tac-toe, two players try to be the first to pick three locks in a row in an illuminated 3×3 grid.

Figure A-8: Jenee Rogers of FoxPick ready to start a game of PicTacToe

Gameplay is straightforward: each player is given an electronic game board with nine locks, as well as tension tools and picks. Rakes are not allowed. All locks start illuminated blue, as shown in Figure A-8. When a player picks a lock, it turns green on their game board. The corresponding lock on the opponent's board turns red to indicate that spot is taken. The first player to get three green locks in a row vertically, horizontally, or diagonally wins, and the winning line flashes. In the event of a draw (as in Figure A-9), both players' boards flash. After the game ends, the organizer presses two reset buttons, which clears the boards and relocks all the locks.

Figure A-9: A completed game of PicTacToe that ended in a draw

PicTacToe Tips

As it's a fairly new game, none of us have yet had a chance to try PicTacToe. Luckily, the friendly folks at FoxPick have offered several suggestions for competitors. First, as with the head-to-head challenge, players should practice picking locks mounted on boards. Since the PicTacToe board is even larger than the head-to-head lock stands, players won't be able to make significant adjustments to the position or angle of the locks.

Second, the locks in PicTacToe aren't all the same. The center lock is the hardest, the corners are medium difficulty, and the four remaining locks are the easiest. Having a strategy for which lock to target first and which row/column/diagonal you plan to pick before starting will save you time during the competition.

Third, since rakes aren't allowed, practice picking using standard hooks. You may also want to practice with picks other than your usual set. Since picks are provided, it's best to be comfortable working with one that isn't your favorite.

Lastly, this is a player-versus-player contest, so it's a good idea to practice picking under pressure against someone. Also consider whether you'll just go for the locks you need to open or also try to block your opponent by targeting a lock in the row they've selected.

Escape Challenges

Escape challenges are a type of game that used to be played regularly at various conferences and may still crop up from time to time. The premise is that the contestants have been unlawfully detained and must free themselves from their captors. In the original version, created by Deviant Ollam, the hypothetical scenario was that contestants had been detained by corrupt police officers in a foreign country. Their passports and wallets had been confiscated and locked in a filing cabinet, but their concealed set of lockpicking tools was overlooked.

Contestants started handcuffed and had five minutes to remove the handcuffs, pick their jail cell or interrogation room lock, pick the filing cabinet lock to retrieve their passport, disable a guard, pick a locker lock to retrieve a guard uniform for disguise, pick a lock on the door leading outside, and optionally pick the lock of a car to use for a getaway.

WARNING

While escaping a captor or playing a secret agent can be fun to imagine, don't use your locksport skills to actually resist arrest or try to escape the police. Doing so is illegal and dangerous, not to mention it goes against the rules described in Chapter 1.

Of course, an entire jail can't be transported to all competitions around the world, so suitable stand-ins have been used. A pair of handcuffs, a couple of deadbolts, a wafer cabinet lock, a padlock, and an ignition lock represented the locks described in the scenario. To make the game playable and enjoyable for expert and novice pickers alike, the game's organizers provided several locks of varying difficulty for each part of the challenge. Scores were determined based on the difficulty of the lock opened at each stage, with extra points added for faster escapes.

The original version ran for several years at conferences like ShmooCon, Ekoparty, and DEF CON, but it was officially retired in 2011. However, variations of the game live on, surfacing every few years at InfoSec conferences. For example, a spy-themed challenge was presented at ShmooCon 2017. In this variation, two contestants went head-to-head and had to break out of handcuffs, pick a deadbolt to get out of a room, pick a rotary-phone-dial lock (wafer lock) to call for backup, and finally pick a padlock on a duffel bag containing a Nerf gun to shoot a final target and escape (see Figure A-10).

Figure A-10: The various locks to overcome at one jail break–style competition at ShmooCon 2017

Escape Challenge Tips

Most of the locks in these competitions, such as deadbolts and padlocks, are ones that most locksporters have picked before—even if they haven't seen them on a phone or duffel bag. As in the timed lockpicking challenge, the only real hurdles are picking the locks at a potentially uncomfortable angle and making sure you're turning the plug in the proper direction. However, the other locks in the escape challenge may be new to you. We'll start with handcuffs and then look at wafer locks.

