Little Black Book of Lockpicking

Lock opening and Bypass techniques for Security Professionals

Alexandre TRIFFAULT

Alexandre Triffault
Co-authors: Sylvain Hajri, Tristan Guedel
Front cover picture by: Alexandre Triffault
Back cover picture by: Frédéric Vigier
Translator: Sonia Bloch

Little Black Book of Lockpicking

Lock opening and Bypass techniques for Security Professionals

Security Consulting
Tools and Training

www.ats1851.com
alexandre@intrusion.eu

Table of contents

Warning

This manual is published as an aid to security professionals who want to improve their technical knowledge, and all such professionals who may wish to add a range of services to related activities such as locksmithing or pentesting.

It is also intended as training material that I (and anyone else) can use while giving an in-depth training about Physical Entry to security professionals.

As so-called destructive opening methods are relatively well known, they are not covered in this book. Instead, this book is focused on non-destructive opening techniques that aim at opening a lock and/or produce its key, without damaging the mechanism.

This book will therefore concentrate on the mechanisms and methods used to open each type of lock, hoping that by highlighting the required skills and technical nature of proper lock opening, this might bring real added value to professionals and craftsmen who want to improve their work and stand out from their competitors.

On a legal matter, it should be pointed out that it is perfectly legal to purchase and use lock-picking equipment in most countries, provided the equipment is only used on the performer's own locks, or with the express permission of the lock owners.

The use of these techniques in any other context would, in most cases (apart from some specific legal searches), constitute the criminal offence of breaking and entering, an aggravating circumstance of burglary.

Also, please note that it is usually perfectly legal for a Police Officer to detain you if they strongly suspect that you are about to commit a crime. Ostensibly carrying picking tools without an explainable good reason can lead to such a situation.

While it is perfectly legal to buy, own and carry a screwdriver, there are multiple situations where is not wise to do so. So it is for lock opening tools.

The authors of this book cannot in any way be held liable on this account for any improper and illegal use of the techniques described below.

That being said, I have myself never been bothered for carrying such tools, instead, it always led to interesting conversations and even sometimes led to organizing an impromptu training.

Foreword by Alexandre Triffault

It is my pleasure to share some bits of my experience and knowledge in this book, to bring Pentesters, Locksmiths and Law Enforcement Agencies officers, a concentrate of lock opening techniques that have proven their efficiency to perform their jobs.

My approach to learning lockpicking and its associated techniques has the following two objectives:

1. The art of circumventing locks arises first and foremost from a desire to discover the shortcomings of our physical security systems, in order to improve them and protect ourselves from the flaws that exist.

2. Understanding the internal workings of locks and their mechanisms also provides security professionals with the opportunity to discover or rediscover techniques that are little known or unjustly considered to be too complex, but which allow them to improve their professionalism and extend their range of actions.

Apart from the business aspect, as you will discover in this book, learning Non Destructive Entry opening techniques is an exciting discipline that combines technical skill, inventiveness and patience.

This discipline teaches you, if need be, a simple precept:

When there is a problem, there is a solution.

Besides, each time you defeat a lock mechanism, you will find that you experience real pleasure when your painstaking, meticulous work triumphs over that mystery box you targeted.

This book also aims at sharing with you the necessary ethics and passion, by including the knowledge required to practice lock opening techniques, which must be complemented by regular practice on different lock models.

Alexandre TRIFFAULT / @Frenchkey_FR

Foreword by Sylvain Hajri

When people think about Computer Security, the first words coming to the mind are "web vulnerabilities", "privilege escalation", "golden ticket", "reverse engineering"… Most of these words are part of the technical language of computer security researchers, leading companies develop web pentest campaigns, internal application pentests…

Unfortunately, when people actually suffer from a security breach, the human factor and *a fortiori* the physical factor are the least protected, although they are of great importance in regards to the Information System.

The news show it too often, several companies across the world discover a malicious device, implanted in their internal network performing attacks for months. To plant it, the attacker had to physically penetrate the premises.

That is where Physical Pentesting comes into play!

In order to perform a successful Physical Intrusion, it is obviously necessary to conduct an OSINT[1] analysis, including physical reconnaissance, but beforehand it is essential to know the concepts of Non Destructive Entry and Bypass techniques.

While spending time with Alexandre, we happened to receive phone calls for help from loosely prepared Red Teamers[2], equipped with proper lockpicking and bypass gears, but unable to use them properly or even assess the intended use of some of their tools.

---

1 OSINT = Open Source INTelligence: collection and analysis of data available from public sources (online and offline).

2 Professional simulating an attack to test the security system of its client. This simulation can include electronic and physical aspects..

This is why it is my belief that this book is a "must read" for all security professionals seeking involvement in physical security missions.
When I started working as a RedTeamer, I was not well prepared and I learned on-the-job. A book such as this "Little Black Book of Lockpicking" would have taught me the necessary locksmithing concepts, both on the attack and defense point of view, and would have made me far more effective on my firsts RedTeams.

All the information included in this book will give you the theoretical concepts, leading you to the development of methodologies specific to your activities.

Being able to identify the different lock types will allow you to know beforehand that it is better to attack a wafer lock or a day-latched door seen during your reconnaissance, instead of the doors equipped with dimple locks and always closed securely.

Whether you are a newcomer willing to understand these objects, or a Pentester with a need for physical intrusion for a RedTeam, or a Security Consultant whose mission is to identify vulnerabilities to make recommendations, or a member of Law Enforcement Agencies, or a Locksmith, in all those cases, Alexandre's expertise in this book will be essential for your activity.

I wish you a good learning experience, and don't forget to have fun while discovering this wonderful world.

Sylvain HAJRI / @navlys_

Introduction to NDE lock opening

Every year, new people, interested in improving their professional skills, look for a training course to learn and master lock opening techniques.

Although this book only covers the most basic lockpicking and associated opening techniques, it will most certainly play an important role in creating or strengthening interest in this field, to ensure the continuity and transmission of knowledge associated with this specialty.

There are probably three types of professionals interested in this very specific domain of Non Destructive Entry, namely Pentesters, Locksmiths, and Law Enforcement Agencies Officers.

Pentesters and Red Teamers

While Pentesting usually doesn't involve much Physical Security assessment (even though it probably should), Red Teaming definitely requires at least one "Lockpicking specialist" to be performed efficiently. And if the term "Lockpicking" is in quotation marks, it's mainly because when a Physical Penetration occurs, it's seldom due to actual Lockpicking, but rather with Bypass, Impressioning, Key Copying and the like.

Pentesting and Red Teaming are both pretty broad fields, including mainly computer skills, but also related skills, such as Social Engineering, information gathering skills (OSINT, SINGINT, GEOINT…), and last but not least, Physical Intrusion.

Physical Intrusion can indeed be thought as the Holy Grail of Pentest/RedTeam, since it gives direct access to all target's resources, while allowing the physical installation of persistent devices on target's physical network.

Physical Intrusion also facilitates information gathering of all forms, specifically facilitating the installation of various monitoring and manipulating devices such as Audio and Video surveillance, Keyloggers, Screenloggers, or HID emulating devices.

A Pentest or a Red Team aim at simulating a real attack to identify the flaws in a system as requested by its owner, and as such, it is necessary to include the Physical aspect, not to be mistaken with the Human aspect as it is often the case when a Red Team successfully penetrates a building using Social Engineering.

In such case, we are not dealing with Physical Intrusion, but rather Psychological

Intrusion, absolutely not related to the level of security of doors, locks, keys…
It is absolutely necessary to assess the efficiency of physical security systems against a physical intrusion attempted without insider help.
This book brings you all necessary information to quickly identify a lock's type, and to efficiently evaluate its flaws.

Locksmiths

There are multiples professions going by the name of Locksmith.

In several countries, this naming officially designates ironsmiths or blacksmiths, the former mostly working with a forge, and the latter mostly working with metal sheets, tubes and rods, applying to them various techniques of drilling, milling, bending and welding, sometimes fabricating doors or fences.

The term Locksmith is often used to name the shop down the street where you can have your keys duplicated, shoes repaired, or a rubber stamp made.

We also sometimes call Locksmiths the workman that will install a new door in your premises.

Although all of them have a good reason to be called Locksmiths, none of the above have the specific task of opening doors in case of a malfunctioning mechanism or lost keys *per se*.

For those who do have that specific task, we often use the name Emergency Locksmith, which are the most suited professionals to use the techniques described in this book in their daily job.

And while most Emergency Locksmith usually prefer destructive techniques to help out their customers, this book aims at bringing the most meticulous among them to add a wide range of Non Destructive Entry techniques to their current arsenal as a professional door opener.

Contrary to common belief that damaging the existing lock is necessary to sell a new one, the use of the techniques found in this book will likely result in better service for the customer and more sales for the locksmith. The use of these techniques allows for the demonstration of professional skills and sets the foundation of a trustworthy relationship. As a result, the customer is more willing to purchase an improved security system rather than a strictly identical replacement.

In this situation, the Locksmith is no longer a necessary evil, but becomes an adviser for improving the security of the client. This leads to additional sales,

far more lucrative for the seller, and far more satisfactory for the buyer.

At a technical level now, non-destructive opening has multiple advantages for the Emergency Locksmith, namely the lower quantity of consumables, the considerable quietness in comparison to a destructive opening, and probably the most important, the lock being opened remains perfectly working after the opening.

It is therefore not necessary to struggle looking for the perfect replacement, sometimes requiring to travel back and forth to the supplier, increasing the time required to finish a specific job, without the certitude that the replacement lock will fit perfectly.

Last but not least, at a personal level, it is infinitely more rewarding, as a Locksmith, to execute an opening following the rules of art in this trade, rather than using destructive techniques that always give a degrading image of the profession.

Law Enforcement Agencies officers

Although most agents seldom need to open doors in the course of their missions, some specialized units do have to open doors regularly.

Either for a dawn raid, in which case the Non Destructive Entry techniques are focused on the approach phase, reserving the intimidating breaching for the very last door, springing a major surprise. Or for a long-term investigation, requiring discreet intelligence gathering such as drugs, human trafficking, terrorism… implying the covert opening of buildings or vehicles, along with their proper closing not to tip off the people targeted by the ongoing investigation.

Thus, raid unit agents will learn in this book the essential skills of Covert Methods of Entry, improving the discretion of their approach phase by applying the various bypass techniques as well as the basic lockpicking techniques.

On the other hand, operatives whose mission requires a discreet way-in and way-out will be able to use this book as an introduction and training material for their latest recruits, leading the way to more sophisticated tools and techniques, that are obviously not dealt with in this book in order not to leak sensitive information that could help criminals to protect themselves against.

Criminals

Speaking of criminals, it is hard to speak about door opening without raising the case of burglars and other criminals that open doors illegally here and there, to break into homes, offices, vehicles, safes and vaults.

This book is obviously not aimed at these people, in particular due to the difficulty of actually using the described techniques, needing cleverness and patience, while criminals would most certainly have chosen the legal path if they followed what the smartness dictates, such as respect and goodwill.

Besides, it is probably relevant to inform the reader that most of the techniques described in this book will leave traces in a manipulated lock.

It is then possible to detect and identify the fraudulent act of manipulation, by applying the principles of Forensic Locksmithing, to expose wrongdoers.

Woe to those who, believing they could act inconspicuously using this book's techniques, would use them to commit crimes.

They can be found and pursued.

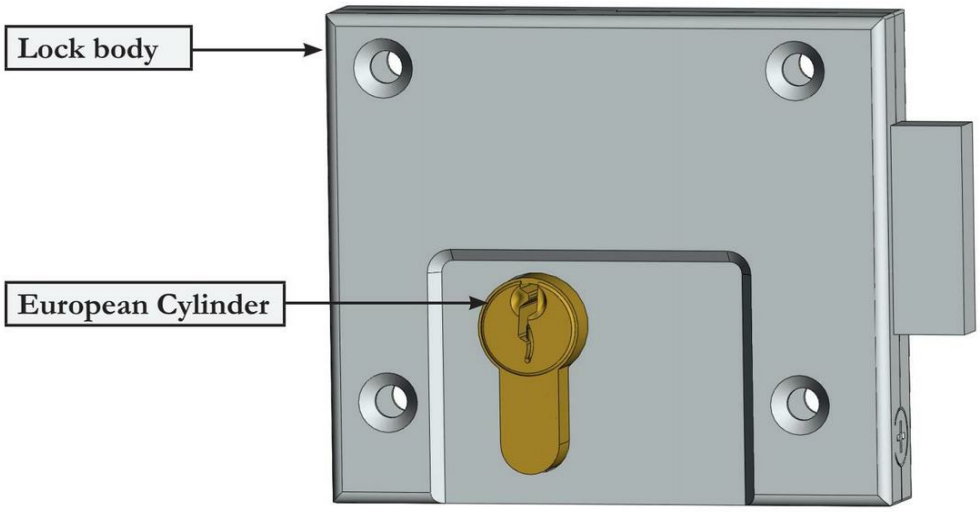
Chapter 1

How a standard lock works

The most common locks are **pin tumbler locks** known as "regular pin tumbler locks" or "flat key" locks, or more simply as "regular" locks.

They are not strictly speaking *locks*, since a lock is a term that refers to the mechanism used to secure or lock a door.

The diagram below shows a lock assembly, to which a security device is fitted, in this case a European cylinder:



In the context of non-destructive opening, the lock is usually of no direct interest to the professional.

In fact, except in special cases, if a lock is locked, the only way to operate it without causing any damage is to manipulate the cylinder.

On the other hand, with destructive opening, it is often possible and sometimes simpler to open a door by directly tackling the lock, which you only need to know how to drill in the right place to operate the mechanism without having to worry about the cylinder.

As this manual only deals with non-destructive opening methods, the security device (the assembly into which you insert a key to work its mechanism) is the part that will concern us throughout the following pages.

As regards the terminology used, you will sometimes notice that the lock is also known as a "cylinder" or a "barrel". These are ambiguous terms that have long since passed into everyday language, but are really used to designate specific parts of the lock.

On the other hand, to avoid too many repetitions of the term "lock", we will sometimes interchange the terms "cylinder" or "lock" in this book, on the understanding that the term "lock" actually refers to the "cylinder" or security device and not to the lock assembly.

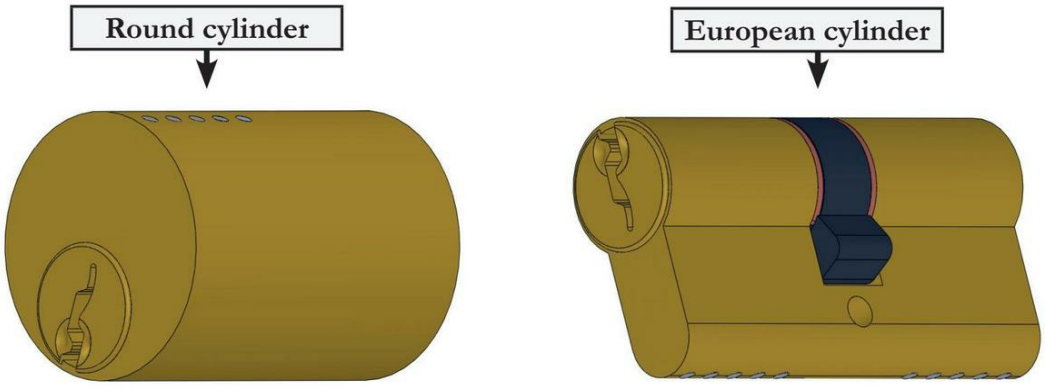
You will usually encounter two types of cylinders in your work:

1. **Round cylinders**, mounted on rim deadbolts or surface locks.

2. **European cylinders**, generally mounted with a lock assembly that can be embedded in the door (which is called a "mortise lock"), or with a lock assembly fixed to the door (which is called a "surface lock").

Round and European profile cylinders work in exactly the same way and you must have a thorough understanding of how they function, before you start to learn how to pick them.

Diagram of the two most frequently encountered cylinder shapes



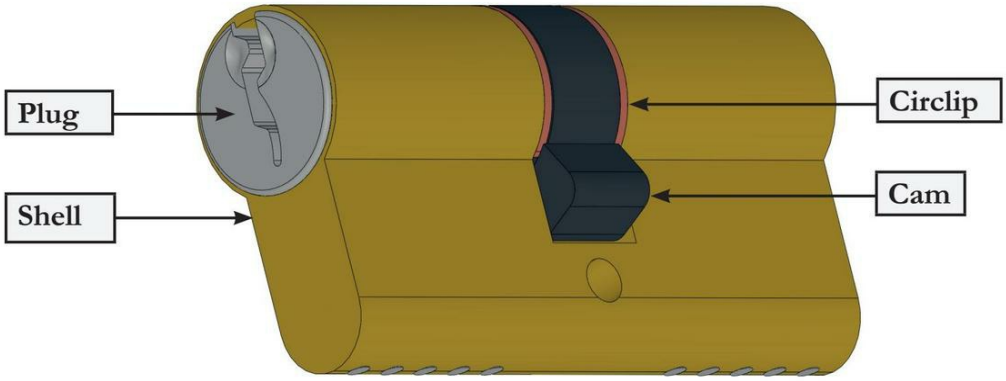
Chapter 2

Components of a cylinder

Before putting our non-destructive opening techniques into practice, let's start by determining the role and position of every component of a cylinder.

Once we have done this, we will be able to use a more technical vocabulary that will allow us to understand why and how it is possible to open a lock without its key.

External view of a cylinder



Shell:

The shell is the stationary part of the cylinder, which is directly fixed to the lock or rim deadbolt.

Plug:

The plug is the part into which you insert the key. It rotates when you open or close the lock, but theoretically cannot do so without its corresponding key.

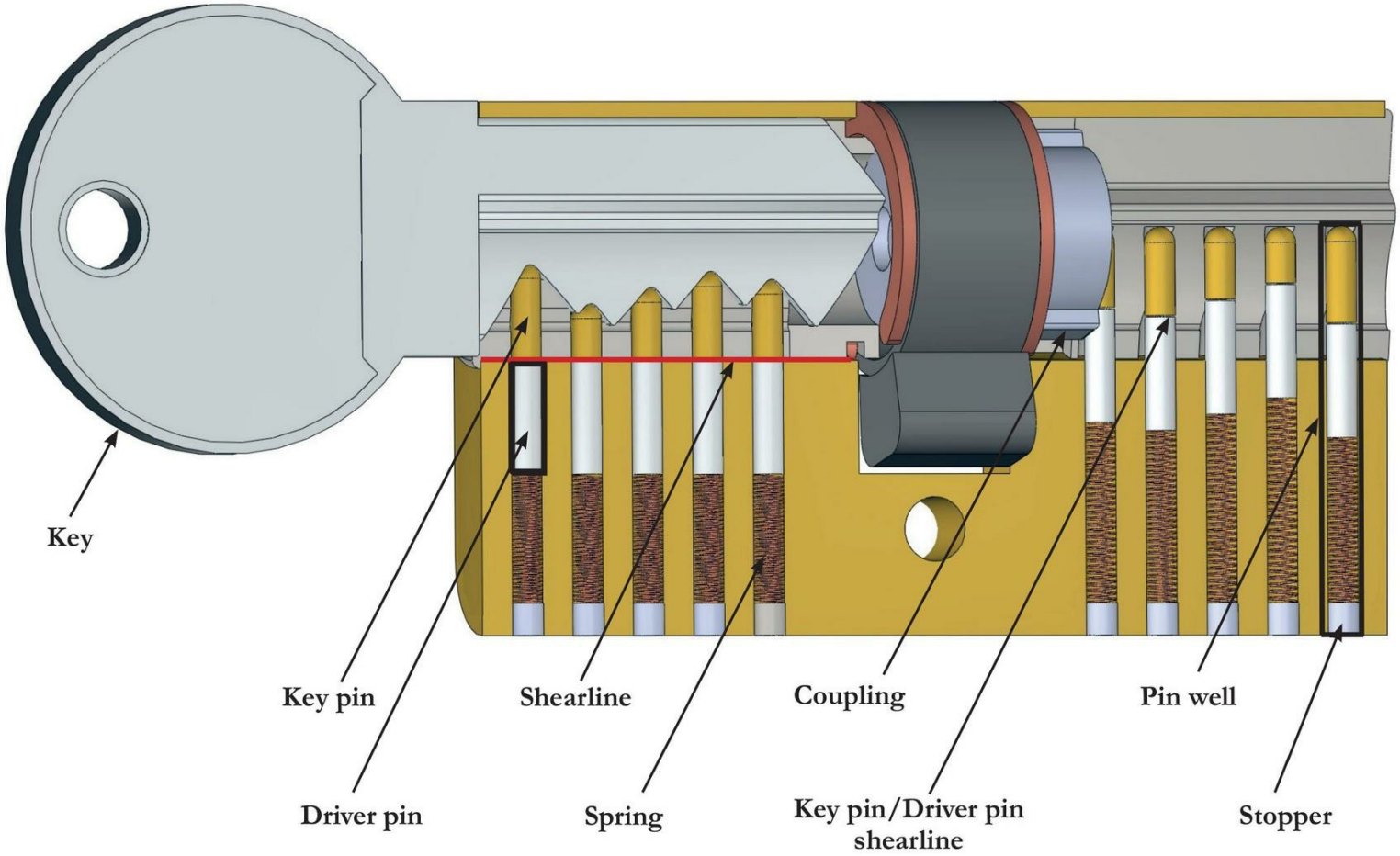
Cam:

The cam, which is often located in the middle of the cylinder, is connected with the plug and rotates with it inside the lock or rim deadbolt to operate the locking mechanism.

Circlips:

Circlips are C-shaped metal rings inserted in a groove at the rear of the plug that prevent the plugs from coming out of the lock when the key is in the plug.

Sectional view of a European cylinder



The following explanations refer to the components illustrated in the diagram on the previous page:

Pin wells:

The pin wells, or simply wells, pass through the plug and the shell. They act as receptacles and guides for the pins and springs.

The wells are theoretically aligned in a straight line.
In reality, there are always positioning variations of a few hundredths of a millimeter between the wells. We will see later that these imperfections constitute one of the fundamentals of non-destructive opening.

Driver pins:

The driver pins are in direct contact with the springs and the key pins. They pass through both the plug and the shell.

If no key is inserted, the driver pins act as an obstacle to prevent the plug from rotating and thus preventing the cylinder being opened, as shown on the right-hand side of the diagram on the previous page, they block in shear.

Conversely, when the correct key is inserted, the driver pins remain in place within the shell, on the shearline and flush with the plug, which can then rotate to open or close the mechanism, as can be seen on the left-hand side of the diagram on the previous page.

Key pins:

The bases of the key pins are in contact with the driver pins and their tips are in contact with the key. As they are of different sizes, only the correct key bitting can align their shearlines and open the lock.

The tip of the key pins can be dome-shaped, cone-shaped or in the shape of a truncated cone to minimize friction with the key when it is inserted into the plug.

Springs:

The springs are constrained in the wells to allow the pins to move up and down through the plug and the shell according to the pressure exerted on them when the key or as a pick is inserted into the cylinder.

They allow the pins to return to their original position when the key is removed from the lock.

Stoppers:

The brass or steel stoppers are fixed inserts, installed during the manufacturing process, to obstruct the pin wells after the pins and springs have been inserted.

Key-pin/driver-pin shearline:

The key-pin/driver-pin shearline is the physical separation between a key pin and its associated driver pin.

Shearline:

The shearline, which is also known as the "plug/shell shearline", refers to the physical separation between the plug and the shell.

The lock is open when the key-pin/driver-pin shearlines are aligned with the plug/shell shearline, because there is no longer any obstruction preventing the plug from rotating.

Only in this case can the plug rotate to open or close the lock, while remaining integral with the shell, thanks to the circlip that fits tightly around it to prevent it from being withdrawn.

The whole art of lockpicking therefore consists in understanding how to successfully align the key-pin/driver-pin shearlines on the plug/shell shearline to unlock the cylinder.

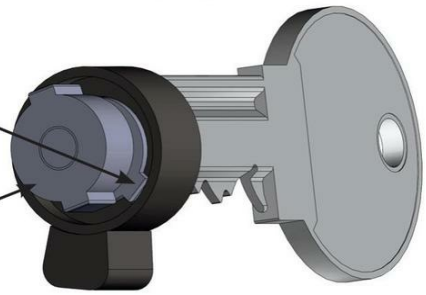
Coupling:

The coupling, which is found at the end of the key, inside the cam. It is a component that generally consists of an axis around which rotate two moving parts, the shape of which corresponds to an empty space inside the cam.

When a key is inserted, the moving part on the key side is pushed inside the cam, allowing the cam to interlock with the plug. That is why, when a key is inserted on one side of the lock, it is not normally possible, except in special cases, to insert a key on the other side to rotate the plug.

One of the moving parts on the coupling, pushed by the key, is inserted into the cam and interlocks the cam with the plug.

The other moving part seperates from the cam.

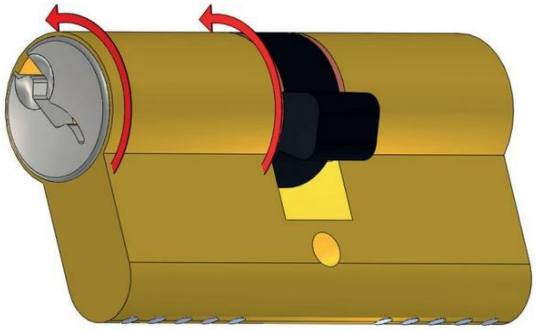


Cylinder components: essential points to bear in mind

Cylinders consist of a fixed part, called the "shell" and a moving part, called the "plug".

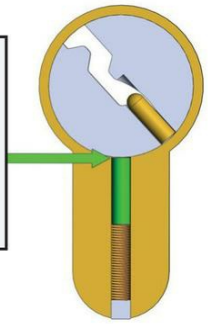
The rotation of the plug drives the cam, thus allowing the lock to open or close.

1. Example of a plug rotating in relation to the cam

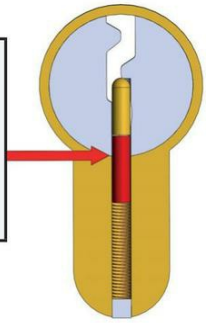


2. Front view of the action of the key on the pins

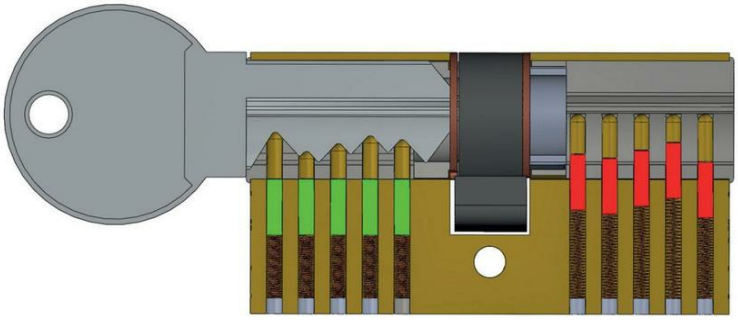
When the correct key is inserted, the key-pin/ driver-pin shearline is aligned with the plug/ shell shearline and the plug is free to rotate.



If no key is inserted, the plug cannot rotate, as its rotation is blocked by the driver pins.



3. Sectional view of the action of the key on the pins



Chapter 3

Disassembling a lock

Before describing the different non-destructive lock opening methods, let's start by gaining a good understanding of how a lock works.

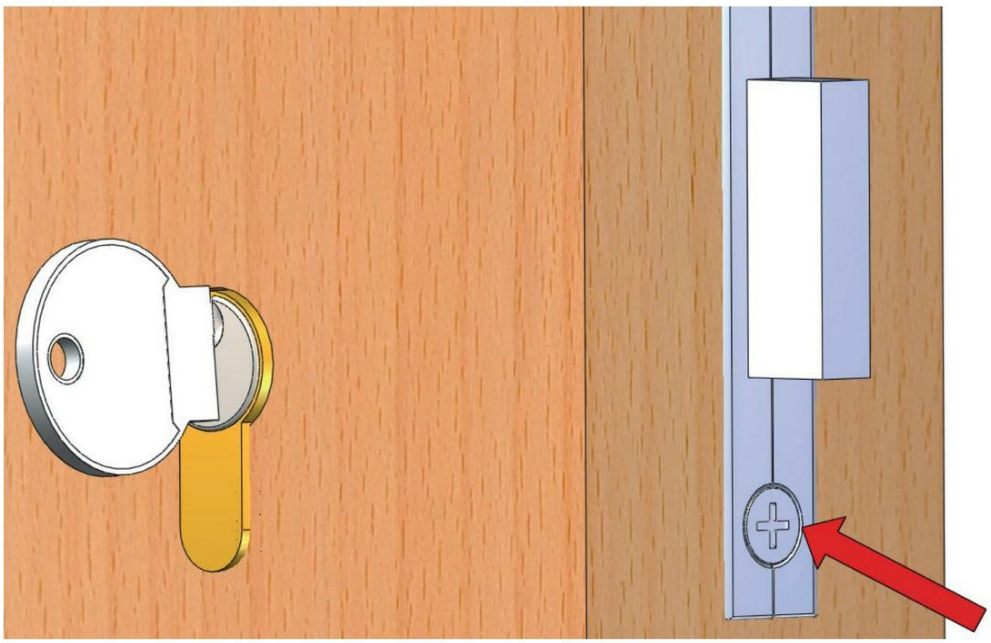
Although this is not strictly speaking related to non-destructive opening, it will, however, be useful to give you a complete understanding of locks working.

It will also be useful to learn how to make a new key from a lock, even if you do not have a working key available, or to make a practice lock that you can use to learn non-destructive opening techniques, by seeing how the key and driver pins act inside the cylinder.

1. Removing the lock from a door

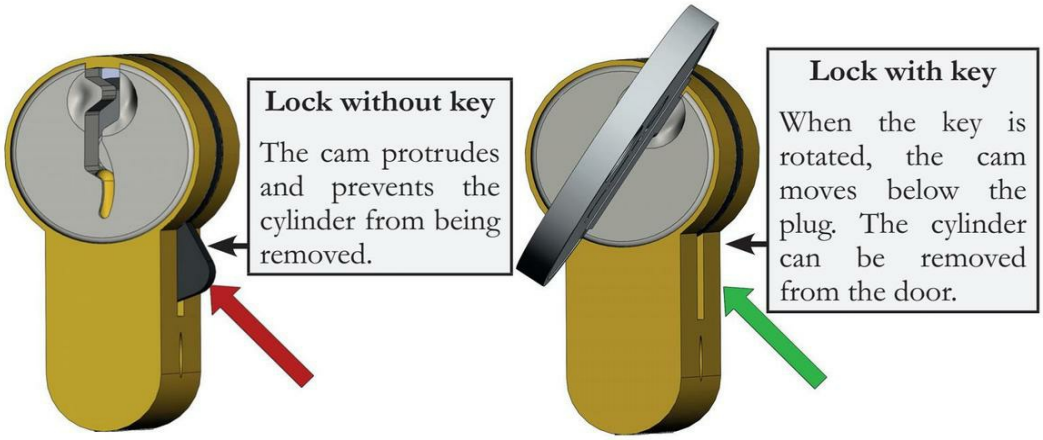
If you want to work on a European cylinder installed on a door, you must first remove the screw from the edge of the door.

In most cases, once you have removed the screw, you will still need to move the cam by turning your key to align the cam with the lock, which will then allow the cylinder to be released from its housing.



Older lock models can sometimes be removed without turning the cam, which is naturally aligned with the body of the lock. However, this security flaw tends to be rare, because a simple screwdriver is sufficient to remove a lock from an open door, even if you do not have the key.

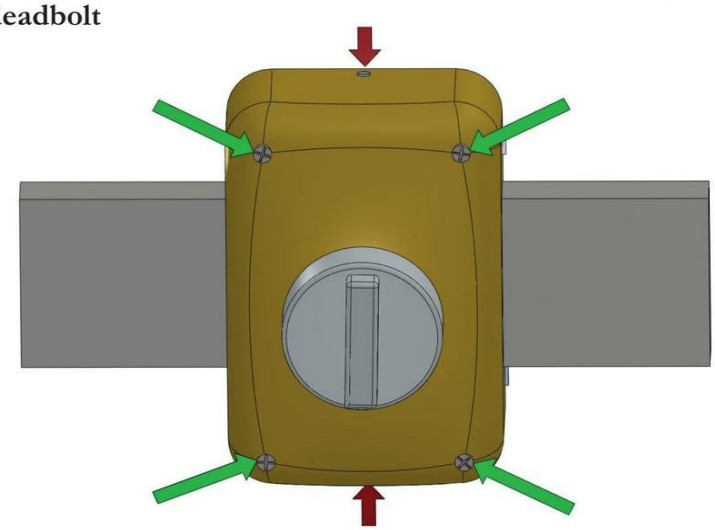
Position of the cam on a recent European cylinder



2. Removing a round cylinder mounted on a rim deadbolt

If you want to remove a round cylinder, which would normally be mounted on a rim deadbolt, it must first be separated from the door by removing the four screws located in its corners (green arrows).

Position of screws to be withdrawn for removing a round cylinder mounted on a rim deadbolt



After removing the screws from the four corners, you must remove the metal plate (known as the lock cover) that prevents access to the internal mechanism, by unscrewing the two screws located at the top and bottom of the assembly (red arrows).

You can now access the inside of the mechanism and remove the cylinder and the last screws still holding it to the lock cover.

Now that you have seen how to separate a round or European cylinder from the lock to which it was fixed, let's now see how to disassemble it.

You will get a better understanding of how it works and also learn how to repair a component, change its combination or make a new key if needed.

3. Separating the plug from the shell

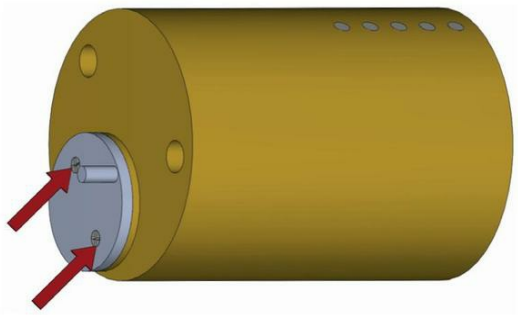
In the case of a European cylinder, the first step when disassembling it is to remove the circlip holding the plug and shell together so that you can then separate these two components. To do this, it is best to use pliers specially designed for this purpose (sold under the name of circlip pliers) or two pointed tools to remove the clip.

Circlip removed from a European cylinder

In the case of a round cylinder, the plug and shell are not held together by a circlip but by a metal disc with a protruding pin that drives the bolt.

The disc is fixed to the plug with two screws that you only have to unscrew for the plug and shell to now only be held together by the pins.

Removing the cam holding the plug and shell together on a round cylinder

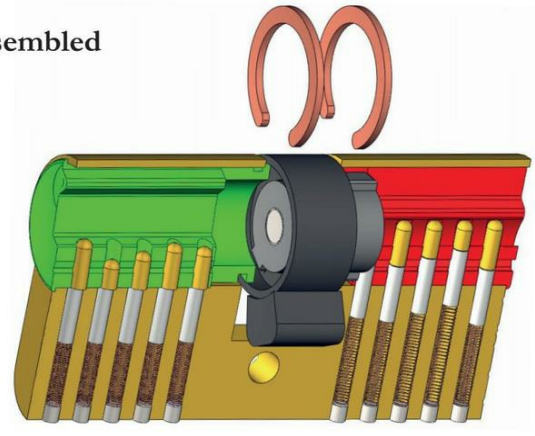


4. Releasing the plug

Once the circlip or cam has been removed from the cylinder, the plug is now only attached to the shell by the pins which, as they are not on the shearline, are blocked in shear between these two components.

The last step required before you can disassemble your lock is therefore to set the pins on the shearline, which implies that you have to either pick the lock or insert the key into it.

Sectional view of a lock being disassembled



Left-hand side: the pins are set on the shearline, the circlip has been removed and the plug can be extracted from the shell.

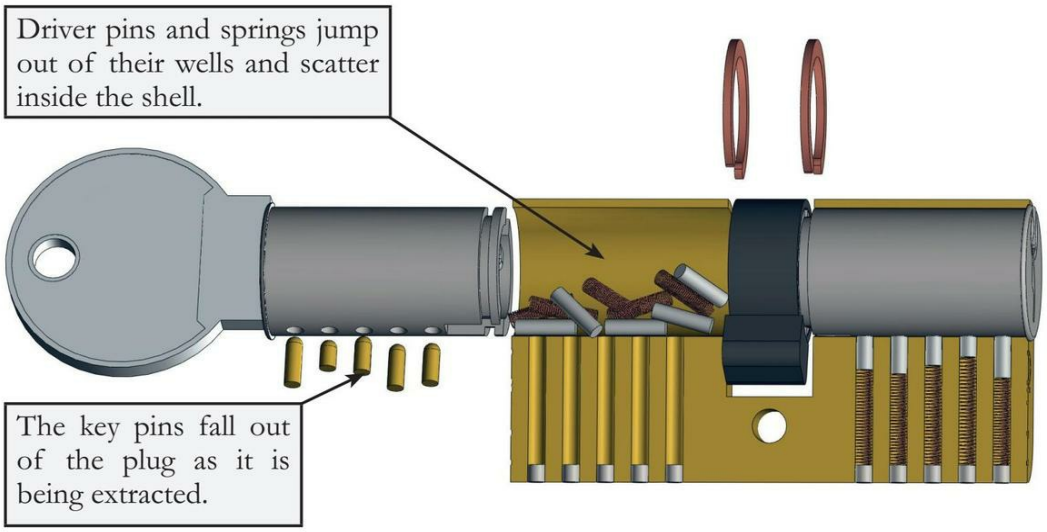
Right-hand side: as the pins are not set on the shearline, even if the circlip is removed, the plug cannot be extracted from the shell.

Once the circlip (or cam in the case of a round cylinder) has been removed, and as soon as your pins are set on the shearline by inserting the key or by picking the lock, you can then slide the plug freely out of the shell, but... **don't attempt this before reading the following paragraphs!**

As a matter of fact, if you take your plug out without doing any other preparatory work, the driver pins and springs will then be completely free and even the most skilled locksmiths are always surprised by how far a spring or pin can roll from the workbench and under the foot of an inaccessible piece of furniture.

Putting everything back into place would require tweezers and a lot of patience (and on top of that, you would probably have lost the original lock combination).

Illustration of the consequences of extracting the plug without preparation



As you can see in the sectional view above, removing the plug without adequate preparation makes the key pins come out of their wells and fall to the ground, while the driver pins and their springs, which are freed from the constraints of the plug, jump out like a jack-in-the-box and scatter inside the shell...

5. Preventing the pins from falling out

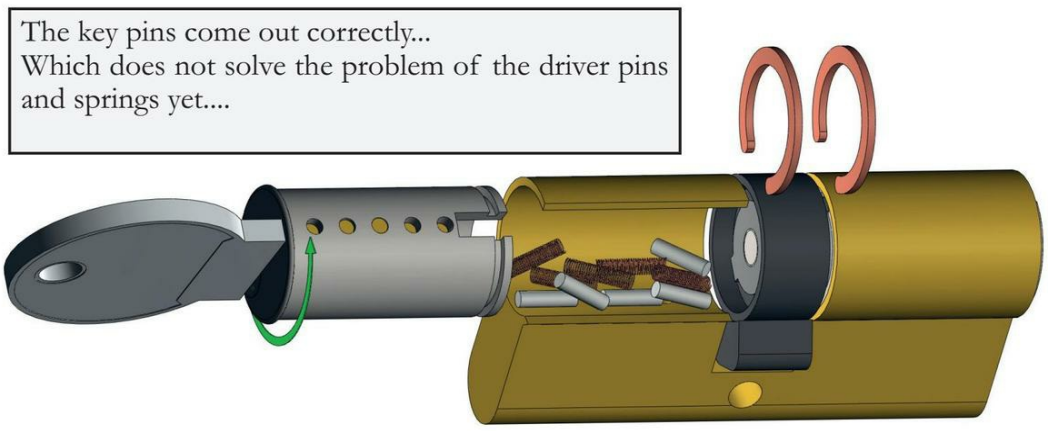
Before doing anything, always keep your pins configuration in mind:

- When the key pins are positioned above the shearline, they are in their wells, inside the plug.

- If, when you withdraw the plug, the openings of the plug pin wells are not facing upward, the key pins will obviously fall to the ground.

- Ensure that you always withdraw the plug with the well openings facing upward, regardless of the direction in which the lock is mounted, i.e. the plug must be withdrawn when the teeth of the key (assuming you have one) are turned upward.

Plug in the correct position for key pin removal



Now let's think about the driver pins, which must remain in the shell when you withdraw the plug.

Their situation is more delicate than that of the key pins because they are naturally pushed out of their housings by the springs.

To prevent them from scattering as soon as the plug is withdrawn, it is therefore essential to keep them in their housings with a pressure that is greater than the pressure of their associated springs.
In this case, a pinning shoe must be used to prevent the driver pins and their springs from jumping out of the wells.

A pinning shoe consists of a clip in the shape of a big staple, which is used to hold the driver pins in their wells.

The bottom of the clip rests on the bottom or outer sides of the plug, while the top of the clip holds the driver pins in place by obstructing the shell wells from the inside.

Although excellent clips are available in the trade, you can also easily make your own disassembly clip. For example, by bending a wiper insert blade or any other thin metal rod, preferably a flat, flexible one, into a "U" shape.

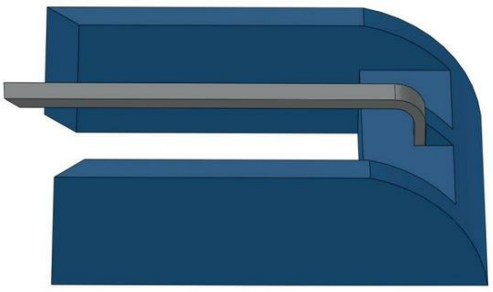
The clip should be long enough to reach the rear of the lock, so that once it is in position, it has the best possible chance of holding the driver pins in the shell.

For maximum effectiveness, it may be useful for it to be slightly shorter than the gap between the bottom of the shell and the plug cavity, which will require a little force to insert it, but will best prevent the pins from moving.

When you have done this, it is a good idea to wrap a few layers of adhesive tape around it to ensure that it is securely attached.

If you want to invest a little more time in your clip, you can also make a more functional one, using a rigid base that will hold the lock in position, while a blade attached to the structure can be inserted over the driver pins.

Factory-produced clip



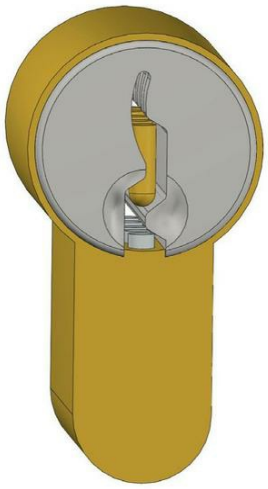
Homemade clip

As you will see, to insert your clip, you must be able to access the driver pins, which implies that you have to rotate your plug 180°.

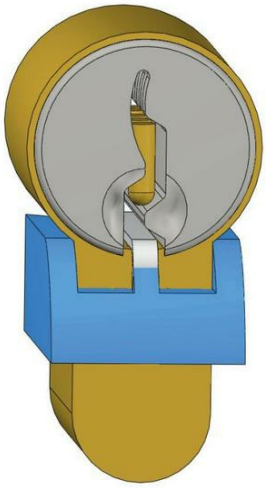
In addition, if you do not pick the lock and use a key to set the pins on the shearline, **you must file the back of the key by about 1 mm** to leave enough room to insert the blade of the clip over the driver pins.

You can now withdraw your plug without worrying that all your pins and their springs will fall out of the lock and scatter.