Handcuffs

Handcuffs have been around for centuries and have used a variety of styles and locking mechanisms throughout their history. That said, in many countries, the most common handcuffs are ratcheting cuffs that go on the wrists and are connected by a couple of chain links, like those in Figure A-11. These are manufactured by companies such as Peerless Handcuff Company, ASP, and Smith & Wesson.

Figure A-11: A standard pair of handcuffs

These handcuffs all work the same way: one half of each wrist's cuff pivots open on a riveted hinge point and has a series of teeth on the end. This part, called the *single strand*, is functionally equivalent to the shackle of a padlock. These teeth of the single strand interact with a *pawl* inside the handcuff's housing, which is a spring-loaded piece of metal with a few teeth of its own and is similar to the latch found in a padlock (see Figure A-12). The locking mechanism for these cuffs is essentially a warded lock. A small protrusion on the key depresses the tip of the pawl, retracting it from the single strand's teeth, to unlock the cuffs.

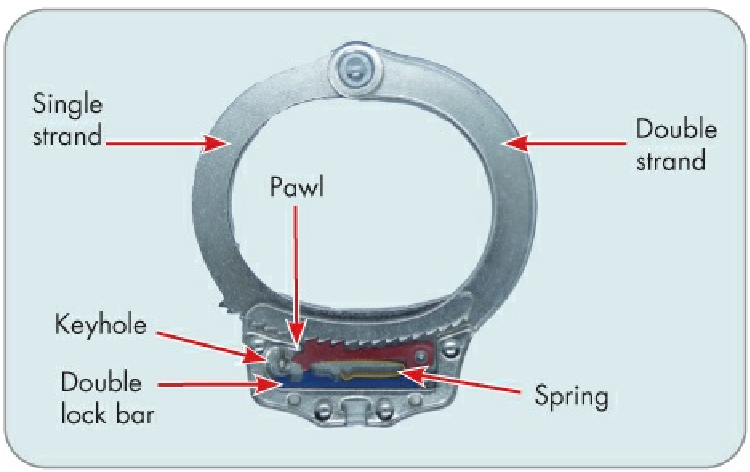


Figure A-12: Cutaway of a standard handcuff

Since the handcuffs ratchet, they are susceptible to the same type of shimming attack as padlocks that have latches. By slipping a thin piece of metal between the single strand and the pawl, you can depress the pawl, unhook the teeth, and pull on the single strand to get it to open. Figure A-13 shows Matt using a thin tension wrench for this purpose during a competition. Thinner, commercially available handcuff shims also work well and can be purchased online from retailers such as Serepick (*https://www.serepick.com*) or Handcuff Warehouse (*https://www.handcuffwarehouse.com*).


Figure A-13: Matt shimming his way out of handcuffs at ShmooCon

NOTE

Getting a piece of metal between the teeth of the single strand and the pawl can take a fair bit of force, possibly requiring you to hit the cuffs against a hard surface. Be careful, as this can easily result in bruised wrists, as Matt proved shortly after this photo was taken.

Using a shim is straightforward: insert the tip of the metal below the single strand into the housing, apply pressure on the shim, and then click the single strand one notch tighter. As the teeth of the single strand depress the pawl, the shim should slide between the pawl and the teeth and allow you to pull back on the single strand to release it.

Realizing this issue with the design, handcuff manufacturers have made most modern handcuffs *double locking*: a second piece of metal below the pawl can be pushed into place after the cuffs are applied to block the pawl from lowering. This not only prevents shimming but also serves as a safety feature for the handcuffed person; the cuffs can't be tightened further when double locked, so they won't accidentally constrict the person's wrist. To unlock a double-locked handcuff, you must turn the handcuff key in one direction first to release the double lock, then in the opposite direction to lower the pawl.

In competitions, the double lock is rarely applied. Usually, the only added difficulty is the handcuffs' placement: behind the back. If you're flexible, you might be able to overcome this by trying to step over your own arms as if they were a jump rope or by bringing your arms over your head.

If the cuffs are double locked, you won't be able to shim them, so you'll have no choice but to pick the lock or use a handcuff key. From a standard lockpick set, we suggest using either a short hook or half-diamond, though if you have any dimple lock picks, those might work well. Insert your tool in the keyhole perpendicular to the face of the handcuffs, as shown in Figure A-14.