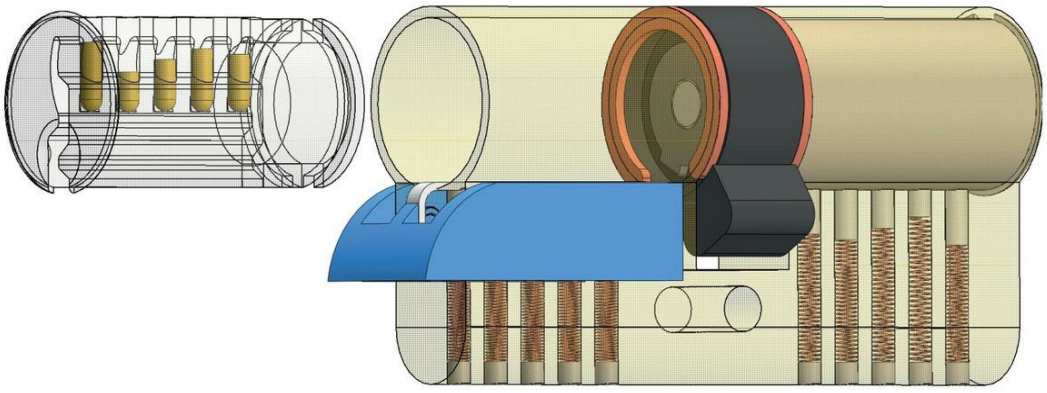
1/ Rotate the plug 180°



2/ Insert the clip



3/ Withdraw the plug



When you have withdrawn your plug, you can take the key pins out one by one and arrange them in order, so as not to mix them up.

A good tip for keeping your pins in the right order is to fold a simple sheet of paper into pleats like a fan and arrange the pins on them according to their position in the lock. Pin number 1 will be the one closest to the shoulder, and pin number 5 the one closest to the tip of the key.

You can then change the order of the pins, exchange them or remove them, which will be invaluable for practicing different combinations on the same lock. You can also make a new key if you do not have one (we will see how to do this in Chapter 5).

Sorting the pins after full disassembly

It is useful to know that during your lock guttings, you will sometimes come across locks from a masterkeyed system, which are often used in companies or public buildings. You will recognize them by the masterkey wafers separating the key pins and driver pins.

Masterkey wafers are used to increase the number of possible shearlines on the plug, offering several possible key combinations for the same lock.

This principle makes it possible, for example, to have a masterkey that opens all the locks in a building and to assign more restricted access rights to certain users by giving them a different key that can only open a few doors.

Chapter 4

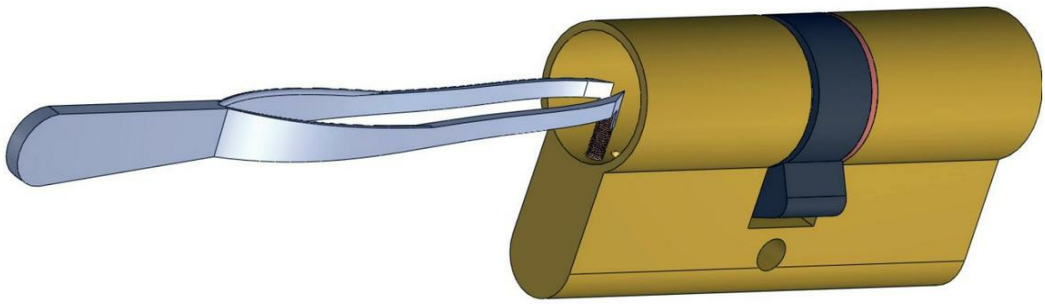
Reassembling a lock

If you have followed the advice given in the previous chapter, reassembling the lock is a simple formality and you can proceed directly to step 4 of this chapter.

On the other hand, if your driver pins and springs came out of their respective housings, here are some tips to make it easier to reassemble the lock without it being too tedious.

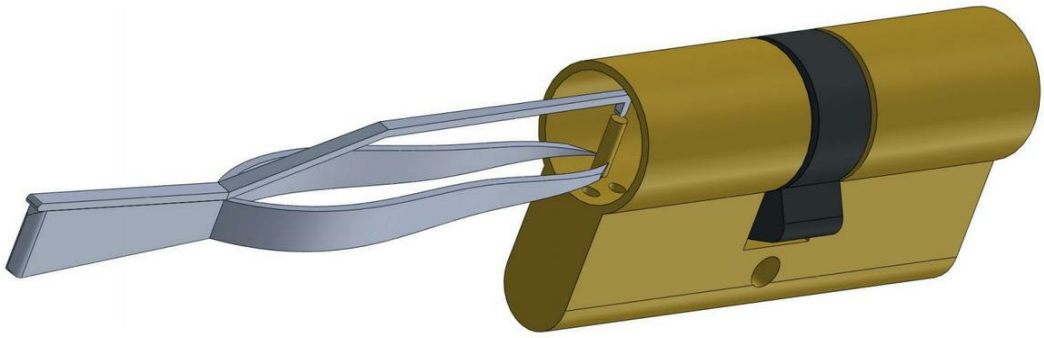
Step 1: insert the springs

Insert the springs into their housings with tweezers



Step 2: insert the driver pins

Insert the driver pins with tweezers fitted with a hook

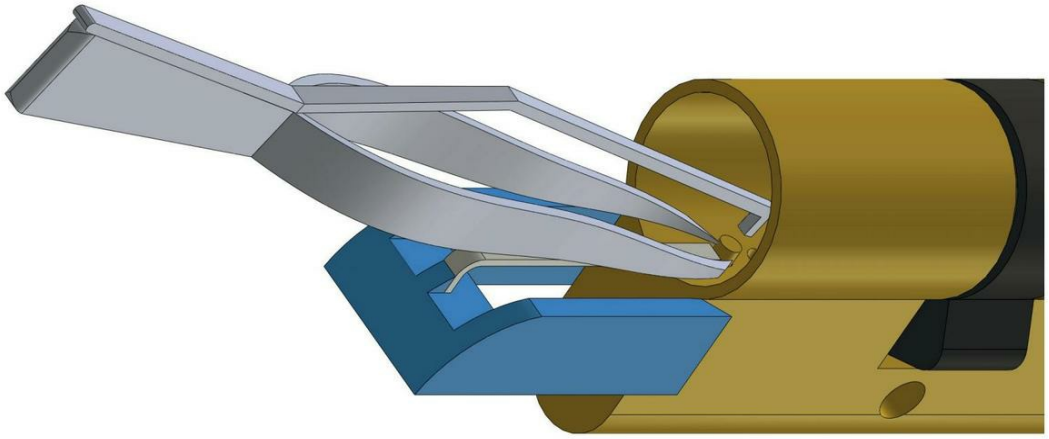


As shown in the diagram above, tweezers fitted with a hook are used to insert the driver pins.

For information: you can easily make suitable tweezers from an ordinary pair of tweezers by soldering or gluing a branch from a second pair onto them.

Step 3: block the driver pins

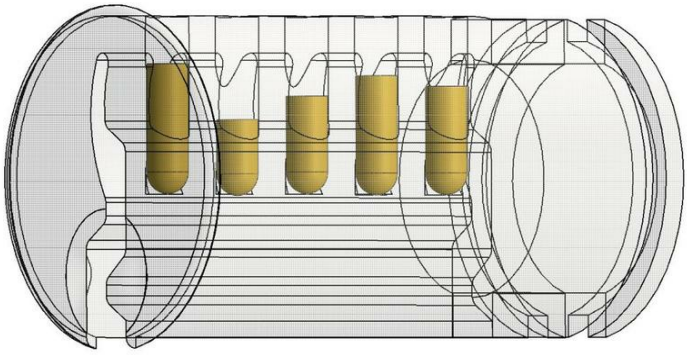
Gradually block the driver pins with a pinning shoe



As you progress, use a pinning shoe to block the driver pins and springs that you have put back in place.

Step 4: insert the key pins

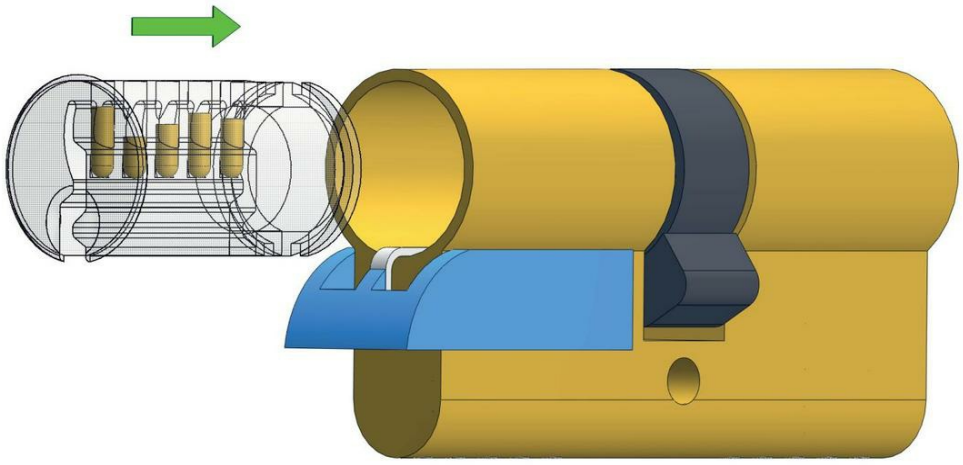
Place the key pins, tip side down in the plug



Warning: if you have a lock with a key, make sure you put the key pins back in the original order, otherwise the lock combination will change and the key will no longer open the lock.

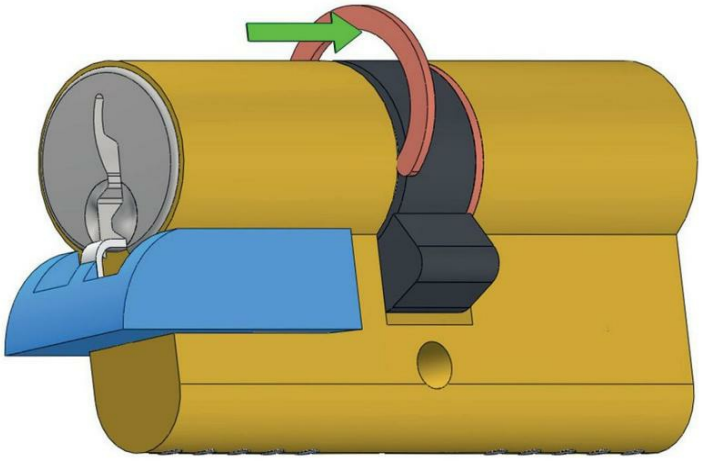
Step 5: put the plug back in place

Reinsert the plug along the axis of the pinning shoe



Step 6: tighten the circlip

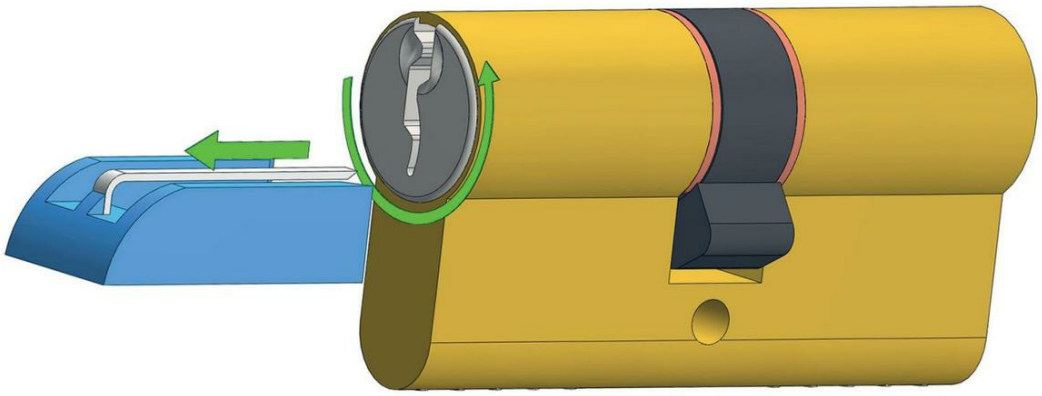
Put the circlip back in place to interlock the plug with the shell



Note: as the circlip is generally made of copper or iron, it is fairly easy to tighten it and return it to its original shape with circlip pliers or with a more standard type of pliers if you do not have a dedicated tool.

Step 7: complete the reassembly process

Remove the pinning shoe and rotate the plug 180°



If you have followed these steps correctly, your lock is ready to be reused and you will have been able, during the process, to change its combination or replace a damaged component in order to restore it to working order.

Chapter 5

Making a key from a disassembled lock

You can easily make a key from a disassembled lock, either because you don't have one, or because you want to make a duplicate of an existing key, or because you want a different key for your lock (a masterkey, for example).

To make a new key, you must first have a blank that matches the profile of your lock.

You will also need a half-round, 0 to 2 grit file, that is no more than 6 mm wide to ensure that when you are filing one pin location on the key, it does not overlap with the next pin location.

You can buy such files online or at jewelry and watch repair stores; but less often in large DIY stores where such fine grits are relatively uncommon.

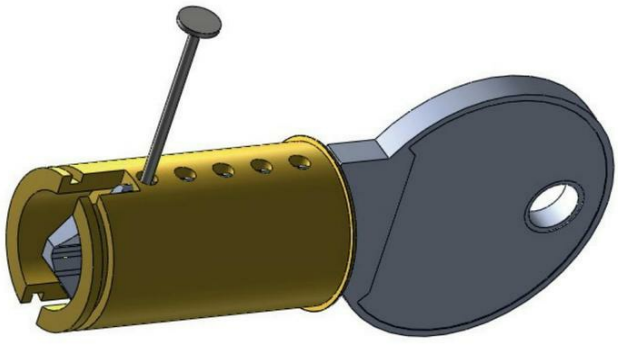
Finally, you need a nail, a pin, or any other pointed object with a smaller diameter than the pin well.

It goes without saying that a homemade key can later easily be copied on any key duplication machine if required.

Step 1: mark the location of the pins

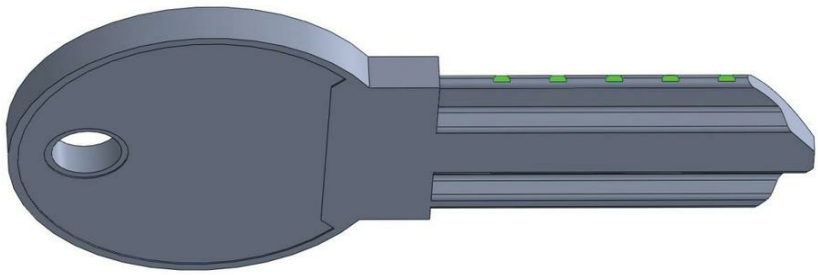
Insert the blank into the plug after emptying it of its pins and scratch the key blade to mark the pin locations, or better still, use a fine permanent marker to obtain a clean, clearly visible mark.

Insertion of a pointed object into the plug wells, scratching the blank at the pin locations



Once the key has been removed from the plug, these markings serve as a guide to determining exactly where to position your file in order to correctly form your key bitting.

Pin location marks on the blank (green markings)

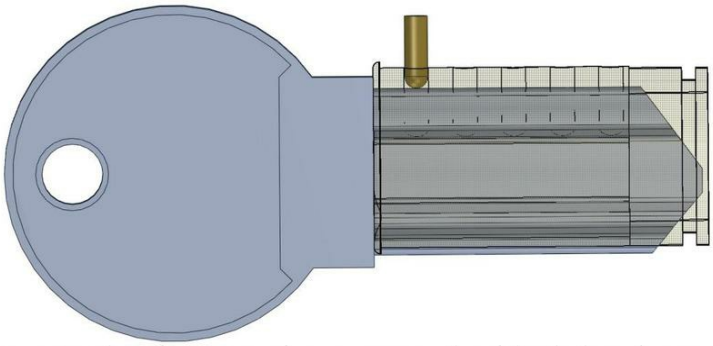


That being said, it is a good idea to lightly file each of these marks, which will serve as a guide as you make your new key.

Step 2: file the blank to align the pins at the shearline

Place the first pin in its housing and insert the blank into the plug. In the case of key bitting with large variations in height from one pin to another, **it is often easier to start with the last pin to avoid unintentionally blocking the key during the procedure.**

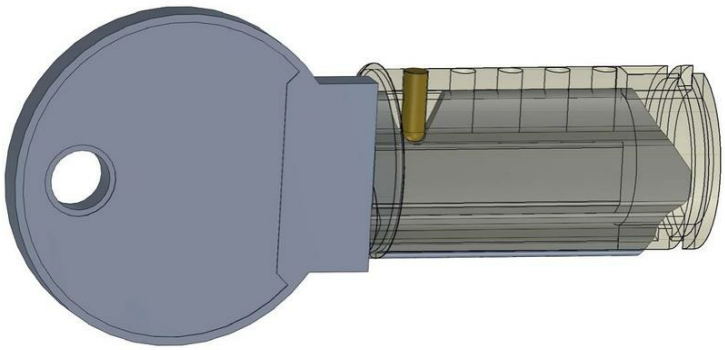
Cutaway view of the blank and first key pin in the plug



As you can see in the diagram above, once the blank has been inserted, the pin protrudes from the plug, so we now know that the correct key bitting corresponds to the alignment of the key pin/driver pin shearline with the plug diameter.

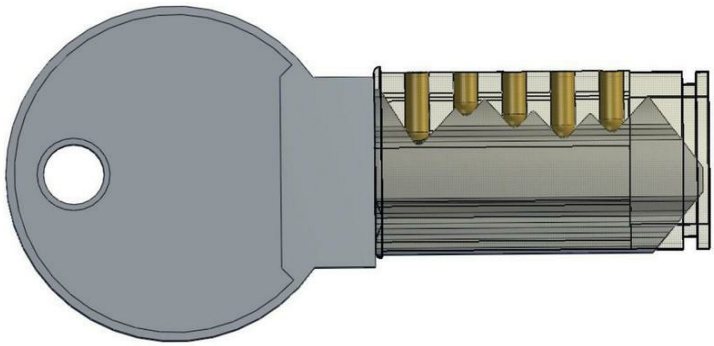
To create the key, you will have to file the blank at the pin location until the pin is flush with the plug, using the round part of the file.

Filing the blank until the pin is flush with the plug



When you have done this, do the same with the following pins until you get a working key.

Working key: all pins are flush with the plug

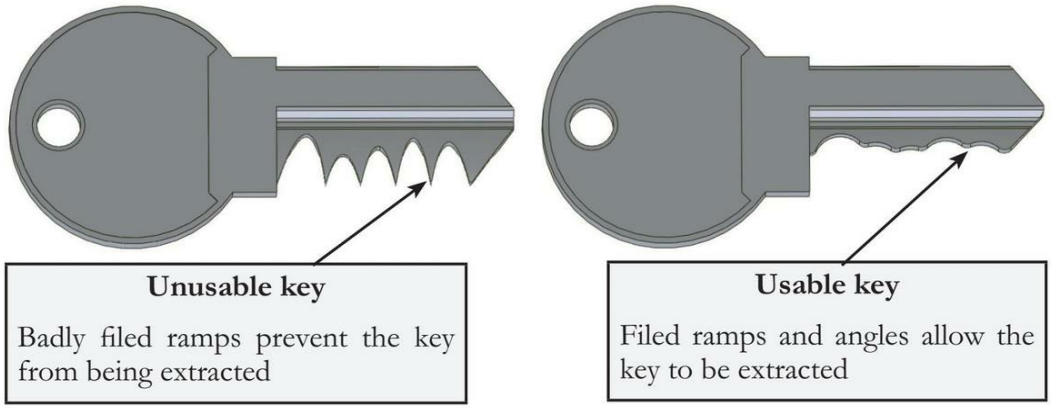


Practical advice:

1/ Make ramps for the pins

If you do not make ramps between the teeth of the key and do not carefully file off as much of the unnecessary material as possible, the pins will not be able to slide out of the cuts and you will not be able to get your key out of the lock.

You must therefore use the flat side of your file to create the smoothest possible ramps between the pin locations and flatten the sharp tips of these angles.



Unusable key

Badly filed ramps prevent the key from being extracted

Usable key

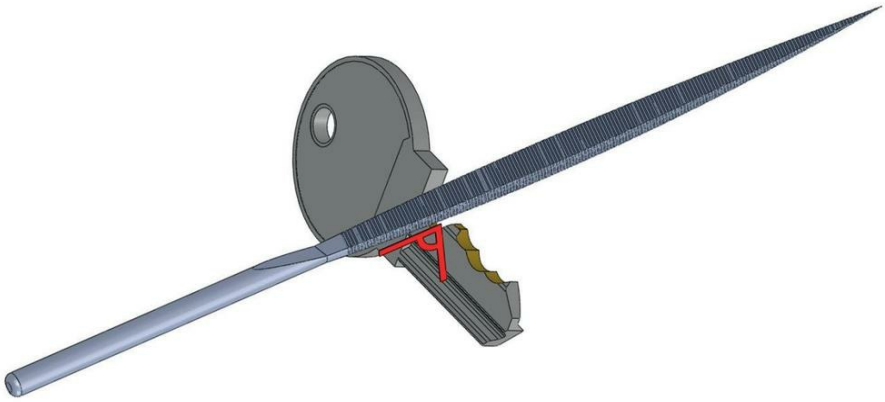
Filed ramps and angles allow the key to be extracted

2/ Place the file at 90° to the key blade

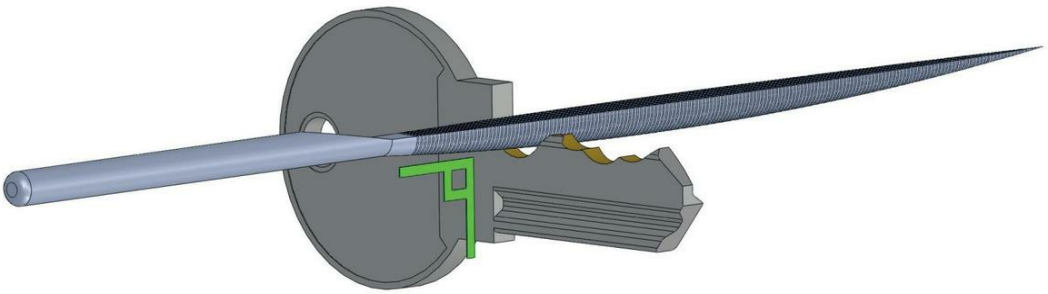
One last precaution you should take to ensure that your key works perfectly is to always place your file at right angles to your blank.

In fact, if the cuts are filed at an angle, you may get a key that will turn in one direction but not in the other since, depending on the direction of rotation of the key, the pins will touch the right or left side of the blade, thus slightly changing their combination in the lock.

File incorrectly positioned, forming an acute angle with the blank blade



File correctly positioned, at right angles to the blank blade



Chapter 6

Making a practice lock

A practice lock is a lock that is cut away at the wells so that you can clearly see the action of a key or a pick on the pins.

It is therefore an extremely useful tool, which will help you fully understand how a lock works and, above all, help associate what you see with what you feel.

This will allow you to visualize what is happening inside the lock as you pick it, including when you practice on unmodified locks that do not have these "windows".

Although excellent practice locks are commercially available, you can also make them yourselves by first emptying the lock of all its fragile parts (pins and springs) and then cutting through the shell along the well lines. Be sure to make a cut that is narrower than the width of the pins, so that you can put the pins back later without them escaping.

When making practice locks, you are advised to work with the locks clamped in a vice, using a hobbyist rotary tool with a disc less than two millimeters thick to cut through them.

Otherwise, you can start cutting through the shell with a triangular or flat file to create a guide and finish it off with a simple hacksaw.

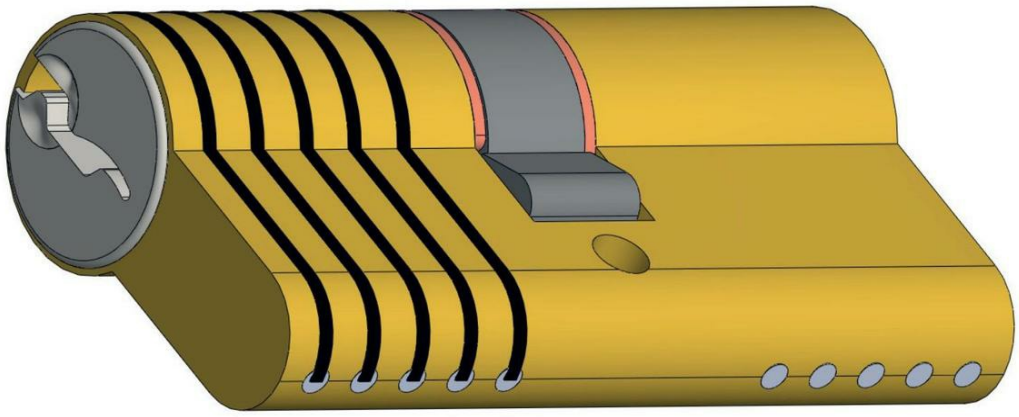
Step 1: draw cutting lines

Before drawing your cutting lines, you must first determine the exact location of the pin wells.

When a lock is made, the springs and pins are inserted through the empty wells, which are then stopped with small brass or, less frequently, steel inserts.

The pin stoppers are usually clearly visible on the bottom of the shell, so in most cases, you can simply draw a straight line from the center of the stoppers, to the top of the shell to find out exactly where to cut.

Lock marked for cutting, starting from center of the well stoppers



Note: sometimes the well stoppers are not visible, especially when the surface of the lock has been treated to make it look perfectly smooth. In this case, a few strokes of your file are often sufficient to remove the sheen and show the location of the stoppers.

Step 2: cut through the lock

Method 1: creating a repinnable practice lock

Take the lock apart and then drill your stoppers using a small drill bit. Then cut through the plug and shell separately.

It is important to cut through the plug and shell separately, because if you try to cut through them at the same time, the plug, which no longer contains any pins to stop it rotating, will move as you work and prevent you from making a clean cut.

When you have done this, reinsert your pins and springs through the empty wells and then make a new stopper that will again prevent the pins and springs from falling out.

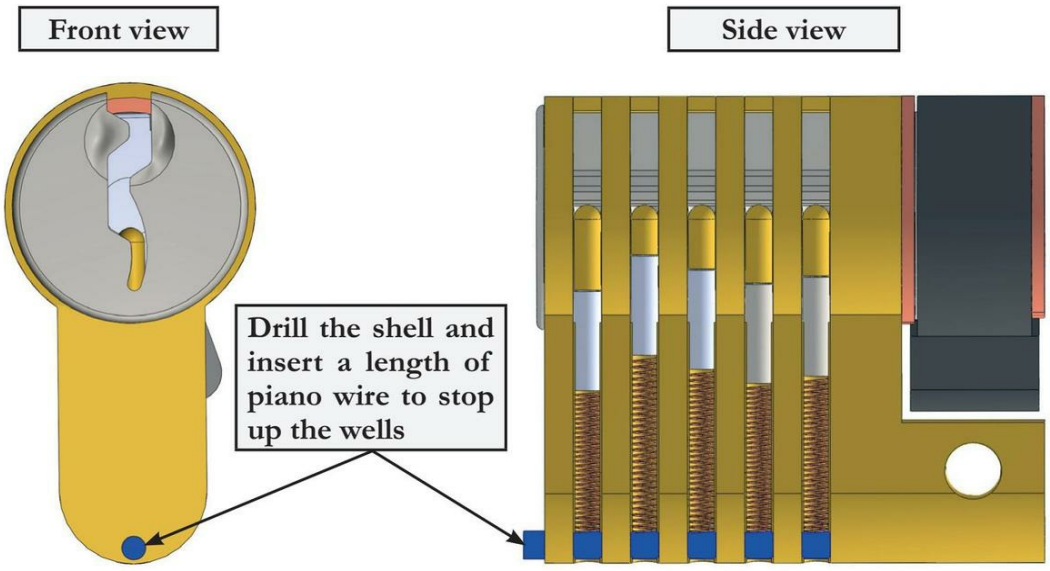
Depending on the equipment you have available, various types of replacement stoppers can be made by:

1. **Using steel ball bearings** (available in hardware stores), that you will need to force into the shell where the stoppers were located.

2. **Tapping the inside of the wells** with an M4 tap to a depth of 3 or 4 mm, and then screwing in grub screws (these screws can easily be removed and replaced later, e.g. to change the combination of the lock or the lock pins).

3. **Drilling the shell lengthwise** at the stoppers place to insert a rod of the same diameter as the drilled hole to replace the stoppers and allow you to easily change the combination.

Illustration of a practice lock made according to option no. 3



Method 2: creating a non-repinnable practice lock

This method involves completely disassembling the lock and removing the pins and springs without drilling the stoppers.

You should choose this solution if you do not have the necessary equipment to drill the wells and if you want a better looking practice lock.

On the other hand, it will take much longer to reassemble and you will be less tempted to frequently change the combination.

Variations on the two methods: simultaneously cutting through the plug and shell

To cut through the plug and the shell at the same time, you can fit them together, leaving at least one pin stack (key pin, driver pin and spring) inside the lock.

Warning: only cut through wells that no longer contain any pins or springs, then empty the well still containing springs and pins and put these back into a well that has already been cut through. You will then only cut through the uncut well.

Chapter 7

Principle of lockpicking

If there are trades that do not tolerate approximation, locksmithing is the perfect example.

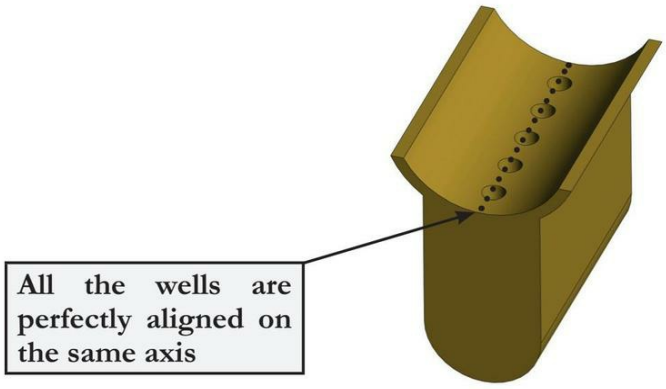
The most minute flaw, the slightest defect, can often be used to good advantage if you take the trouble to look for it and understand it. This can negate the effectiveness of certain theoretically perfect systems.

The whole essence of non-destructive opening therefore consists in discovering and exploiting these various flaws and taking advantage of them to successfully operate the locking mechanism in question without having to destroy it, and, of course, without having the key in first place.

To understand the first of these flaws, let's start by imagining a perfect straight line, along which a certain number of wells containing the pins are aligned.

This theoretical line corresponds in principle to the alignment that can be found in all pin tumbler locks, as shown in the diagram below.

Sketch of the theoretical alignment of wells in a plug



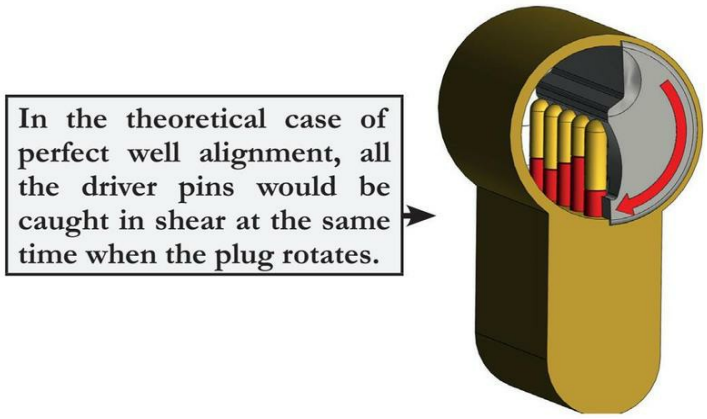
Note: luckily for the lockpicker, the perfect line only belongs to the realm of pure geometry.

In reality, even the most advanced cutting and milling machines cannot draw a perfectly straight line.

Consequently, wells can withstand misalignments and even differences in diameter generally not exceeding a few hundredths of a millimeter.
This is the basis of the whole principle of picking pin tumbler locks.

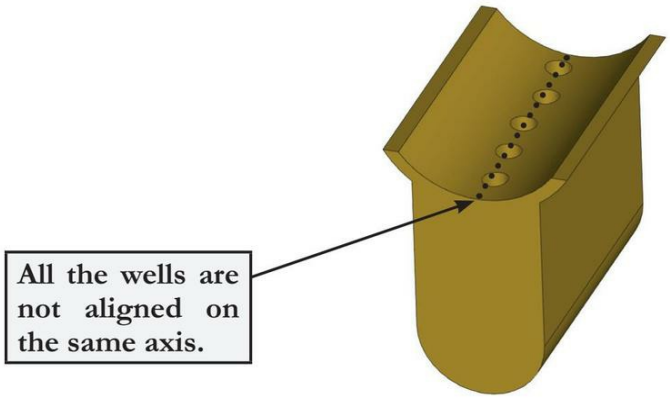
In fact, if all the pins were aligned in a perfect straight line, they would simultaneously be in contact when the plug rotates, and therefore in friction between the plug and shell. It would then be impossible to hold a pin down correctly at the shearline and the lock could not be picked.

Diagram of the theoretical "perfect" alignment of pin wells



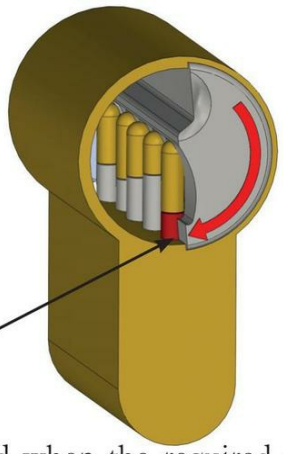
In reality, as we have explained, the line on which the pins are located is never perfect and would be more similar to the following diagram, which has been deliberately exaggerated to illustrate the problem more clearly:

Sketch of the non-alignment of wells in a shell



As wells are never perfectly aligned, if tension is applied to the plug, its rotation in the shell is blocked by one of the pins only, rather than by all of them. The blocking pin can arbitrarily be any of the pins. In the example below, due to the offset illustrated on the previous page, it is pin number 1.

Cross-section of a plug with wells not perfectly aligned



Only one driver pin comes into friction when rotational tension is applied to the plug.

As a result, while the lock is being picked and when the required tension is applied to the plug (using a dedicated tool called a tensioner), the rotation of the plug is blocked by only one pin at a time, which is in shear between the plug and the shell.

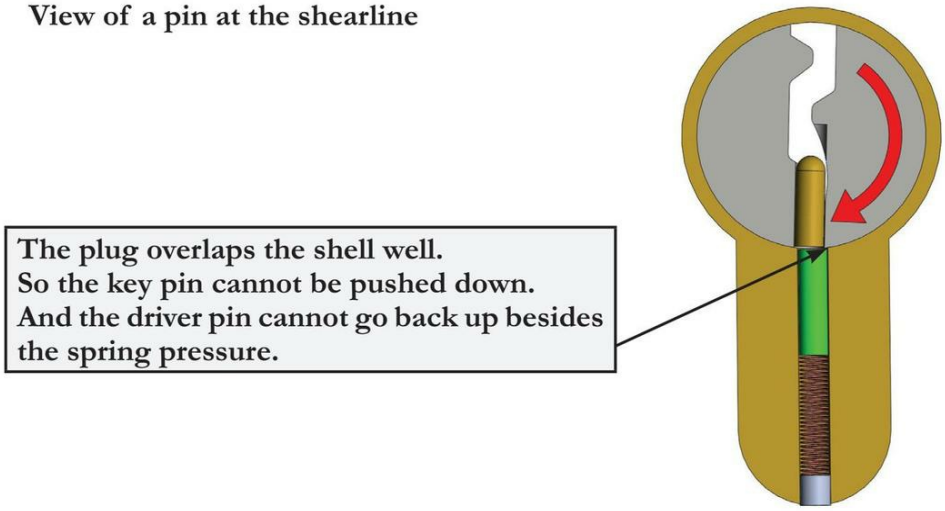
At this stage, the other pins could easily be pushed down but would immediately spring back into place as soon as they are released, as they are still free to move in their wells due to the lack of friction between the plug and the shell.

You will therefore need to acquire the necessary dexterity to be able to feel which pin is binding, so that you can lower it and bring its base down to the shearline that separates the plug and the shell.

When a binding pin reaches the shearline, you will feel a fairly distinct "click" sensation and it will be impossible to push the pin further without releasing the tension.

In fact, once the pin has been set, it remains on the shearline, because the offset that has just occurred between the wells in the plug and the wells in the shell prevents the pin from returning to its previous position.

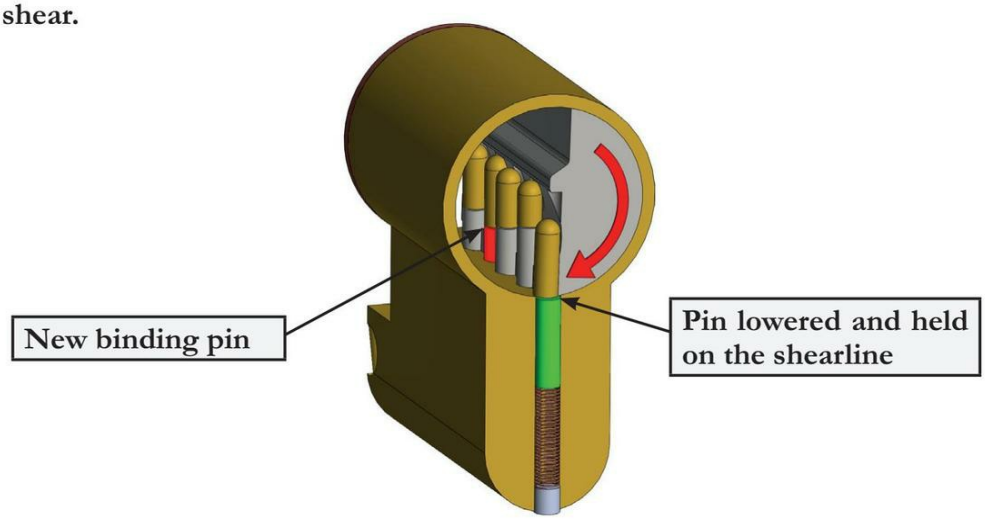
View of a pin at the shearline



Once the first binding pin has been set at the shearline, there is no longer any obstacle between the plug and the shell at this location. As this pin is no longer blocked in shear, it even has a slight play which will confirm that it is at the right depth.

As a result, the plug, driven by the tensioner, rotates a few degrees, until it comes up against the next pin in shear, keeping the pin that has just been brought below the shearline in its well.

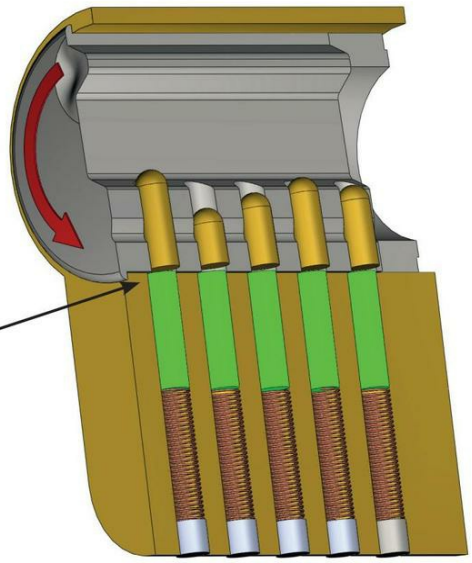
Internal view of a plug on which a rotational force is exerted. After the first binding pin has been brought down to the shearline, a new pin is caught in shear.



To open the lock, you now simply need to repeat the process of lowering the binding pins one after the other until all the pins are set at the shearline. The lock can then be opened, just as if the original key had been used.

Sectional view of a plug in which all the pins have been brought to the shearline. The plug can now be fully rotated.

The driver pins are forced to remain in the wells of the shell because they are overlapped by the rotating plug, while the key pins, situated inside the plug, rotate with it.



Of course, although the theory seems simple, you will probably need long hours of practice to understand the sensations produced by machining defects of a tenth or hundredth of a millimeter…

Moreover, in many cases, the machining defects are so subtle that several pins come into friction at the same time as a rotational force is exerted on the plug.

In this case, picking the lock can be a rather lengthy and tricky process, because you will not know which pin to set first.

If you set the wrong pin at the shearline and then press on the pin that should have been placed first, the plug will move back slightly and the pin already at the shearline will return to its original position.

Without, at this stage, going into the details of how more complex locks work[1], we can assume that, at the present time, a good lockpicker equipped with a tensioner (to exert tension on the plug) and a simple set of picks (to push the pins down) is potentially able to open almost 70% of pin tumbler locks.

With this understanding of the principles of picking pin tumbler locks presented in this chapter, we can now look at how manufacturers try to protect themselves against this security flaw.

1 This is the case with so-called "dimple" locks or certain pump locks, which also include pin systems, set in a different configuration, but susceptible to the same lock-picking principles.

Chapter 8

Security pins

Manufacturers use several methods to try to prevent, or at least delay, the use of non-destructive techniques to open their locks, in particular by trying to distort the sensations perceived when someone attempts to pick a lock, or by using complex key profiles to discourage the insertion of tools into the plug.

1. Difficulty interpreting sensations

As we have seen, the sensations transmitted by the tools to the lockpicker tell him/her whether or not a pin is set at the shearline.

To prevent their locks from being picked, manufacturers therefore use "anti-pick pins", sometimes referred to as "security pins" that give the impression that a pin is set at the shearline, while this is, in fact, not the case.

These anti-pick pins are generally used as driver pins, but some manufacturers also insert them as key pins.

Comparative view of the most common anti-pick pins

"Mushroom" pin **"Spool" pin** **"Serrated" pin**

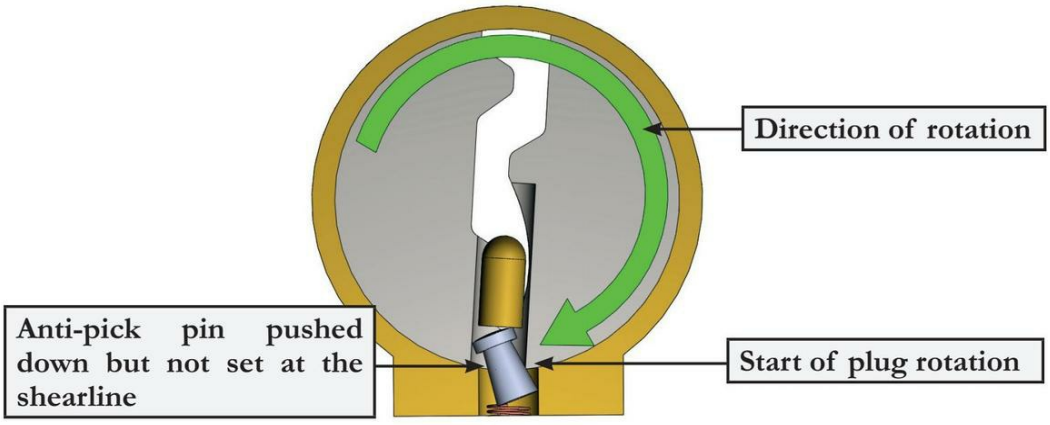
All combinations of the number of anti-pick pins in a lock are possible: it may happen that all the driver pins in a lock are anti-pick pins, of similar or different shapes, but there is usually at least one standard pin, and sometimes a lock contains only one or two anti-pick pins.

On the other hand, it can be noted that "spool" type pins are the most frequently encountered, while "serrated" and "mushroom" pins are less common.

Bear in mind that these locks are “pick-resistant”, not “pick-proof”.