Figure A-14: Proper orientation for the picking tool to open handcuffs

Try to push away the double-locking bar and then catch the pawl with the tip of the pick. The bar will be at the bottom of the cuff, near the chain, while the pawl is closer to the wrist, as shown in Figure A-15.


Figure A-15: Rotate the picking tool clockwise to release the double lock, and counterclockwise to retract the pawl

Using picks on handcuffs can be tricky, especially if the cuffs are oriented with the keyhole facing away from you. Another option is to bring your own handcuff key (see Figure A-16 for an example). The vast majority of handcuffs can be opened using a universal handcuff key, which you can order online for a few dollars. Some universal keys are made to look like zipper pulls, buttons, coins, and cufflinks in order to be easily concealed. Be sure to check with the contest organizers to see whether these are allowed. In some contests, they're not permitted at all, and in others using them might deduct partial points from your score. They might also be illegal, so check your local laws!

Figure A-16: A standard hook pick profile (top) and handcuff key (bottom). The "spike" on the back of the key (left of the bow) is used for the double lock on some handcuff models.

To prepare for such a competition, you might want to get a set of handcuffs of your own. Again, check local laws to make sure possessing them is legal. If so, we suggest avoiding clear or cutaway cuffs like the example shown earlier in Figure A-12. The acrylic on these can be fragile, and you might break it when attempting to shim or pick the lock. Consider buying the handcuffs in a color other than the popular metallic silver or black to facilitate keeping track of them. If you already have a silver pair, you can always add some decoration to make them stand out.

Finally, and *most importantly*: when playing with handcuffs, always have several spare keys available, and practice with a friend nearby. You don't want to get stuck in a situation where you've dropped your key and can't reach it!

Wafer Locks

The wafer locks used on filing cabinets, phone-dial locks, and even vehicles may also be unfamiliar to you from a locksport perspective. Wafer locks are similar to pin tumbler locks in that they contain several blocking elements that need to be lifted to the correct height to allow the plug to rotate, so it's possible to approach picking them as you would a pin tumbler lock. However, you should be aware of a few tricks and gotchas when you're dealing with wafers.

First, wafers are flat plates, not round cylinders like pins. They have no shear line, but if you lift them too high, they'll block at the top of the plug rather than catching at the bottom. Particularly sharp or aggressively used rakes can then catch on the wafers, potentially damaging them, the small springs used to hold them, or even the rake itself.

Second, wafers can come from both the top and bottom of the keyway, so on some locks you'll need to move some wafers upward and some downward. For this reason, *ball-end* and *double-ball* picks (also called *snowman* picks), shown in Figure A-17, are popular choices for wafer locks. While these picks are often scorned in pin tumbler picking, their gentle curves and double-sidedness do well on wafers. Having said that, regular hooks and rakes will also work on wafer locks.

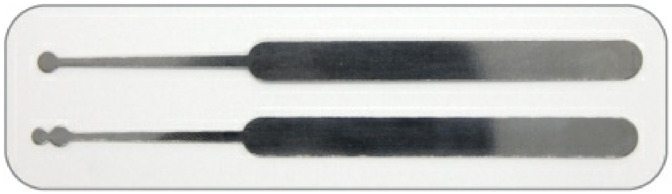


Figure A-17: Single- and double-ball picks

Next, most wafer locks contain only a few wafers. For file cabinet–type locks, three to five wafers is the norm. Additionally, their tolerances are often poor, meaning the wafers aren't precisely set to the correct standardized height. Taken together, these two traits mean that key-shaped objects might well open such a lock. Enter the *wafer jiggler* set: thin pieces of metal cut into shapes that look vaguely key-like, as you can see in Figure A-18. By inserting these in the lock (one at a time) and using rocking, raking, or jiggling motions, you have a good chance of opening the lock. You can purchase jigglers from many of the same sellers as regular lock picks.

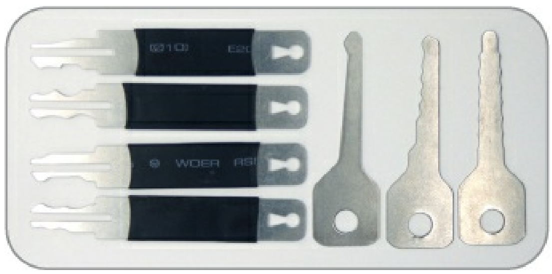


Figure A-18: Two sets of wafer jigglers

Another method of opening wafer locks involves using a flat piece of metal, like the handle of a pick or an uncut key that fits the keyway. Insert the object all the way into the keyway, using it both to lift all the wafers and to apply slight rotational pressure on the plug. Then, while still applying turning pressure, slowly pull out the object. Because of the lateral pressure, the wafers may bind on the lock housing as they drop, allowing the plug to rotate. This can take some practice and may not work on higher-quality locks.