This is what happens when tension is applied and an anti-pick pin is present:

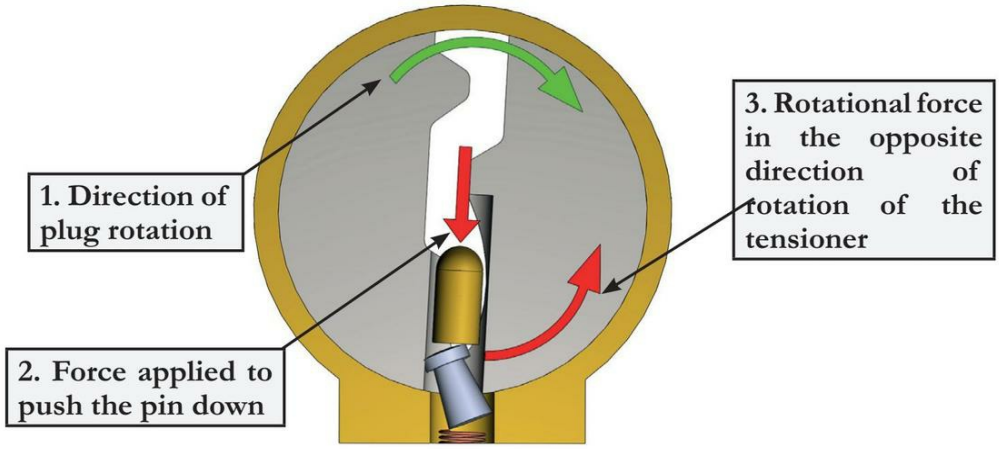
Tension applied on a plug containing a "mushroom" pin



As you can see, when one of these anti-pick pins is present and tension is applied, the plug rotates slightly due to the smaller diameter of the pin, giving the impression that it has been set at its shearline.

However, it is quite easy to spot the difference between the false impression given and the positioning of the pin on the true shearline: in fact, when an anti-pick pin is depressed but not set on the shearline, as in the diagram above, you will see that if you press this pin with a hook a second time, the plug tends to counter-rotate since the play provided by the anti-pick groove has been reduced.

How to detect an anti-pick pin



Circumventing anti-pick pins

The method of circumventing anti-pick pins is very simple in theory, but you will need some practice to master it.

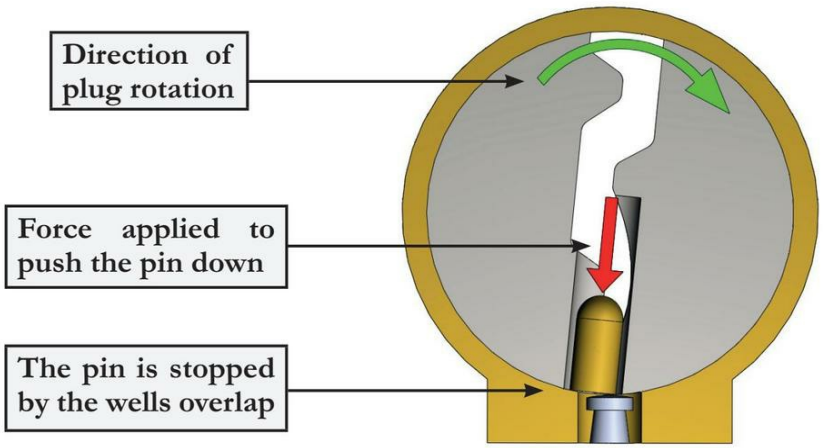
It involves applying an extremely low tension to the tensioner (actually just enough to hold it in place), while pressing on the binding pins.

When you depress an anti-pick pin, you will first feel the plug rotate a few degrees in the tensioning direction, but you will find that as you run your tool over the pins again, the anti-pick pin can be pushed down further, which tends to rotate the plug in the opposite direction as you press that pin.

Push the pin down further, varying your tension to allow the plug to counter-rotate a little, until you hear and/or feel the slight click of the pin as it sets at the shearline, as the plug rotates a few degrees more in the tensioning direction again.

You can then be sure that this is the shearline and not an anti-picking decoy, because pressing on the pin again will no longer cause the plug to counter-rotate, as it is simply held in place by the overlapping plug and shell wells.

Mushroom pin set at the shearline and unable to be depressed further



Anti-pick pins are therefore generally fairly easy to detect and bypass, provided you pay particular attention to the amount of tension exerted on the plug via your tensioner.

If your tensioning is greater than the pressure your hook is applying to the pins, you will not feel the plug come backwards and will not be able to continue picking the lock.

In the same way as with picking a lock without anti-pick pins, if you place one of the anti-pick pins correctly but one or more of the pins already set on the shearline jump out, this means that this pin must be set before the others. Once the setting order has been determined, opening the lock should only be a formality.

This would be the case if the locks only had security pins, but there is sometimes another obstacle to be overcome: the difficulty of positioning and using tools on complex lock profiles.

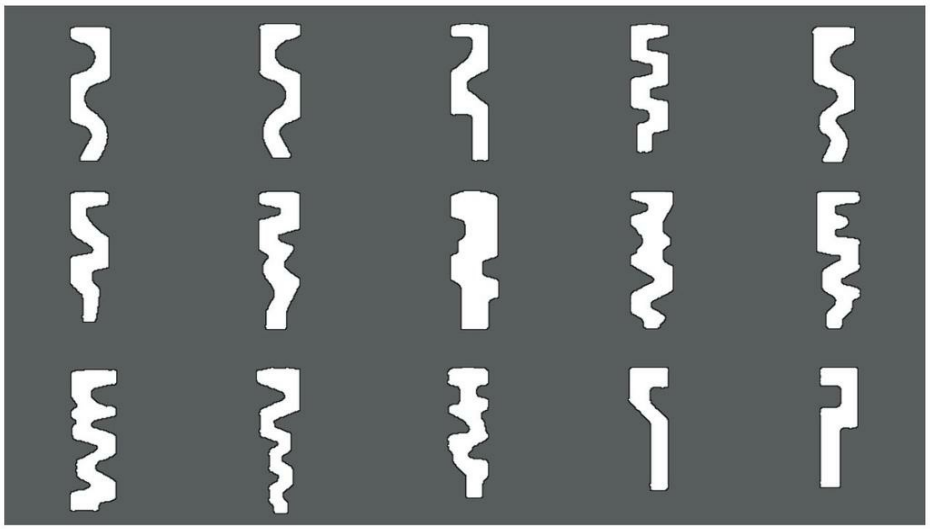
2. Difficulty of using traditional tools in some locks

In addition to anti-pick pins, manufacturers have focused on making non-destructive opening more difficult by using very specific key profiles.

These key profiles have the double advantage of ensuring that the manufacturers sell blanks that are more expensive for the user, while at the same time partially preventing the insertion of conventional lockpicking tools.

All types of profiles can be found in the field, from the simplest to the most convoluted.

Diagram representing some of the wide variety of profiles available



The most uneven profiles can usually be bypassed using hooks of different curvatures and thicknesses, as described in Chapter 11 which is dedicated to picks and how to use them.

If you have thin picks designed for the European market, you should probably be able to cope with most situations, even though you may have to adapt your tools for a very specific lock profile.

Another technique used to make opening more complex consists in adding single, double or triple action elements to the lock.

Before you see what this concept means exactly, you should already know that triple-action components are usually reserved for very high security locks. You will therefore only encounter them very rarely.

So do not be discouraged if you fail to open a lock fitted with such security features.

The best lockpickers are able to open practically all existing pin tumbler locks, but they do not have exceptional equipment.

Regular practice, combined with real motivation to understand and analyze the weaknesses of security systems, will be sufficient to ensure your progress.

Nevertheless, as with any other "sport", do not expect to achieve the same kind of performance as the best athletes on your first attempt.

You will need a lot of practice on locks of increasing difficulty before you can open those with the most complex profiles.

On the other hand, when lockpicking proves to be too random, remember that there are always alternative methods, such as the bumping, impressioning and bypassing techniques that we will describe in the following chapters and which, where appropriate, will sometimes allow you to open your lock far more efficiently and far faster than more conventional destructive methods.

Chapter 9

Advanced understanding of security locks

1. The single, double and triple action elements concept

This concept was developed by Peter Field, a highly experienced collector and world-renowned inventor in the field of locksmithing.
It will give you a good understanding of the security systems you are likely to encounter on pin tumbler cylinders.

2. Single-action components

Single-action blocking components are the protective devices installed in locks, which do not require any specific action for the lock to work.

The most commonly used single-action component is the so-called "control pin", sometimes called a profile pin.
These pins are free to move in their wells and are not under pressure from a spring.
They are located in the plug, opposite or parallel to the side of the key pins.

You only need a sufficiently deep cut on the key to allow these pins to drop to the shearline and the lock to open. On the other hand, as opposed to a conventional key pin, if the cut is deeper than it should be, the key operation remains unchanged.

Sectional view of a dimple lock with control pins

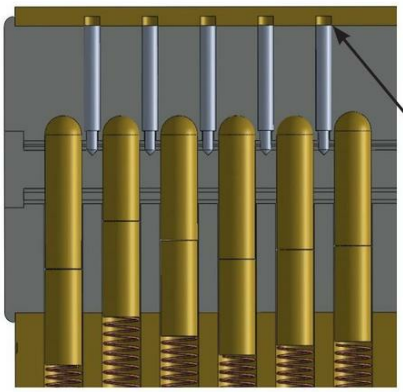
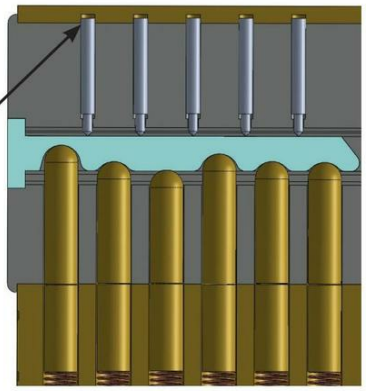


Diagram 1: No key in the plug

If no key is inserted, gravity causes the control pins to drop below their shearline. They therefore do not prevent the plug from rotating, unlike driver pins that are blocked between the plug and shell.

Diagram 2: Key with no holes

When the key has no holes for the control pins to pass through, they are pushed by the key. They then slip between the plug and shell, blocking the rotation of the lock, even if the inserted key brings the key pins to the shearline.



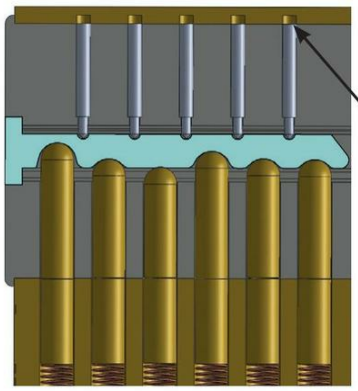
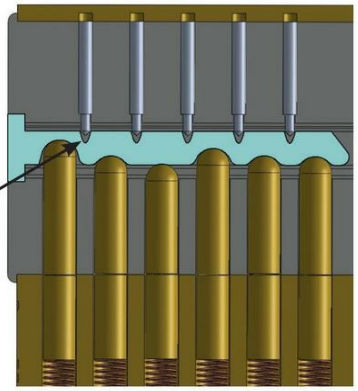


Diagram 3: Key with holes

When the key has the necessary holes, these holes allow the control pins to drop below the shearline, while the key bitting also brings the key pins to the shearline. Nothing now prevents the lock from being opened.

Diagram 4: Key with oversized holes

Even if the holes corresponding to the control pins are cut deeper than necessary, the control pins will be able to drop freely below the shearline and the lock will still open.



The single action concept also applies to the keyhole profile.

In fact, if a suitable profile can easily be inserted into the plug, a much thinner profile can similarly be inserted, without affecting its ability to open.

"Single-action" blocking components therefore present only a limited problem with respect to lockpicking or impressioning techniques, since they do not need to be placed in any specific position to allow the opening of the lock.

3. Double-action components

So-called "double-action" blocking components are components that need to be arranged precisely, i.e.:

- at the right height for pin, wafer or lever keys
- at the right depth for pump keys
- at the right angle for disc detainer keys

In fact, as we have seen in the previous chapters, it is not sufficient to push a key pin down as far as possible for the lock to open.

On the contrary, each key pin must be pushed to precisely the right height, before it can be set on the shearline.

Double-action components are therefore the most frequently encountered in locks and, as opposed to single-action components, they require a certain amount of dexterity to set them in the right position.

4. Triple-action components

Triple-action components, which you will rarely encounter, are components that need to be set in exactly at the right height and at the right angle.

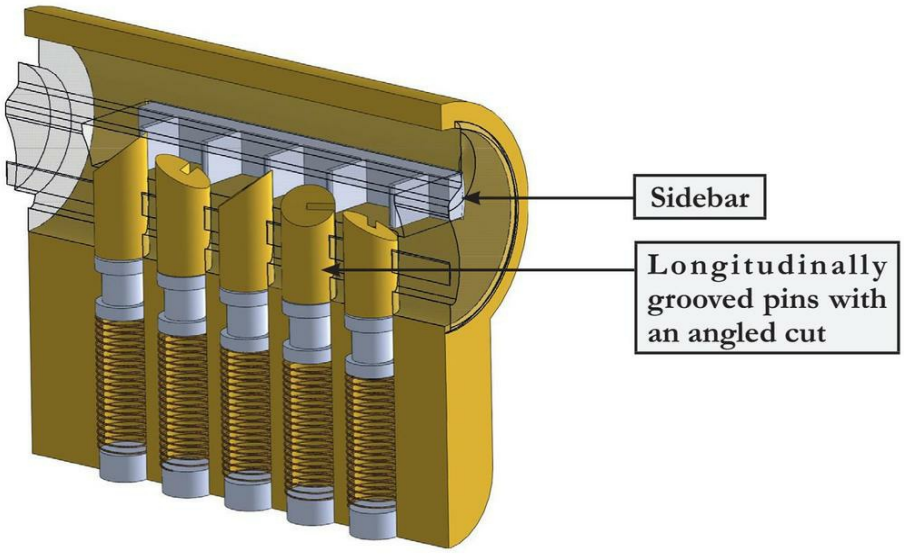
The best-known triple-action component is the key pin/driver pin assembly, which must not only be set at the right height, but also at the right angle.

Depending on the model, blocking caused by the triple-action component occurs only at a sidebar, or at the shearline and groove line drawn on the periphery of the plug.

Some lock models that do not use pins also have triple-action components, which is the case with some locks installed on safes.

Triple-action components are, of course, the most difficult to get into position, because they require a perfect understanding of how they work and excellent dexterity to put them in place according to their three blocking actions.

Sectional view of a lock with triple-action key pins

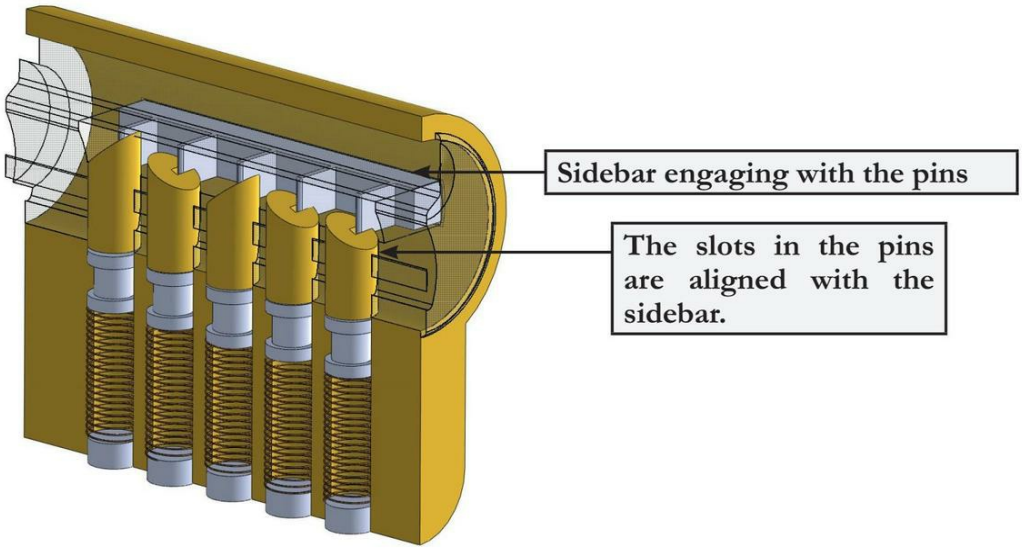


As can be seen in the diagram above, even if the pins are correctly aligned on the shearline, i.e. at the right height (double-action principle), the plug cannot be rotated because the sidebar, which has been pushed back by the body of the pins, is blocked between the plug and the shell.

For the lock to open, it is essential that the pins are at the right height AND at the right angle so that the sidebar fits into the slots on the pins in the plug, allowing the lock to be unlocked.

That is why the teeth of the key are cut at specific angles, causing the pins to rotate as the key is inserted into the lock. This puts the pins in the correct position, not only at the right height, but also at the right angle, as shown in the diagram on the next page.

Sectional view of a lock in the opening position, with triple-action key pins



Chapter 10

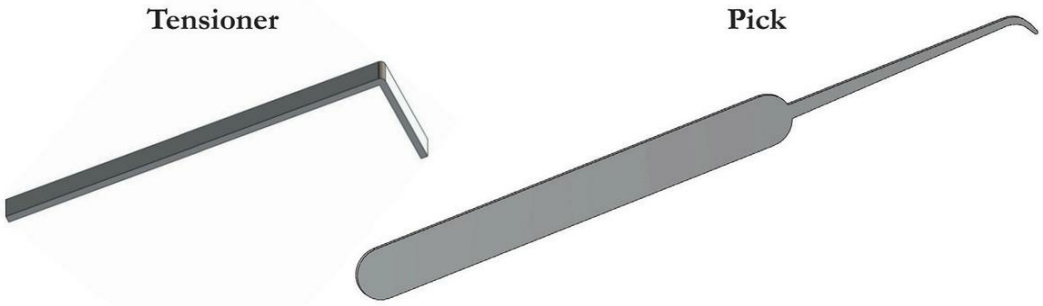
Tensioners

The many varied tools available to beginners when they buy their first lockpicking kit can be confusing.

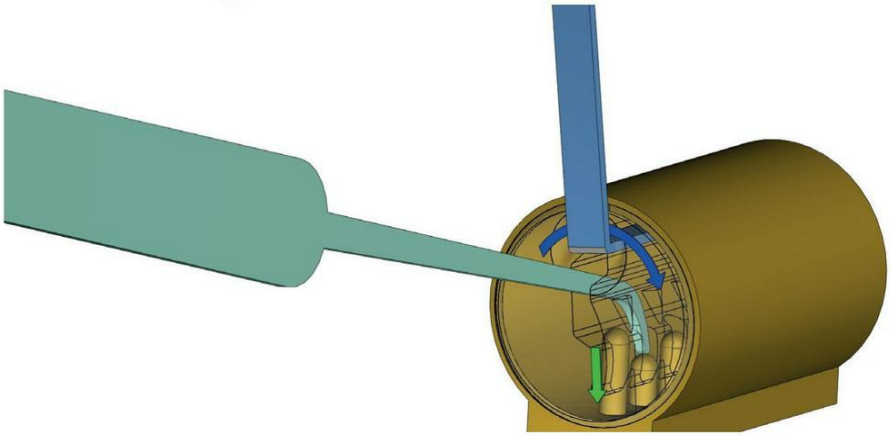
However, although this wide variety of tools seems to have no limits other than those of the (sometimes excessive) imagination of the manufacturers, only a small number of them will prove to be truly useful.

First of all, we should note that lockpicking always requires the simultaneous use of two distinct types of instruments:

1. A **tensioner**, which is used to exert a rotational force on the plug to block the pins and eventually allow the lock to open.
2. A **pick**, which is used to press the pins down into position at the shearline.



Tensioner and hook pick in action



Using tensioners

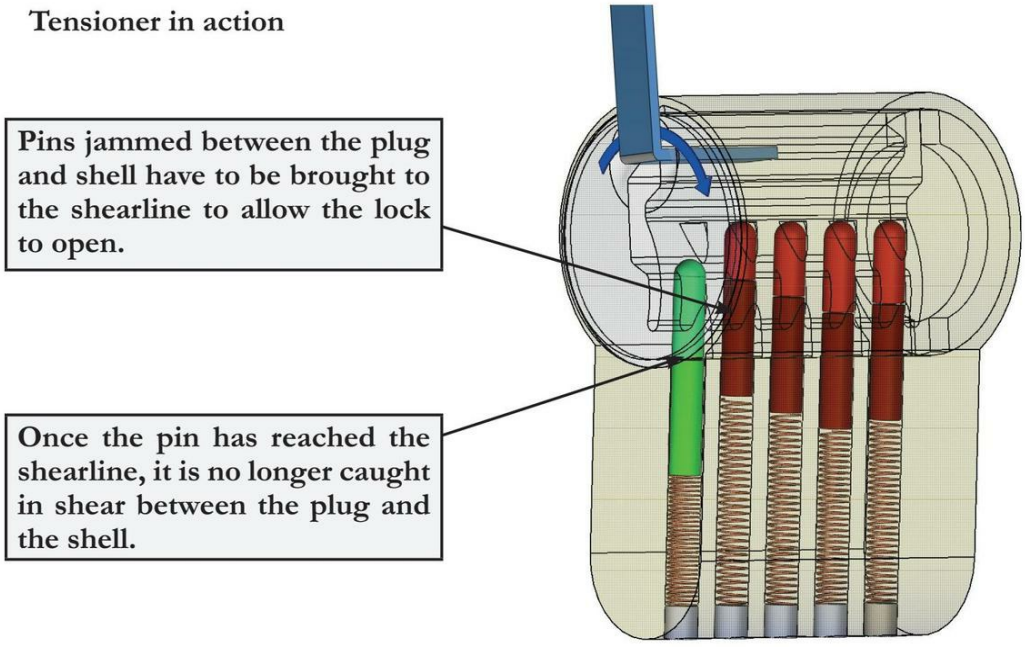
Also known as tension tools or tension wrenches, less attention is often paid to tensioners than to picks.

Consequently, the manufacturers themselves seem to think that one or two tensioner models are sufficient for all situations.

This is a mistake, because in most cases, the choice of tensioner, how it is positioned in the lock and the amount of tension applied will be as important, if not more, than the choice of pick you will use to apply pressure to the pins.

As explained earlier, the role of the tensioner is to exert a rotational force on the plug, so that the pins are caught in shear between the plug and the shell and are then gradually pushed down to the shearline where they remain in position.