If all these methods fail, simply try single-pin picking the wafers or raking with your least aggressively shaped rake. One final word of caution: some wafer plugs are held in their housing by the rearmost wafer in the lock, which is usually spaced a bit farther away from the other wafers. If you pick this wafer, which is especially likely if you're raking the lock, the entire plug will come out of the lock. This feature allows a special key to remove the plug to make rekeying easy. If this happens, you might still be able to open the lock by reaching a tool into the back of the housing and rotating the cam or manipulating the latch directly. To reinstall the plug, depress the wafers so they're flush with the plug and slip the plug back into the housing.

Direct-Entry Chain and Cable Locks

In informal competitions at locksport events, you'll frequently come across *direct-entry* combination padlocks and cheap bike chains, with too many variations and manufacturers to name. These generally have three, four, or occasionally five code wheels, like the one shown in Figure A-19. Each code wheel has one gate through which the teeth can pass, so when all the gates are aligned, all the teeth can pass and the lock opens. The better locks include one or two smaller false gates that the teeth can't fit through to make it harder to find the true gate.

Figure A-19: A five-wheel direct-entry cable lock, partially opened

As always, you'll need to tension the lock and look for the binding element. Pulling on the shackle will cause one or more of the wheels to tilt or jam against a tooth (see Figure A-20). Simply find the wheel that is binding (it will be the most difficult wheel to turn), and rotate it until it is free, or loose, or wobbly. Often the shackle will come out a little too. Now locate the next wheel that's binding and repeat the process until the lock opens.

Figure A-20: The wheels of a direct-entry combination lock (left) and the shackle (right)

Figure A-21 shows a cross-section of the lock. You can see that the blue shackle interacts directly with the yellow wheels. The housing is red. The two wheels on the left are still blocking the shackle, preventing it from being removed, and the two on the right are in a true gate. Under heavy tension, the righthand two wheels would wiggle loosely, and the other two would be jammed.

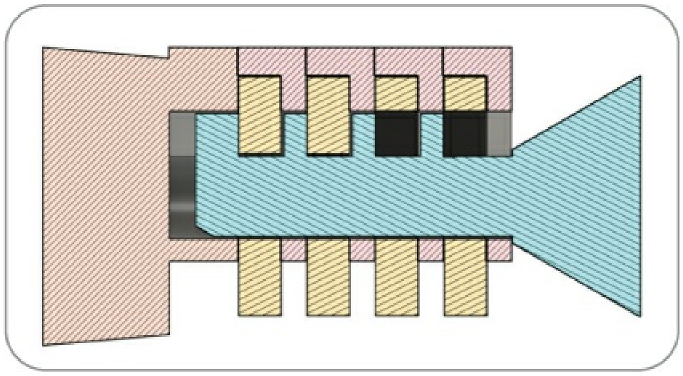


Figure A-21: A cross section of the shackle interacting with the wheels

When you come across antimanipulation false gates, you'll generally find that they're smaller. With practice, you can differentiate them from a true gate by feel; a true gate will give a bit more play in the shackle than a false one. Even if you haven't mastered differentiating false and true gates, you'll find that once all the positions are set on a gate, you can easily tell which wheel is in a false gate, as it will start to bind again. Often there's only one false gate per wheel, which is usually directly opposite the true gate. Sometimes, however, two or four false gates are located at fixed intervals all the way around.

Some of the better designs have a release button for the shackle that you may have to press to tension the lock. With practice, you'll be able to amaze your friends with how fast you can beat these locks.

The Room

At the HackerHotel conference held in the Netherlands in 2019, locksporters Jos, Jan-Willem Markus, and Rob Wiegertjes from TOOOL NL introduced a new competition called The Room. This competition is a spy/detective–themed scenario challenge. Teams are given seven minutes to enter a staged hotel room and gather as much information about the occupant as possible, while leaving no evidence they've entered the room. For videos of the 2019 event, see *https://blackbag.toool.nl/?p=2772*.

While not strictly locksport focused, the challenge has some interesting lock-related aspects. First, teams must find a way to enter the room. You'll be provided with an *under-door tool*: a long piece of stiff metal wire about 100 cm (40 inches) long, with a handle bent into one end and a hook bent into the other, shown in Figure A-22. A flexible wire, slightly longer than the rigid wire, is connected to the hook end. You slip the tool in the gap between the bottom of the door and the floor and rotate it upward to hook the door handle. Pulling down on the flexible wire flexes the rigid wire, pulling down on the door handle.

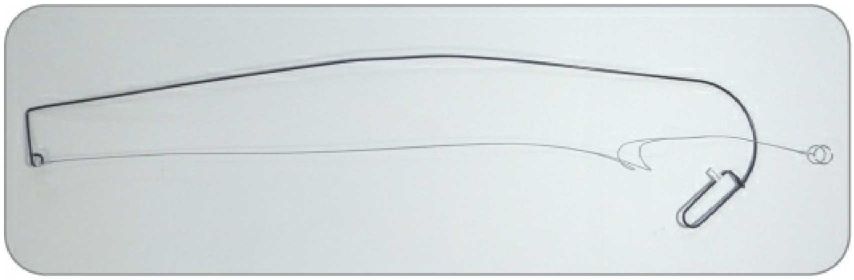


Figure A-22: An under-door tool

In Figure A-23, you can see Walter opening a glass door with an under-door tool. Since most commercial doors automatically unlock when the inner handle is pulled, this tool allows you to open the door without a key.

Figure A-23: Walter using an under-door tool

Once inside the room, the team must procure evidence from several locked items. The locked items are sure to change from year to year, but past examples include a wafer lock on a cash box (Figure A-24), a hotel room safe with electronic code keypad, a briefcase with a three-wheel combination lock, and a high-security padlock on a lockbox. You can approach these locks in multiple ways, but keep in mind that part of your task is to leave no trace, so you must pick them back to the locked position when you're done.

Figure A-24: A keyed lockbox from The Room

You can sometimes decode briefcase wheel locks like direct-entry bike locks—by pressing the release button on the case while spinning the wheels. If this doesn't work, you could slip a thin piece of metal between a wheel and the lock housing, rotate the wheel, and try to feel for any notches or flat sections of the wheel; then repeat this for the other wheels. If you've found a flat section or notch on each wheel and the case doesn't open, rotate all the wheels in the same direction and try again. For example, if you found notches at 3-7-2, try 4-8-3, then 5-9-4, and so forth. Many wheeled combination locks, like the one shown in Figure A-25, can be decoded this way.

Figure A-25: The combination lock on a briefcase used in The Room

For other locks, such as the electronic safe lock shown in Figure A-26, you'll need to look around the room for clues. You may find three- or four-digit codes written somewhere that could open combination locks, or you might find keys hidden someplace that can open keyed locks that aren't realistic to pick within the limited timeframe.

Figure A-26: An electronic safe used in The Room

Opening the most locks, or even getting the most evidence, doesn't guarantee a win in this game. It's more important to leave no trace of your presence. The winning team in the 2019 competition gave this advice: take lots of pictures. Photos not only provide copies of evidence but also can be used to reference an item's original position in the room so you can put everything back accurately. That team took over 850 photos during its seven-minute run.

Second, remember to wear gloves. Touching items in the room leaves fingerprints, which will count against you. You could take this a step further and wear a mask to avoid being identified on any hidden cameras. Taking it to the extreme, you might also consider wearing protective covers on your shoes to avoid tracking in dirt.

Third, assume that the subject of the investigation is very detail oriented. This means that simply leaving items *where* you found them isn't enough; you must also leave them *how* you found them. For example, if a pen was on the edge of a notebook and pointed toward the door, make sure it's in the same orientation before you leave.

Fourth, don't take items from the room. Even if something looks like trash that won't be missed or is just one piece of paper out of a large stack, the subject will likely notice it. Similarly, don't throw away or leave behind anything you brought into the room.

Finally, remember to look everywhere you can. Items may be hidden in unusual locations, like under the mattress, in a pillowcase, under the trash bag inside the trash can, or taped to the underside of a drawer. Simply finding the obvious items won't be sufficient to win the competition.