Tensioner in action

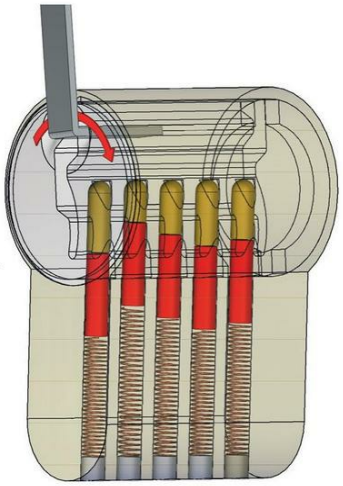


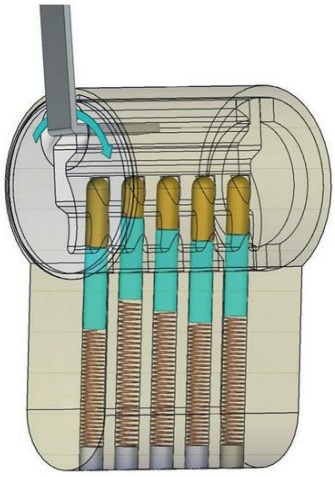
The tension you apply to the plug with the tensioner is an important element of non-destructive opening. Indeed, it is not only sufficient to apply a simple mechanical force, but this force must be carefully measured and constantly varied according to the feel of the action of your tool.

Excessive tension

Too much tension will block all the pins and you will not know which one to lower first and therefore risk breaking your picks when you try to use them.

If you are new to this field and are struggling to open your first lock, be aware that the problem is probably the result of applying too much tension to the plug.





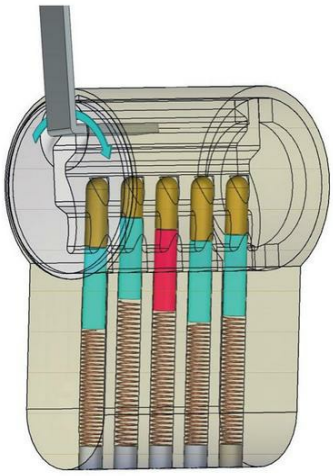
Insufficient tension

In contrast to the negative effects of too much tension, too little tension will not make the pins bind between the plug and the shell.

You will therefore not feel which binding pin to be set first and the pins you have already pushed down into position will not stay in place after reaching the shearline because the wells will not overlap sufficiently.

Correct tension

The correct tension is the force exerted on the plug as only one pin gets caught in shear between the plug and the shell, so that it starts to rub against its wells, while remaining free enough to be pushed down by the pick.



Let's metaphorically compare the tensioner with the wind filling the sails of a ship.

If the wind is too strong, it will not be possible to steer the ship. If the wind is too weak, the ship will not be able to move forward.

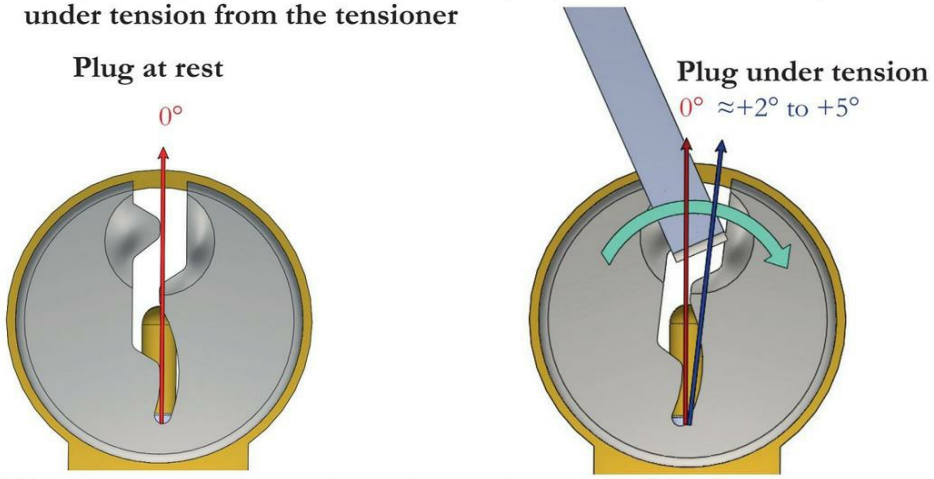
Of course, on a sailing boat, the sails can be adjusted as required.

Similarly, on a lock, you will have to constantly adjust the tension, according to the feel of the action of your pick on the pins.

When you insert a tensioner into the plug and rotate it, you will see that it rotates very slightly at an average angle of 2° to 5°.

If you increase the tension exerted on the plug you will not notice any change, as the plug can no longer move because it is blocked by the pins that prevent it from continuing to rotate.

Respective position of the axis of a plug at rest, and the angle it can assume under tension from the tensioner



The correct amount of tension to be applied is the amount required to achieve this first rotational movement and maintain the angle assigned to the plug so that it rubs lightly against the pins.

For example, if a weight is attached to the tensioner so that the tension is continuously applied without you having to hold the tensioner in your hand all the time, a weight of 10 to 20 grams is, as a general rule, more than sufficient for you to practice with. You can actually use this technique, or even a rubber band attached to the tensioner.

The tension applied must therefore be moderate, but still sufficient to bind the plug and pins.
As soon as the friction becomes too strong, you will no longer feel the lockpicking sensations and opening the lock will become very difficult.

And of course, some locks need more tension than others, but with a little experience, you will quickly be able to detect the amount of tension to apply, depending on the sensations you feel when you push the pins down with your hook.

Correct tension is usually a tension that allows you to feel the difference between the following three situations when picking a lock:

1. Pin not set and free to move in its well: as you push the pin downward, you will feel the reverse effect of the spring under the pin, and the pin will jump back up after it has been released.

2. Pin not set, in friction with the plug and needing to be pushed down into position at the shearline: you will feel that this pin can be pushed by forcing a little and you will notice a small "click", followed by an almost imperceptible rotation of the plug when the pin reaches the shearline.

3. Pin set at the shearline and can no longer be moved: you will feel a very slight play in this pin on the shearline and that it cannot be pushed any further unless you apply excessive force to your pick (or release tension).

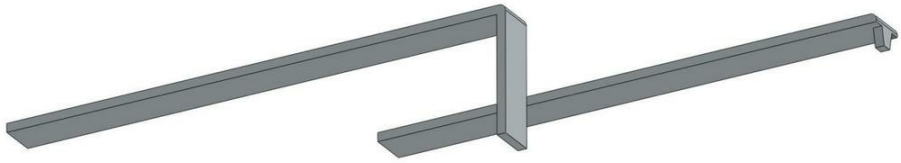
Using conventional tensioners

"Conventional" tensioners consist of a simple metal blade bent into an L-shape. The foot of the L is designed to be inserted into the lock, while pressure is exerted on the leg to tension the plug.

To leave enough room to use your pick to lower the pins, the tensioner must be positioned at the top or bottom of the keyway.

In fact, only these two positions leave enough room for the pick to subsequently push the pins against their spring.

The two types of "conventional" tensioners

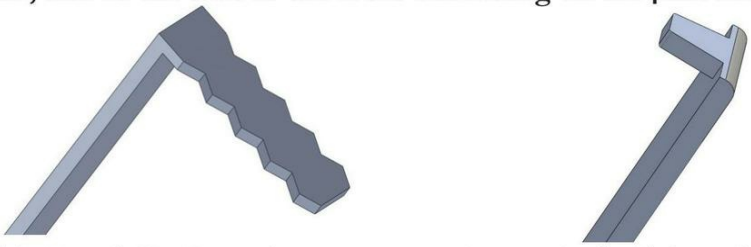


Depending on the tensioning method, i.e. insertion on the opposite side of the pins or on the pins side, the foot of the L will vary in length and width. For tensioning on the opposite side of the pins (Top in Europe, Bottom in America), a foot of about 1 cm will be perfect.

To ensure that this foot slips as little as possible in the plug, you are advised to buy, or make, a tensioner with a serrated end, to ensure a good grip inside the plug.

For tensioning on the pins side (Bottom in Europe, Top in America), as the tensioner must not come into contact with the first pin, the foot of the L must not be more than 2 to 3 mm long. It will often be narrower than the leg of the L, so that it can be correctly inserted into the keyway.

Comparative views of the foot of the L for tensioning on the opposite side of the pins, and of the foot of the L for tensioning on the pins side



Note : ToK and BoK tensioners names (respectively "Top of Keyway" and "Bottom of Keyway" tensioners) use the American standard designation, where the keyway is at the bottom and the pins are at the top. So basically, BoK means "long foot", and ToK means "short foot".

The length of the leg is not as important, but it will be best to choose relatively short tensioners (about 5 cm) to prevent you from bumping into the door frame or handle when picking a lock.

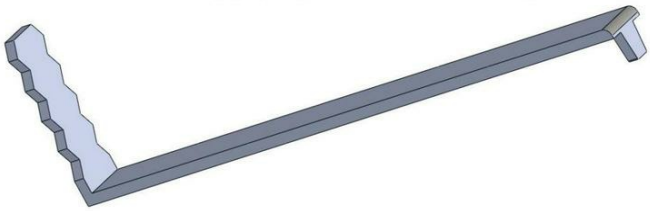
On the other hand, the tensioner, just like the pick, transmits information about the rotation of the plug and the movement of the anti-pick pins to the hand that guides it, which requires you to let the tensioner move backward in some situations.

It is therefore better to choose a tensioner made from rigid metal, which will have the advantage of best transmitting this type of sensations, even though some people also successfully use more flexible tensioners.

Although the most common tensioners are L-shaped, it is quite possible and even recommended to use Z-shaped tensioners to reduce the number of tools required.

You will therefore have at your disposal a tensioner with two ends that can be inserted into the lock to apply tension from the top or bottom of the plug, as required.

Double-ended tensioner for applying tension from top or bottom of the plug

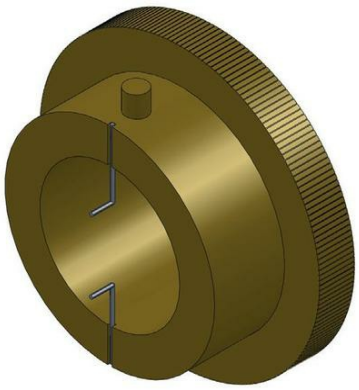


Another, less common, type of tensioner is used to tension a plug from the top and bottom at the same time.

The advantage of these tensioners is that there is less risk of slipping in the plug while you are picking the lock and they also help you find the right tension to apply. However, they do not always match the profiles encountered and are therefore relatively uncommon.

Two types of tensioners for applying tension from top and bottom of the plug

Circular tensioner



Double-tip tensioner

Positioning your tensioner in the lock

If you are using a conventional tensioner, which often appears to be the most practical solution, the question arises as to whether it is better to apply tension from the top or from the bottom of the lock.

Here are some tips on how to use each of these techniques:

a) Tensioning from the opposite side of the pins (BoK)

This is the simplest and most conventional position for the tensioner, but it is not always the most effective.

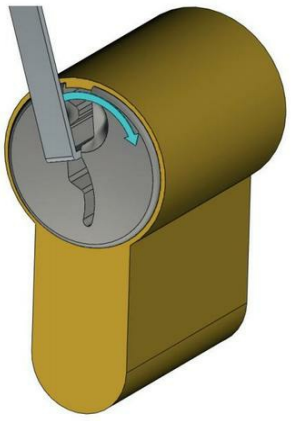
In fact, tensioning the plug this way results in using part of the keyway to insert the tensioner, thus reducing the amount of room available for the pick.

However, this technique is still useful for locks that are relatively simple to pick and is preferable when using the raking technique, as the raking action may be hindered by the presence of a tensioner aligned with the pins.

In addition, tensioning on the opposite side of the pins is sometimes very useful when trying to open the lock by raking because the tensioner can then act as a guide for the tool that rakes the pins.

The two methods of tensioning from the opposite side of the pins

Tensioning for conventional lockpicking	Tensioner in the halfway position to act as a guide during raking

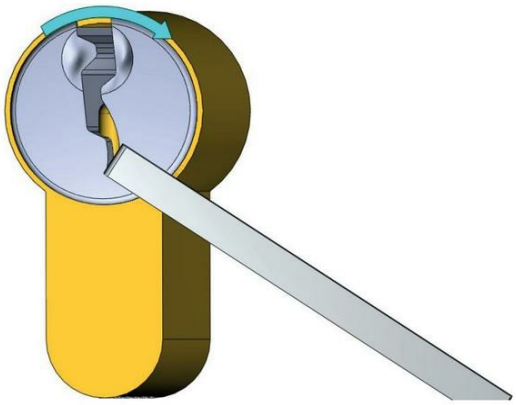


b) Tensioning from the pins side (ToK)

This is probably the most effective way to tension a lock, especially if it is too complex to be opened by simply raking the pins.

In this configuration, the tensioner is inserted just in front of the pins so that the end of the tensioner in the lock does not touch the first pin and therefore does not block it while you are picking the lock.

Inserting the tensioner from the pins side



The advantage of this technique is that it leaves the entire keyway clear for you to individually manipulate the pins.

It does, however, require a little more equipment than conventional tensioning because, depending on the depth of the first pin and the width of the keyway, you will need several different tensioners to be able to deal effectively with most situations.

However, we strongly recommend that you start practicing by tensioning from the pins side.

Most lockpickers begin their journey by using the conventional tensioning technique and then when working on more complex locks, they eventually have to apply tension from the pins side, needing to learn new sensations.

It is therefore better to make the effort to begin learning directly by tensioning from the pins side, so that you don't have to start learning all over again later on.

Which tensioning direction should you use?

The opening direction of a correctly mounted lock depends on where it is positioned on the target door. If it is on the right-hand side when you are facing the door, you will have to apply tension to the left to open it (Counter-ClockWise); conversely, if the lock is on the left-hand side of the door, you will have to apply tension to the right to open it (ClockWise).

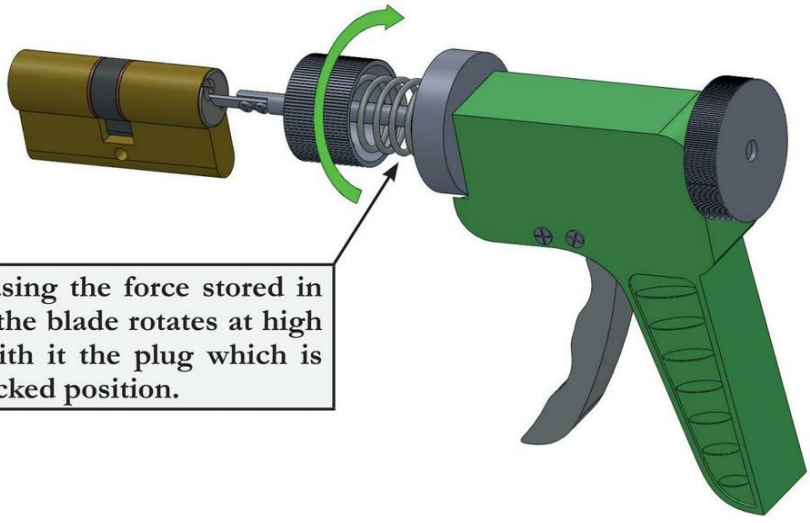
However, if you hardly feel anything when tensioning in the opening direction, do not hesitate to then try to tension it in the opposite direction. It is not uncommon to spend 15 minutes fighting with a lock by tensioning it in one direction, when it would only take a few seconds to open it by tensioning in the opposite direction.

Of course, if you need to open a door, there is no point closing it, but when the lock has been picked in either direction, you can use a *plug spinner* to rotate it in any direction. This allows you to start opening the lock to the right or to the left, regardless of the desired result, bearing in mind that the arrangement of the pins often makes the lock easier to pick in one direction rather than the other.

Using a plug spinner

The purpose of the plug spinner, which is sometimes called a flip-it, is to rotate the plug at very high speed (but by only a few degrees) so that the pins do not have time to get caught in shear between the plug and the shell when the wells are again concentric.

Illustration of how to use a plug spinner

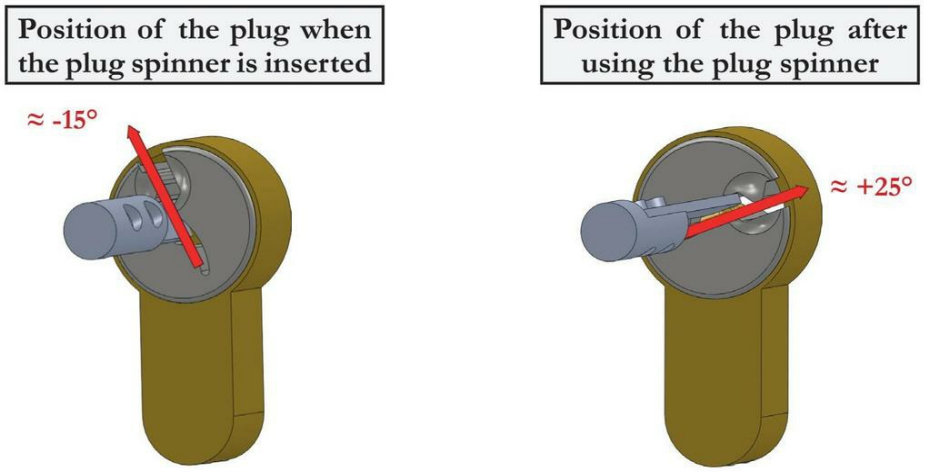


By quickly releasing the force stored in a coiled spring, the blade rotates at high speed, taking with it the plug which is already in the picked position.

In terms of tool design, it is simply a metal blade, identical to that of a tensioner, fixed inside a spring that the user winds up before using it.

Since the speed of rotation communicated to the plug by the plug spinner is higher than the speed at which the pins move back into position under the force of their springs at the moment when the wells are aligned, the pins do not have time to reposition themselves and block between the plug and the shell. You therefore do not have to pick a double-locked cylinder twice to open it, or a cylinder picked in the wrong position.

Principle of the plug spinner

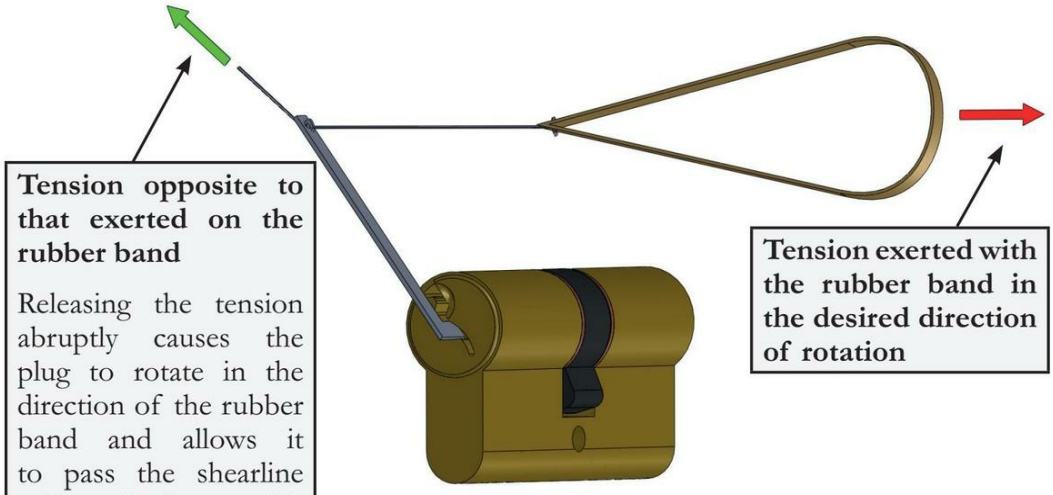


In addition to the possibility of turning a lock in the opening direction, even if the lock has been picked in the closing direction, you can use the plug spinner when the lock is locked with a double turn. This means that the lock must be turned twice to open completely.

Ideally, you should use a factory-made plug spinner with a fairly powerful spring, but you can also make one with a tensioner connected by a wire to a mousetrap mechanism, or more simply with a rubber band connected to a tensioner.

In this case, you should hold the tensioner at approximately minus 15° with one finger while applying tension to the rubber band.
Once the rubber band is taut enough, release the finger that holds the tensioner. The tensioner will then quickly rotate, causing the plug to move above the shearline without the pins having time to return to their resting position.

Using a homemade plug spinner



Tension opposite to that exerted on the rubber band

Releasing the tension abruptly causes the plug to rotate in the direction of the rubber band and allows it to pass the shearline without having to pick the lock a second time.

Tension exerted with the rubber band in the desired direction of rotation

As plug-spinners always give random results, an additional solution to using one is to stuff a plastic bag or a relatively strong fishing line into the keyway, once the lock has been picked.

These materials will reproduce the shape of the key inside the lock and hold the pins in position as the plug passes the shearline. You can extract them with a pick or an extractor tool after the required rotations have been made.

Making a conventional tensioner

Although one or more tensioners are usually provided in the majority of lockpicking kits sold on the market, they are not always quite appropriate for European locks, mainly because they are too thick.

Tensioners can, however, be made very cheaply from wiper blades.

Simply get some used wipers and take the metal blade out of the rubber.

This will give you a metal blade that is almost 50 cm long, with good rigidity and the perfect width to make tensioners.

Then, use an ordinary pair of pliers to cut off pieces 6 to 7 cm long and make a 1 cm bend at one end and you will have a conventional tensioner that is as good as those made by the best manufacturers.

Moreover, if you want to use the other side of your tensioner, bend the end back 2 or 3 mm, if necessary filing it across the width of the blade, so that the end of the tensioner corresponds to the thickness of the keyway of your target lock.

Finally, it will be worth your while to make an even better tool, by using a small triangular file, to cut serrations on the foot of your tensioner so that these rough edges catch on the inside of your keyway.

Chapter 11

Picks

Having first studied tensioners, let's now move to picks.

Lockpicking kits offered for sale often contain a large number of picks in a wide variety of shapes.

Although this assortment of picks may sometimes seem disconcerting, it is actually quite easy to find your way around them.