The Belt System

Inspired by martial arts, the organizers of the Reddit lockpicking community at *https://www.reddit.com/r/lockpicking/* have developed a color-based belt-ranking system to classify the relative difficulty of picking various brands and models of locks. Members of the subreddit who can show that they've picked a lock—and met the other requirements corresponding to a given belt color—are then awarded that belt as a flair badge for their

Reddit profile and the Lockpickers United Discord server (see Figure A-27).

Figure A-27: A redacted Reddit thread showing users' belt flair

For the lower ranks, you can simply submit a photo of the picked lock to gain that rank. Middle ranks require you to submit a video of the lock being both picked and disassembled to demonstrate in one take that the lock hasn't been modified to make it easier to pick. For the most advanced ranks—including purple, brown, red, and black—members must pick multiple difficult locks from a list of accepted locks while on video and must also engage with the community in other ways, such as posting frequently, creating and sharing custom challenge locks, and building custom tools.

To give some examples, picking any lock at all will earn you an entry-level white belt; a picked and gutted ABUS 72/40 earns you a green belt; a Fichet 666 is brown-belt territory; and an ABLOY Protec[2] merits a black belt. Note that a lock's specific belt ranking can change over time (for example, if new methods of opening the lock are found), so always check the subreddit for the current list before attempting to earn a belt. A full description of the criteria for earning a belt, and the list of locks that qualify for each, can be found at *https://www.reddit.com/r/lockpicking/wiki/beltranking/*.

The belt system is an interesting way to classify locks and can be helpful for beginners to determine, relatively speaking, how challenging a lock might be to open. However, the system does have its detractors. Some criticisms include the requirement to exclusively use single-pin picking to open locks at or above the green-belt level, the requirement to submit a video for locks at or above orange, and the fact that the system doesn't account for factors such as a lock's bitting.

If you like filming your picking attempts, enjoy socializing on Reddit or the associated Discord server, and like the idea of flair, then go for it! If not, don't feel this makes you any less of a lockpicker. Plenty of highly skilled locksporters don't worry about belts!

B
WHERE TO GET EQUIPMENT

One of the challenges for locksport hobbyists is finding good sources for equipment. Some sellers will deal only with bona fide locksmiths, while others are happy to sell you gear, only for you to find out that it's poorly made and not worth your money. To that end, we're providing this appendix of trustworthy vendors and merchants that sell lockpicking hardware.

It's worth noting that shops sometimes come and go, and others might ship only to a limited number of countries. Additionally, lockpickers each tend to have their own preferences, so what works for one person might not be great for another. Finally, not every tool from every vendor is great. Please don't view this list as an endorsement, but rather as a guide if you're having trouble finding the tools you need for locksport.

NOTE

This book is not a living document, so links we include may not work by the time you read this. Still, searching online for the text descriptions or vendor name should help you find what you need.

Picking Tools and Tensioners

The following sellers make lockpicking and tension tools available to locksport hobbyists:

- Covert Instruments sells several lock pick sets: *https://covertinstruments.com*.
- Foxhole Security sells Rytan and Moki brand lockpicking tools: *https://www.hooligankeys.com*.
- Multipick has single picks, pick sets, pick guns, and a variety of other tools: *https://shop.multipick.com/en/index*.
- Peterson Locksmith Tools sells numerous lockpicking supplies: *https://www.thinkpeterson.com*.

- Red Team Tools sells a variety of tools, including picks: *https://redteamtools.com*.
- SouthOrd lock picks can be found at *https://www.southord.com*.
- Southern Specialties offers several lockpicking tools at *https://lockpicktools.com*.
- SPARROWS Lock Picks makes and sells a variety of tools, including picks: *https://www.sparrowslockpicks.com*.
- TOOOL US sells a good starter set of picks, as well as practice locks: *https://www.toool.us/equipment/*.
- Wendt is more focused on professional users: *https://www.zieh-fix.com/en*.

Impressioning Tools

Several good places offer tools for impressioning:

- LockPicks.com states that it sells picking tools only to locksmiths, but it'll sell other items, including impressioning grips, files, and key blanks, to everyone: *https://www.lockpicks.com/locksmith-tools/impressioning-tools.xhtml*.
- Foxhole Security sells a pocket-size impressioning handle and impressioning file: *https://www.hooligankeys.com*.
- Every now and then, the impressioning handles made by Jord Knaap can be purchased via KJS Tools at *http://www.kjstools.com*.
- The lightweight Pro-Lok handle can be found at *https://www.pro-lok.com* and various resellers.
- For files, magnification solutions, and light sources, check jeweler's supply stores like Cousins at *https://www.cousinsuk.com*.
- Manfrotto Super Clamps can be found at camera and theater stores like B&H at *https://www.bhphotovideo.com*.

For measuring tools, any sliding calipers will do. Calipers with a dialed scale (mentioned in Chapter 9) can be bought from several sources. If you want to purchase Kroeplins, check out the vintage and secondhand market as well, as prices for mint units can be rather steep (eBay is also a good option).

The best tip for getting your hands on locks and blanks is "befriend a local locksmith." Anyone running a key duplication service can also help with blanks. Keep in mind that they might use steel blanks as a default, so be precise in what you want to order.

Safe Locks and Accessories

Ready to start manipulating safe locks? Try these sources:

- MBA USA (*https://mbausa.com*) has locksmith-restricted items, but if you're just purchasing locks and accessories, it'll sell to you. Look for safe lock sales in October, when most retailers celebrate "Locktoberfest." Often bulk buys are an affordable option. MBA also sells lock mounts (search *lock stand*). Be willing to pay a little extra for the models with the threaded inserts; they will survive many a lock swap-out and tightening.

- eBay, both in the US and several European countries, sells plenty of appropriate safe locks. Sourcing closer to home might save you some shipping costs and delays, however.
- Wendt, a large reseller out of Germany, sells safe locks and sometimes cutaway safe locks: *https://www.zieh-fix.com/en*.
- Amazon has plenty of retailers with locks for sale, but their premiums are often steep.
- Large security hardware wholesalers, such as IML Security Supply (*https://www.IMLSS.com*), IDN (*https://www.idn-inc.com*), and Lockmasters (*https://www.lockmasters.com*), have numerous supplies but often require you to jump through some hoops to establish an account in order to purchase from them.

Lever Locks

Lever locks can be hard to find outside of the UK. One option is to search for UK marketplace sites with vendors that might ship globally, such as eBay.uk, Amazon.co.uk, and Alibaba or AliExpress.

Alibaba also often has a few lever lock picks for sale, usually labeled as *locksmith tools*. However, their quality and utility is rather unpredictable, so you're often better off making your own tools to fit your specific lock.

Some lever locks are commonly sold outside the UK, such as safe deposit box locks and keyed safe locks. However, neither option is great for beginners. Safe deposit box locks tend to be small and use smaller-than-average keyways and levers. This can make learning on them difficult.

While keyed safe locks use standard-size levers, they're typically designed to be high-security locks, making them a challenge for even experienced lever lockpickers.

Lock Maintenance Tools

If your locks need a tune-up or a repinning, these vendors sell to non-professionals:

- LockPicks.com will sell pins, key blanks, and repinning tools to hobbyists: *https://www.lockpicks.com*.
- SPARROWS Lock Picks has pinning mats, plug followers, Gut Wrenches, pinning tweezers, and security pins: *https://www.sparrowslockpicks.com*.
- Houdini Lock Lube spray can be found at *http://www.houdinilocklube.com*.
- HUK's 12 in 1 Lock Disassembly Tool kit is great for taking apart Euro profile cylinders. It can be found on merchant sites such as AliExpress or Banggood from

various sellers, usually for about $25. The same kit often appears on eBay or Amazon, but at a significant markup.

Miscellaneous Items

Here are some other places to get locksport-related gear we've mentioned in the book:

- Handcuffs, handcuff keys, and shims can be found at Handcuff Warehouse: *https://www.handcuffwarehouse.com*.
- The SPARROWS Lock Picks Stretcher tool is an excellent under-door tool: *https://www.sparrowslockpicks.com/product_p/underdoor.htm*.
- Travel cases to get tools and locks safely to international competitions can be purchased from Pelican: *https://www.pelican.com*.