Let's first distinguish between dedicated raking tools and those used for single pin picking:

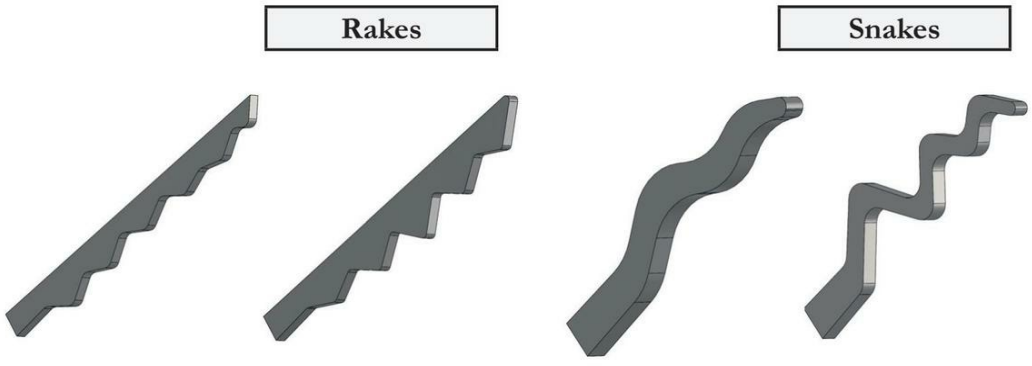
1. Raking tools

In the case of tools specifically designed for raking, which is a technique used to quickly open a lock not equipped with security pins, the tools must act simultaneously on several pins and have tips designed for this purpose.

Dedicated raking tools can be divided into two sub-categories:

1. Tools with teeth, known as "rakes"
2. Tools with curves, known as "snakes"

Rakes and snakes



2. Single-pin picking (SPP) tools

These are the best-known tools. They are designed to act on one pin at a time and enable you to feel the sensations transmitted by the pin.

Unlike raking tools, they are used to circumvent the anti-pick pins and are absolutely essential for opening any good quality lock.

They can be divided into three categories:

1. The first category applies to the curved hook picks used to feel and manipulate the pins inside the mechanism.

   They are probably the most effective and most widely used SPP tools.

   There are many varieties of these with curves that are more or less pronounced, but choosing a tool with a medium-sized curve will be sufficient for most situations.

Hook pick

2. The second category of tools is known as "half-diamond picks" that are triangular in shape and used for the same purpose as the hook picks.

Half-diamond pick

3. The third category consists of tools with a semicircular end, that are mainly intended for use on wafer locks in which the pins are replaced with small metal plates that are cheaper to produce.

Half-moon pick

The rounded shape of the end of the tool prevents it from catching in the lock when moving from one wafer to another.

Wafer locks, which are commonly found on mailboxes and other devices that generally require only a low level of protection (including most vehicles), can also be successfully opened using raking techniques or with any other hook.

All the tools described above, with the exception of the hooks (which only have variations in curvature) are available in different shapes.

You will also find that many lockpicking kits contain double-sided tools with the above-mentioned characteristics for use on locks with two rows of pins or wafers, which can be picked simultaneously... provided that the tensioner is held in the correct position. However, please note that these tools are actually of very little use.

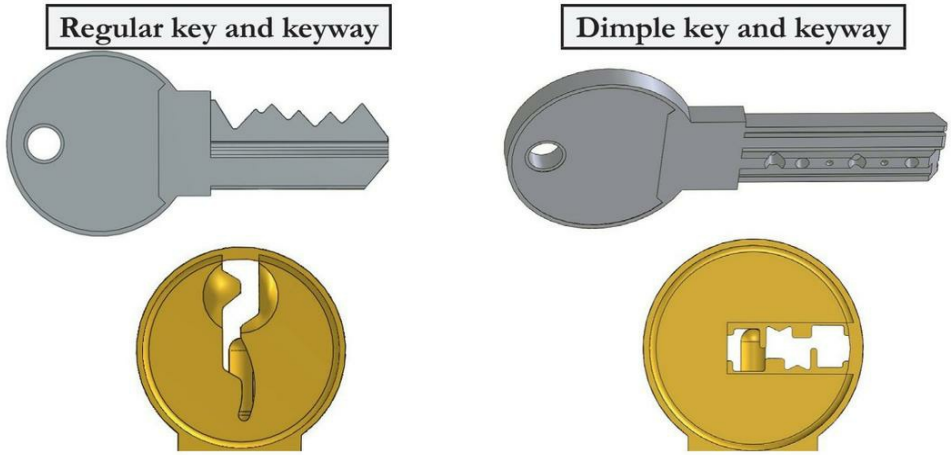
A final category of tools can be mentioned for the sake of completeness. These tools are key extractors that, strictly speaking, are not lockpicking tools, but they have the same overall shape, with a pointed tip including a barb that serves to remove a foreign body or broken key jammed in a cylinder.

Broken key extractor

3) Dimple lock tools

Dimple locks are pin tumbler locks with keys that have non-through holes, whereas standard pin tumbler locks have keys with teeth. Most often, dimple locks have a horizontal keyway.

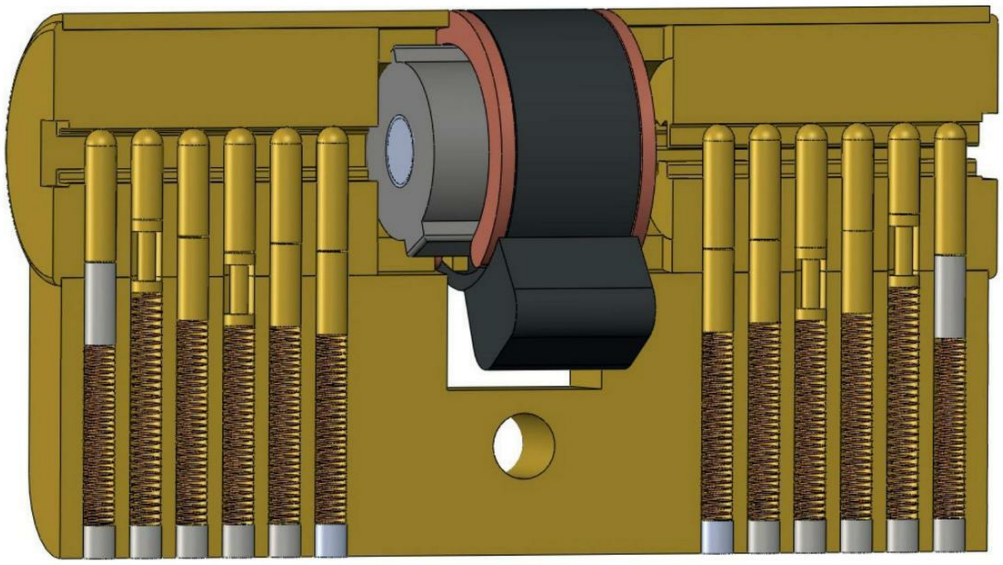
Comparison of a regular pin tumbler lock and a dimple lock



Although the shape of the keys corresponding to these locks is different from the shape of regular keys (for dimple locks they are called "dimple keys" or "reversible keys"), they work in exactly the same way.

A dimple lock is, in fact, a simple pin tumbler lock that has been slightly improved to make it less easy to insert a tool and it often has more pins than a conventional lock.

Cross-section showing how a simple dimple lock works



As you can see in the diagram above, a dimple lock works in the same way as a regular pin tumbler lock. It is susceptible to the same picking techniques and also requires the use of a hook and a tensioner.

It is important to note that locks in this category have sometimes moving components, sidebars or other features designed to hinder any attempt to pick or destroy the lock.

To illustrate this point, in the diagram above, each plug includes a steel anti-drill pin and two "spool" type anti-pick pins.

However, good quality regular pin tumbler locks also have this type of protection. So, just because you find yourself confronted with a dimple lock does not mean, in theory, that it is better protected against picking than a regular pin lock.

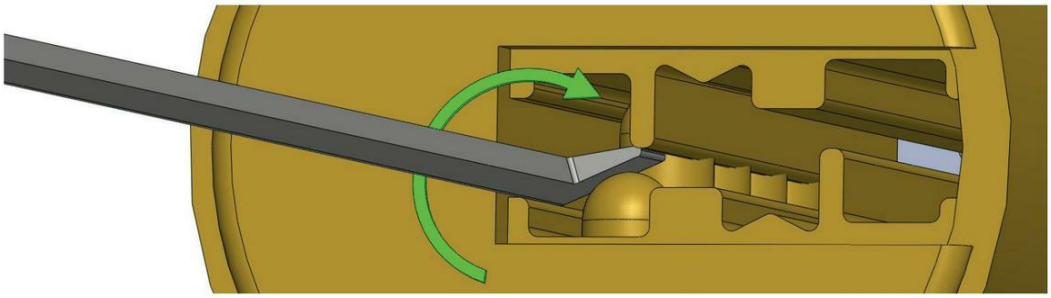
Using dimple lock tools

Although dimple lock and regular pin tumbler lock tensioners can be identical in most cases, the picks are different because the height of the opening is not sufficient to insert a conventional tool.

In the case of SPP tools, the tip of the tool is offset to the right or left to make contact with the pins that are activated when the end of the tool is rotated. The offset tip is called a "flag".

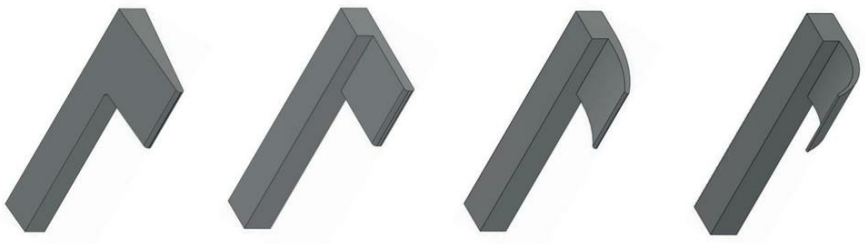
The pins are therefore not operated from top to bottom, but by a rotational movement of the tool, when its flag is positioned on the pins.

Using a dimple pick feeler



In some cases, a very slightly curved regular hook pick will be used to finish picking the dimple lock, especially on some European models where the last pin must be set using a relatively strong pressure that is easier to apply downward than with a rotational movement.

Examples of SPP tool tips for dimple locks



The leftmost tool tip is generally the most useful, but the others may be more suitable for specific profiles.

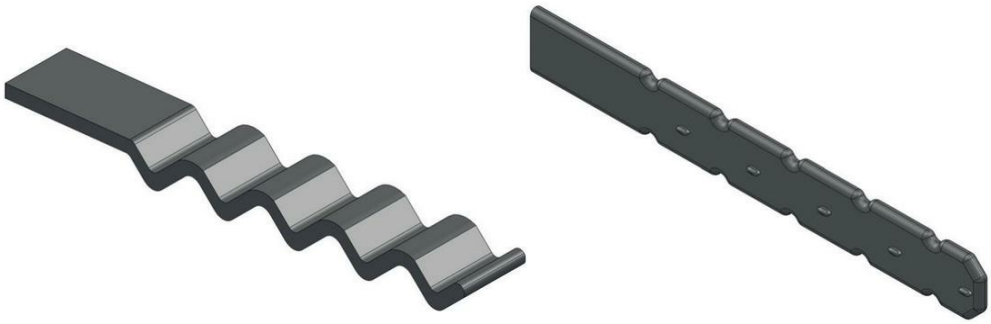
Most dimple lock tools designed for raking techniques consist of a simple straight blade. The blade has several bumps or dips, allowing it to be inserted into the lock and rake the pins to set those that are in the upper position.

Unlike picking regular pin tumbler locks, it is relatively rare to be able to open a dimple lock using only the raking technique, given that this type of lock is usually protected by anti-pick pins, which are difficult to bypass without picking each pin individually.

As for regular pin tumbler locks, if you start by raking the lock, this often makes it possible to set the first pins fairly quickly, which in turn, saves a lot of lockpicking time.

Once this has been done, you can then set the remaining pins, using a SPP tool to feel each individual pin still to be set.

Raking tool tips for dimple locks



Conclusion on the choice of tools to use

Although, as we have just seen, a wide variety of tools are available, only a handful of them will be really useful to you.

If you are buying your first tools, do not expect to find the irregular, distorted-shaped tools very useful, but choose a few proven conventional picks instead.

In theory, a raking tool and a medium-sized hook are sufficient to open almost any lock, provided you have the necessary practice.

Chapter 12

Buying tools

Although, as we will see later, you can easily make your own tools, it is often easier to buy them directly, especially as their cost is not excessive and the finishes and the metal used give added value in the medium term, compared to handmade tools.

When choosing your picks, the three points to consider are the fineness of the tool, its strength and its ergonomics.

1. Fineness of the tool

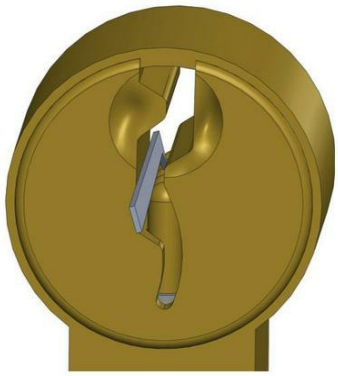
The fineness of the tool refers to both the thickness of the steel used and the height of the blade.

The thickness of the steel should under no circumstances be greater than 0.6/0.7 mm. In fact, it will be difficult to push thicker tools into quite a large number of locks and they will often get stuck inside, making the sensations you feel as you pick the lock much more complex to interpret.

The thinnest tools on the market are currently between 0.3 and 0.4 mm thick. They are often the best, but also the most fragile.

Importance of blade thickness

A thin tool can be inserted into all profiles and avoids too much friction between the plug and the tool.



When purchasing your tools, pay special attention to the height of their blades, because a significant proportion of the tools sold are intended for the American market.

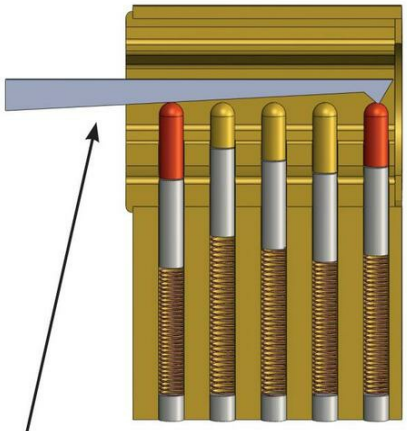
These tools are therefore suitable for "Kwikset" or "Schlage" type locks, which are widely used in America and have a wider and higher keyway than most European lock profiles.

As a result, these tools are very often unsuitable for European locks and can quickly disappoint their users.

It is therefore best to buy tools that are suitable for European locks. **Their blade should not be more than 3 mm high** (even less is better), so that you have a maximum amount of space to move your tools around in the lock.

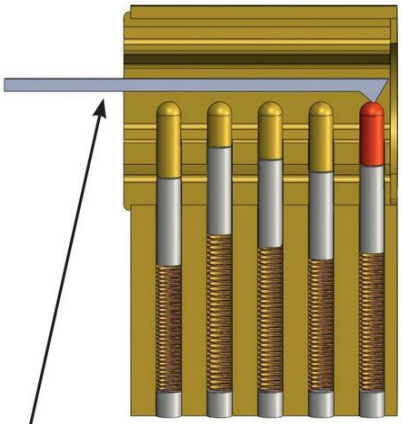
Importance of blade height

Pick suitable for American locks



The height of the blade makes this tool difficult to use. When it manipulates the furthest pins, it also presses the first ones down.

Pick suitable for European locks



The low height of the blade allows the furthest pins to be individually manipulated, without any interaction on the first pins.

2. Strength of the tool

It is difficult to determine the strength of the tool when you buy it, but as a rule of thumb, it is usually best to choose tools made by European or American manufacturers.

However, if you know the specific characteristics of the steel used to manufacture certain tools, you may prefer to buy these.

3. Ergonomics of the tool

Apart from the visual aspect, the ergonomic aspect of the tool handle is also important.
In fact, it determines the grip and feel of the tool when you pick a lock. For example, you should avoid fairly wide, soft plastic handles.

They tend to suppress sensations. This is counterproductive for non-destructive opening, which, apart from needing good technique, is effective because you can feel the action of the tool on the pins.

On the other hand, metal or hard plastic handles are particularly suitable for getting a good feel when you pick a lock, provided, however, that the handle is not so thin that it makes painful marks on the fingers in contact with the pick as you work.

Speaking of ergonomics, it is also highly recommended to buy picks with symmetrical handles, because depending on the mounting of your target lock, it will be necessary to reverse the tool in your hand, **hence a symmetrical ergonomic handle is preferred.**

Chapter 13

Making your own tools

Although there is no need to make your own tools, given the diversity and quality of the tools available on the market, it is nevertheless very pleasing to pick locks successfully with tools that you have made yourself.

To make your own tools, you will need:

- a small bench grinder
- glue and paper
- a glass of water
- an iron
- protective goggles
- hacksaw blades

The most usual material used for making your own picks is a hacksaw blade. Hacksaw blades are, in fact, made from strong, rigid steel and are 0.6 to 0.8 mm thick, which is acceptable, although sometimes a little too thick.

Otherwise, you can use pallet strapping or a feeler gauge intended for measuring spark plug spacing, which is 0.4 to 0.6 mm thick.

Once you have the metal for your picks, you will need to print a scale copy of tool templates you can find online.

When you have printed it to scale, you can cut and glue it onto the metal.

A tip for making this "collage" almost perfect is to cut out a rectangle of paper around the pick you want to make, then soak the rectangle in water for about 5 minutes and apply it to the blade, making sure that the ink is on the blade side.

Then run a very hot iron over the paper so that the ink is deposited on the blade. You will have a genuine printed transfer, which is more practical than simply gluing paper to metal.

When the transfer is finished, all you have to do is to gradually cut out your tool, regularly dipping your blade into a glass of water to cool it down and prevent the metal from losing its rigidity.

If you do not have a bench grinder, a simple metal file can also do the trick, provided you have enough patience...

When you have reproduced the shape of the tool, deburr the blade with a fine grain file or sandpaper, so that the pick does not catch in the lock.

Finally, you can add finishes to the handle for a more pleasant grip. You could put it in a heat-shrinkable sleeve (available from electrical and modeling stores) that you only need to heat for a few minutes in a hot oven to make it stick perfectly to the tool.

Another solution is to cut sleeves out of strips of wood, plastic or metal that you can glue, rivet or weld onto the original pick to give you a thicker handle.

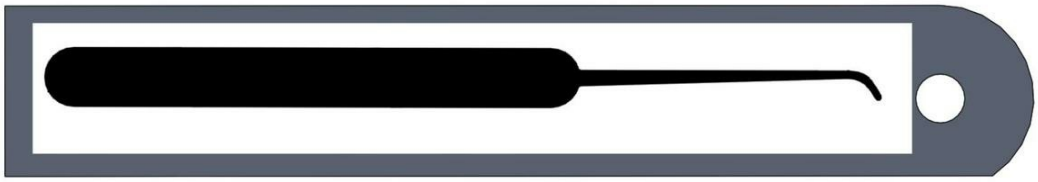
Instructions for making homemade picks

Step 1: choose the material

In this example, we have chosen a hacksaw blade and filed its teeth down.

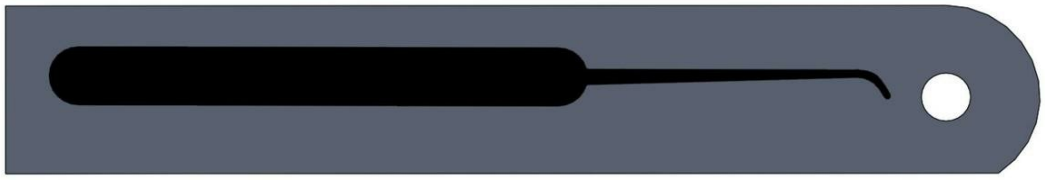
Step 2: glue the printed template onto the blade

After you have soaked the diagram, lay it flat on the blade.



Step 3: transfer the print

After heating the paper diagram with an iron, remove the paper from the blade on which the ink has been deposited.



Step 4: cut out the tool shape

Gradually cut out the tool, then deburr and polish it with a file and sandpaper.

Step 5: make the handle

Cover the handle with the heat-shrink sleeve.

Chapter 14

Lockpicking techniques

After having mastered the theoretical operation of a pin tumbler lock, let's now move on to practical work.

To pick your first lock, start by acquiring a bottom-of-the-range lock from a Do-It-Yourself store or your hardware store.

As a rule, this type of lock does not have anti-pick pins and it will have a fairly large number of machining flaws, so your lock will be easy to pick.

It is important not to start by practicing on more complex locks, because unless you are very familiar with the different available models, you may come up against anti-pick pins.

As a result, you will not be able to open the lock and will struggle to make progress and analyze the sensations you feel when you open it. More complex locks will, however, be very useful once you have mastered how to open "bottom-of-the-range" locks.

Similarly, do not start with locks fitted to doors. Only relatively experienced lockpickers should try to open such locks, because the risk of breaking a tool in your lock, or of not being able to return the lock to the "closed" position once you have opened it, are problems that are frequently encountered when learning non-destructive opening techniques.

1. Raking technique

The raking technique involves simultaneously pushing several pins and setting them at the shearline, without having to manipulate each pin individually in the lock.

This technique assumes that the action of the raking tool on the pins places them one by one in the right order; it proves to be extremely effective in two cases:

a. When the lock is not equipped with anti-pick pins, the raking action theoretically makes it possible to place all the pins on the shearline.

b. When the lock combination is relatively flat, and there is therefore not too much difference in the size of the pins. In fact, we will see later that raking makes it difficult to position pins that are too different in height.

A combination of these two scenarios is, of course, ideal for raking and cases where a lock can be raked open in less than a minute, even by a person with no practice, are not uncommon (about 20% of regular pin tumbler locks).

2. Using raking tools

As explained in the tool description, we must differentiate between the two forms of picks used for the raking technique:

a. "Rake" type tools which, like a key, are made up of teeth of different heights that are used for setting pins at various heights.

b. "Snake" type tools, built on the same working principle, but with curves of different heights, instead of steep angles, as in the case of rake tools.

In reality, the effectiveness of the two tools is quite similar and their uses are pretty much identical.

“Rake" type tools are often preferred. The length of the tip allows them to act simultaneously on a larger number of pins than "snake" tools, which often results in the lock being opened faster and more efficiently and, at the same time, reduces the number of unnecessary movements in the lock.

As the purpose of these tools is to act on several pins simultaneously, it is easy to understand that the pins must be moved relatively evenly, by passing the tool back and forth over the pins, which is different from single pin picking.