Other Books and Papers

While we've tried to include everything you need to know to get started in the world of locksport, covering every topic in a single book is impossible. Several other great lock-related books are available from various publishers. Here are some of our favorites:

- "Safecracking for the Computer Scientist," by Matt Blaze, a paper for the Department of Computer and Information Science, University of Pennsylvania, 2004, *https://www.mattblaze.org/papers/safelocks.pdf*
- *Impressioning* by Oliver Diederichsen (self-published, 2007)
- File Identification Chart by KMS Tools and Equipment, 2012, *https://kmstoolscom.files.wordpress.com/2023/01/84d85-kms_file-id-chart.pdf*
- *Keys to the Kingdom: Impressioning, Privilege Escalation, Bumping, and Other Key-Based Attacks Against Physical Locks* by Deviant Ollam (Syngress, 2012)
- *Practical Lock Picking: A Physical Penetration Tester's Training Guide*, 2nd edition, by Deviant Ollam (Syngress, 2012)
- *High-Security Mechanical Locks: An Encyclopedic Reference* by Graham W. Pulford (Butterworth-Heinemann, 2007)
- *Little Black Book of Lockpicking: Lock Opening and Bypass Techniques for Security Professionals* by Alexandre "FrenchKey" Triffault (self-published, 2021)

INDEX

A

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

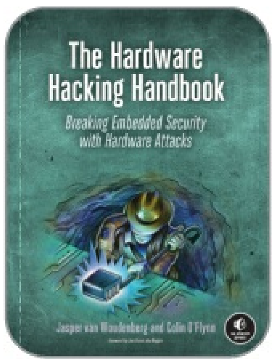
Y

Z

RESOURCES

Visit *https://nostarch.com/locksport* for errata and more information.

More no-nonsense books from **NO STARCH PRESS**



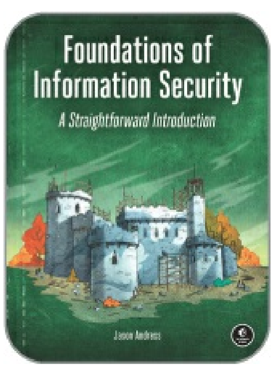
THE HARDWARE HACKING HANDBOOK

Breaking Embedded Security with Hardware Attacks

BY JASPER VAN WOUDENBERG *AND* COLIN O'FLYNN

512 PP., $49.99

ISBN 978-1-59327-874-8



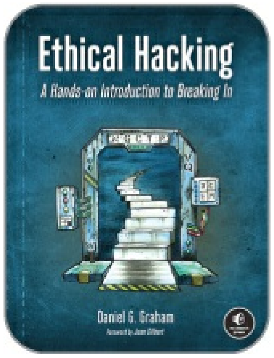
FOUNDATIONS OF INFORMATION SECURITY

A Straightforward Introduction

BY JASON ANDRESS

248 PP., $39.95

ISBN 978-1-7185-0004-4



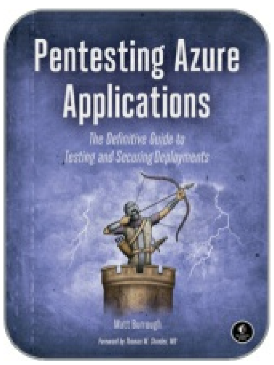
ETHICAL HACKING

A Hands-on Introduction to Breaking In

BY DANIEL G. GRAHAM

376 PP., $49.99

ISBN 978-1-7185-0187-4



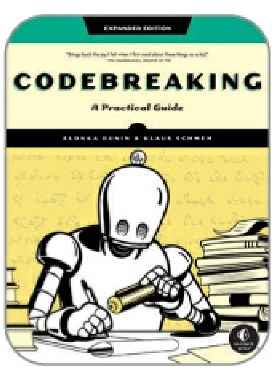
PENTESTING AZURE APPLICATIONS

The Definitive Guide to Testing and Securing Deployments

BY MATT BURROUGH

216 PP., $39.95

ISBN 978-1-59327-863-2



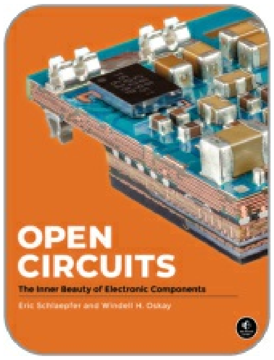
CODEBREAKING

A Practical Guide

BY ELONKA DUNIN *AND* KLAUS SCHMEH

488 PP., $29.99

ISBN 978-1-7185-0272-7



OPEN CIRCUITS

The Inner Beauty of Electronic Components

BY WINDELL OSKAY *AND* ERIC SCHLAEPFER

304 PP., $39.99

ISBN 978-1-7185-0234-5

full color