The procedure is as follows:

While applying a light tension, move the tool back and forth several times in the lock, starting as high as possible so that you only lightly touch the tips of the key pins.

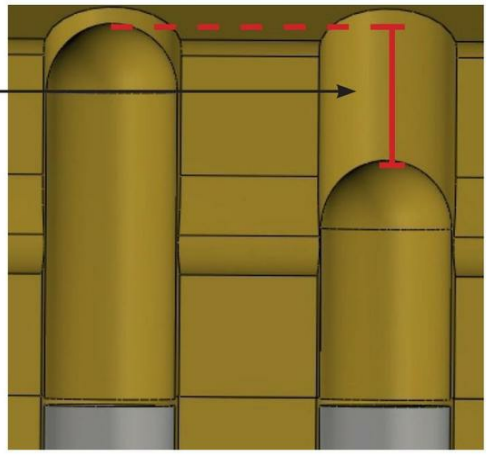
After moving the tool back and forth 4 or 5 times, lower it about 1 mm, move it back and forth several times again, then go down another 1 mm, and so on, until you open the lock or reach the bottom of the profile, meaning that this attempt has failed.

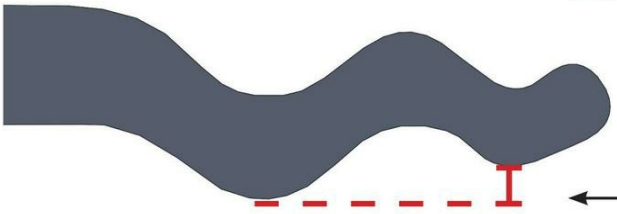
You will then have to repeat the procedure, now varying the angle of the tool or even making a "wave" movement, to operate the pins differently and hope that this will open the lock.

However, depending on the key bitting, the difference between the "highest key pin set at the shearline" and "the lowest key pin set at the shearline" is often greater than the difference between the highest and lowest curve on the tool.

Difficulty in using the raking technique on key bittings with wide variations

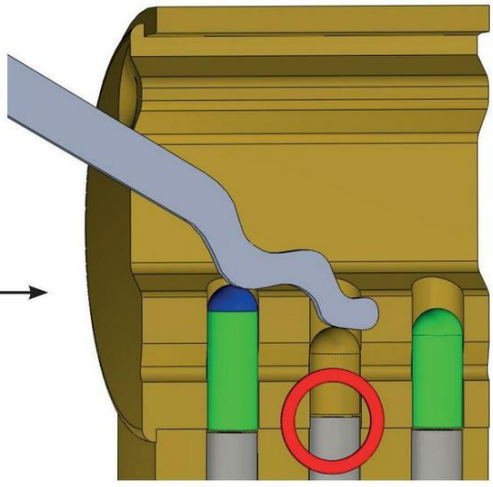
In this example, the difference between the highest and lowest pin is 3 mm.





Here, the difference between the highest and lowest curve on the tool is 1 mm.

Even if you tilt your raking tool to the maximum, you will not be able to compensate for the difference between the highest and lowest pin: the second pin cannot be set at the shearline without pushing the first or third pin below the shearline, and so on.



Bear in mind that, most of the time, the raking technique allows the key bittings potentially formed by the tool to be exhausted fairly quickly.

On the other hand, if after raking for a few minutes, your lock is still not open and your tension on the tensioner is correct, this may mean that the lock contains anti-pick pins. Or that the difference between the highest and lowest pin in relation to the curve of the tool is too big.

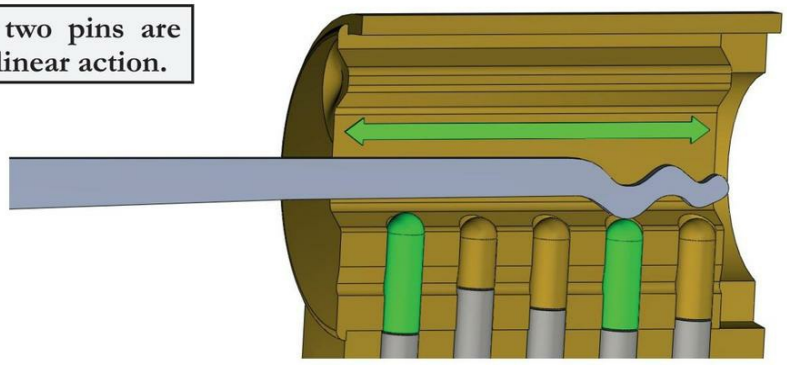
You will then have to use a hook pick to finish opening the lock, although some pins are probably already set on the shearline.

When replacing your raking tool with an SPP tool, be careful not to release the tension on your tensioner, in order to prevent the pins previously set at the shearline from returning to their initial position.

3. Illustration of the raking technique

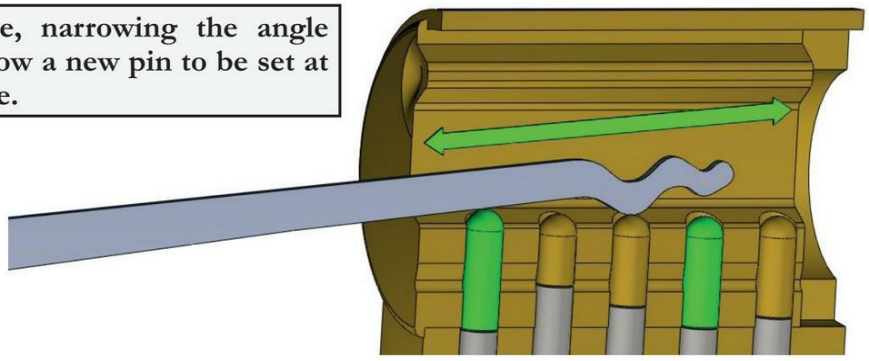
Step 1: linear action of the tool against the pins

In this example, two pins are positioned with a linear action.

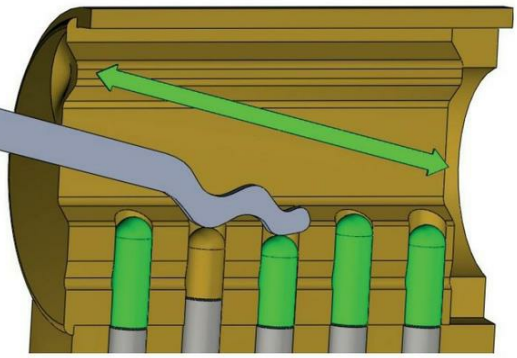


Step 2: narrow the tool angle to vary the combinations

In this case, narrowing the angle does not allow a new pin to be set at the shearline.

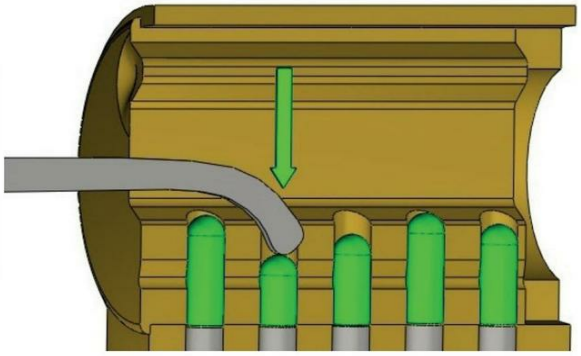


Step 3: widen the tool angle to vary the combinations



Widening the angle sets two new pins on the shearline. There is still one pin to set, but because it is really different in size from the previous pin, this cannot be done with the raking tool.

Step 4: use a hook pick to finish picking the lock



The tension is maintained during the tool change. The hook completes the lock opening process by setting the last pin at the shearline.

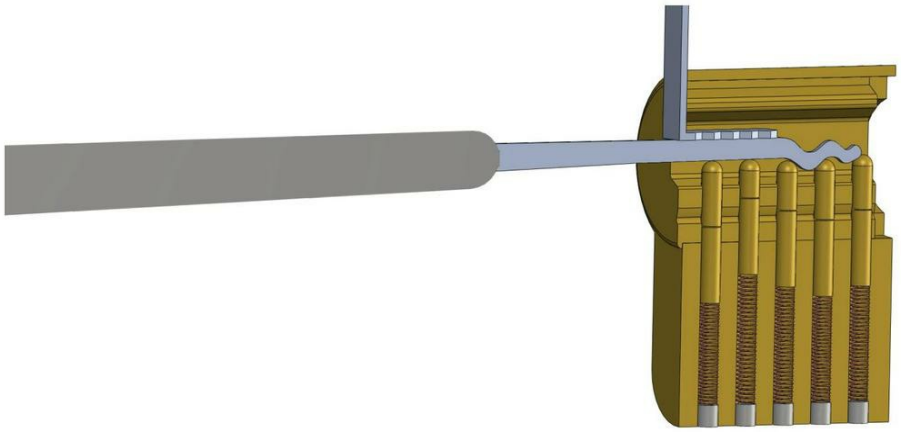
4. Applying the correct tension for raking

Although we have strongly recommended that you start practicing by tensioning the plug on the pins side of the keyway, it is sometimes useful when raking to put the tensioner practically in the center of the keyway.

In fact, when you are raking, the end of the tensioner will act as a guide for your tool which will slide against it, helping you obtain a more effective mechanical action on the pins.

If this tensioner arrangement is not sufficient to open the lock, you must obviously position your tensioner at the top or bottom of the keyway to apply a different raking action to the pins, by widening or narrowing the angle between the tool and the plug.

Using a tensioner as a tool guide for linear raking



As opposed to picking one pin at a time, the action of the tensioner must be relatively flexible because the role of the raking tool is to set several pins at the same time.
The friction between plug and shell must therefore be minimal.

To assess the correct tension to apply, you must be able to clearly hear the pins click as your raking tool passes over them. This sound can, however, also be heard when there is no tension in your lock and the pins do not stay in position after they have been placed at the shearline.

You must therefore listen to this metallic clicking of the pins and associate another sound with it: that of set pins coming back into place once the tension is released.

To find how much tension to apply, practice the following exercise:

1. Move the rake back and forth in the cylinder a few times to detect the regular click of the pins as it passes over them.

2. Then release the tension on your tensioner and listen for the sound of a few pins coming back into place.

3. Repeat this exercise until you can associate the two sounds, the "sound of the pins clicking as the tool passes over them" + "the sound of the pins coming back into position when you release the tension applied with the tensioner".

The combination of these two elements will tell you when you are applying the correct tension to the lock!

5. Why the raking technique is useful for anti-pick pins

The raking technique does not really allow you to bypass the "anti-pick" pins, whether they be "serrated", "spool" or "mushroom" type pins.

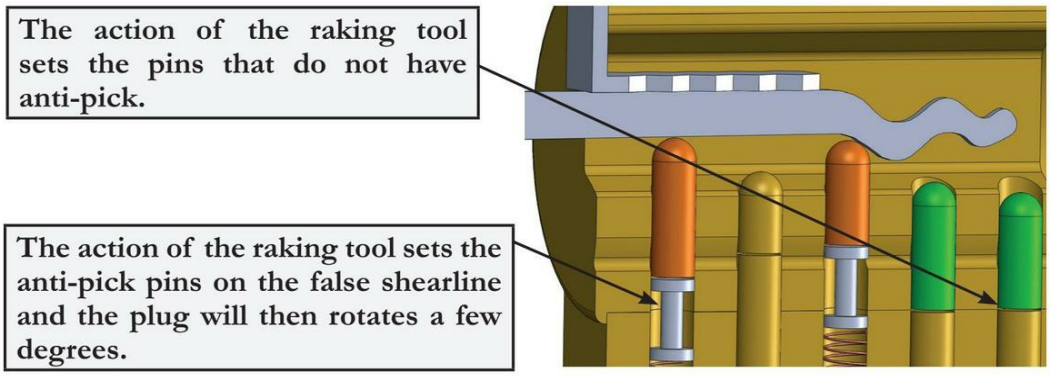
In this scenario, only by using a hook can you feel this type of elements correctly and bypass them by pressing on the pins individually in order to set them accordingly. (See Chapter 8, which is dedicated to anti-pick pins.)

In most cases, locks with this type of protection do not have security pins in all wells.

On the other hand, even if all the pins are fitted with such pins, it is just as important to first block the anti-pick pins on their false shearlines, in order to be able to push them down further later to find the true shearline. Except for some models where it is the key pin that is fitted with such security.

It is useful to use a raking tool when you start to pick the lock because it will help you quickly set the pins that are not anti-pick and/or set the anti-pick pins on their "false gates", which is the first thing you need to do before you can bypass these pins.

Preliminary action of the raking tool on an anti-pick pin



Once you have raked your lock and detected an anti-pick pin on a false notch by rotating the plug very slightly, you will have to use a hook-type tool to set this pin.

As this involves releasing as much of the tension applied to the tensioner as possible, setting an anti-pick pin on the shearline often causes the other pins that were already at the shearline to jump back up.

You will save time by alternating the two techniques to set a few pins by raking and then use single pin picking to set another security pin in position and repeat these techniques alternately until the lock opens.

6. Using single pin picking tools

As explained in the introduction to the tools used for this technique, there are several types of picks that were designed for single pin picking (hooks, diamonds, half-moons) and all of them have in common the fact that they can be used on only one pin at a time.

Single pin picking involves applying the right tension to your plug, then picking the pins in your lock one by one to bring them successively to the shearline.

The order in which the pins are to be placed depends on the friction exerted on the pin when you apply tension to the plug.

As already mentioned, due to machining flaws, when we apply tension to the plug, its rotation is blocked because of the pins that are caught in shear between the plug and the shell.

It is therefore best to start by positioning the pin that has the greatest degree of friction, because it is most likely to remain at the shearline once you have used a hook to lower it into position.

When you have done this, the friction is automatically applied to another pin, which you must again locate by feel to set it at the right depth and then repeat these actions until the lock opens.

While the principle of using the SPP technique is extremely simple, it is far more complicated to do in practice.

In fact, depending on the model of the lock, you will have more or less room to use your tool and as a result, the friction of the hook against the walls of the plug may give you false sensations.
Learning the best way to insert your tool into the lock and correctly pressing the top of the pins to lower them, while maintaining a good feel is therefore not easy.

It's good to start learning the technique by using a practice lock so you can see the position of your tool within the lock and on your pins.
Associating the visual observation of the action of your tool on the pins with a given sensation will undoubtedly help you make fast progress.

7. Applying the appropriate tension for single pin picking

As this subject has already been discussed in more detail in the chapter dedicated to tensioners, we invite you to refer to it for further explanations.

We should, however, bear in mind that it is best to apply tension for single pin picking in front of the pins, without the tensioner making contact with the first pin.

Tension should preferably be applied using a rigid, relatively short tensioner, with as much tension as needed to offset the plug axis by a few degrees from the resting position of the plug. The purpose is to generate friction on the pins caught in shear between the plug and the shell. The tension is then modulated to allow the pin to move when depressed by the pick.

8. Half rotation of a picked lock

Since you have now understood the raking and single pin picking techniques, there is now nothing to stop you using non-destructive techniques to pick your first locks.

However, there may be a problem when you have picked your lock and try to fully rotate the plug to operate the locking mechanism.
You will notice that from time to time your plug may get stuck when you have rotated it 180°.

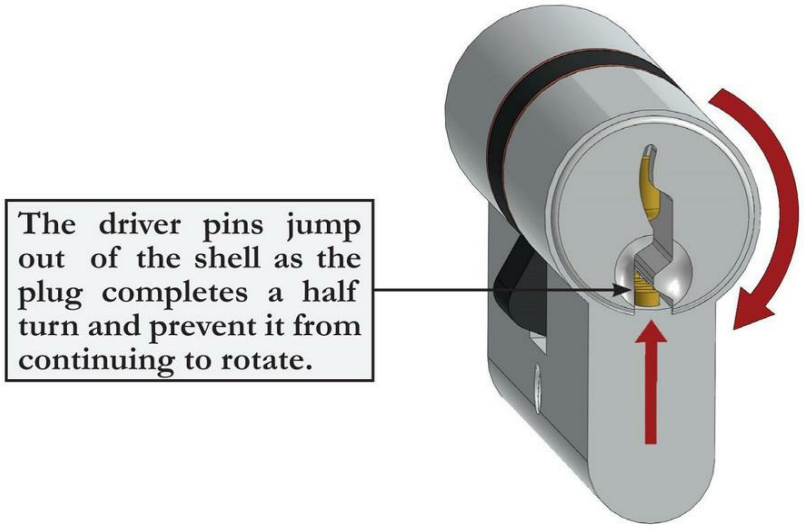
In this case, do not worry, because the lock is not malfunctioning.

Do not try to pick it again, since it is already picked. although you have only rotated it 180° instead of 360°.

In fact, when the plug gets to 180°, the driver pins take advantage of the cut in the keyway to protrude slightly, thus preventing the plug from rotating further.

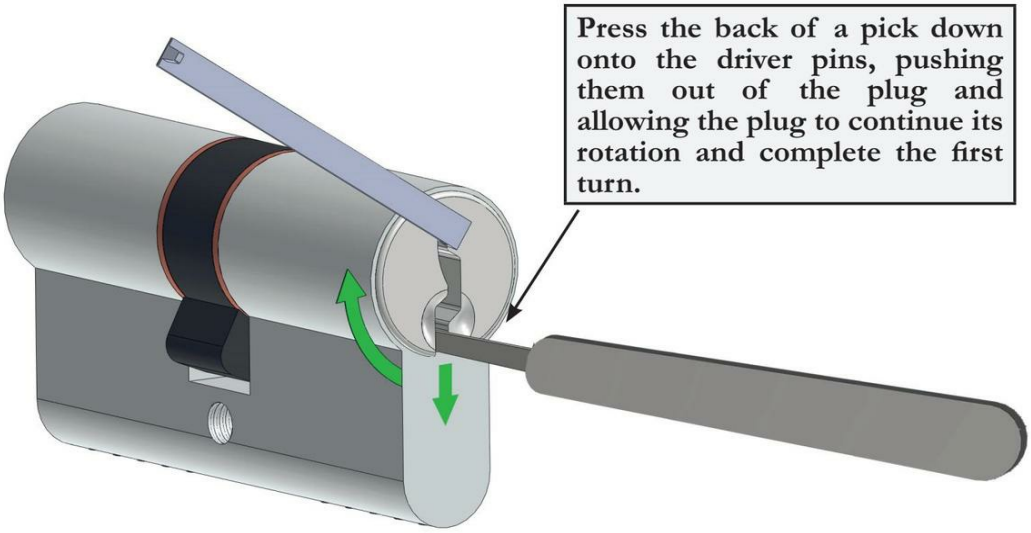
Obviously, this situation is specific to lockpicking because when a key is inserted, it completely fills the channel in the plug and the driver pins cannot come out and block the rotation.

Picked lock, blocked during rotation when the plug reaches 180°



To resolve this problem, simply push the driver pins back down to the shearline with the back of a pick to align them, then use the tensioner to continue the rotation. You will then be able to finish rotating the lock in the usual way.

Unblocking a lock stopped at 180°



Chapter 15

Pickguns

Although the basic techniques used in the "sport" of lockpicking are raking and single pin picking, there are several other techniques and tools that can be used to open most regular pin tumbler locks fairly quickly without damaging them.

These mechanical or electrical tools, known as guns, or "pickguns", are very simple to use and can easily be used by beginners or by professionals who want to use non-destructive opening techniques, as an addition to the other techniques.

As with manual lockpicking, electric or mechanical pickguns only work in conjunction with a tensioner, and once again their purpose is to turn the plug as soon as the pins are set at the shearline.

The opening principles are, however, quite different from one technique to another. And the tips used with pickguns are mainly flat.

We have seen that manual lockpicking involved setting the pins by raking or single pin picking to bring them successively down to the shearline, following a specific methodology.

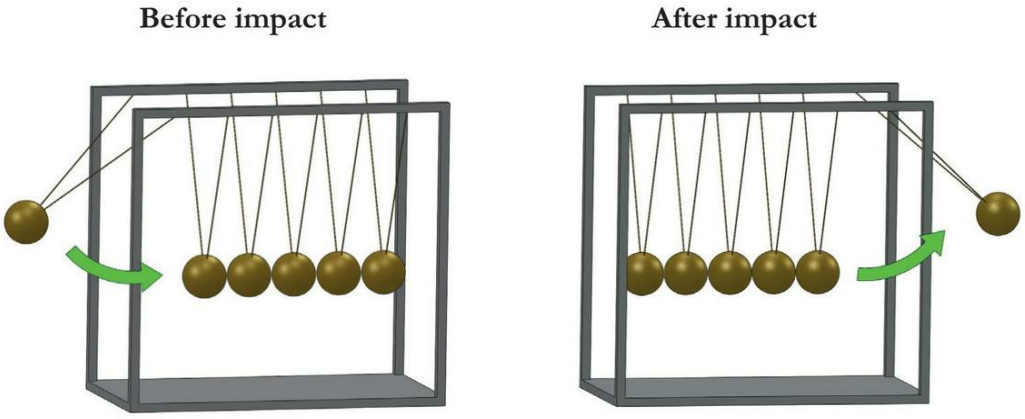
We will now see that mechanical guns work on the principle of transferring kinetic energy between the pins, while their electrical equivalents combine kinetic and random effects, due to the striking force of the needle and the large number of combinations generated by the very fast vibrations of the tool blade.

1. Mechanical pickguns

Mechanical pickguns have a spring that is located inside the body of the tool and connected to a swivel-mounted head.

When the spring is compressed and then released by triggering the gun, the end of the tool suddenly swings and strikes the pins sharply, causing an effect that can be found in the principle of "Newton's cradle", i.e. it transfers energy between the key pin and the driver pin.

Illustration of the "Newton's pendulum" principle



According to the principle illustrated above, when the key pin is struck by the blade of the tool, the key pin remains in place, whereas the driver pin is consequently knocked down, just as in billiards where one ball hits another and comes to rest in its place, while the other, which was stationary, is thrown across the cloth.

The transfer of energy simultaneously applied to all the key pins creates a gap for a fraction of a second at the shearline between the key pins and driver pins, allowing the rotation of the plug driven by the tensioner, which remains the essential complement to the pickgun.

Using a mechanical pickgun

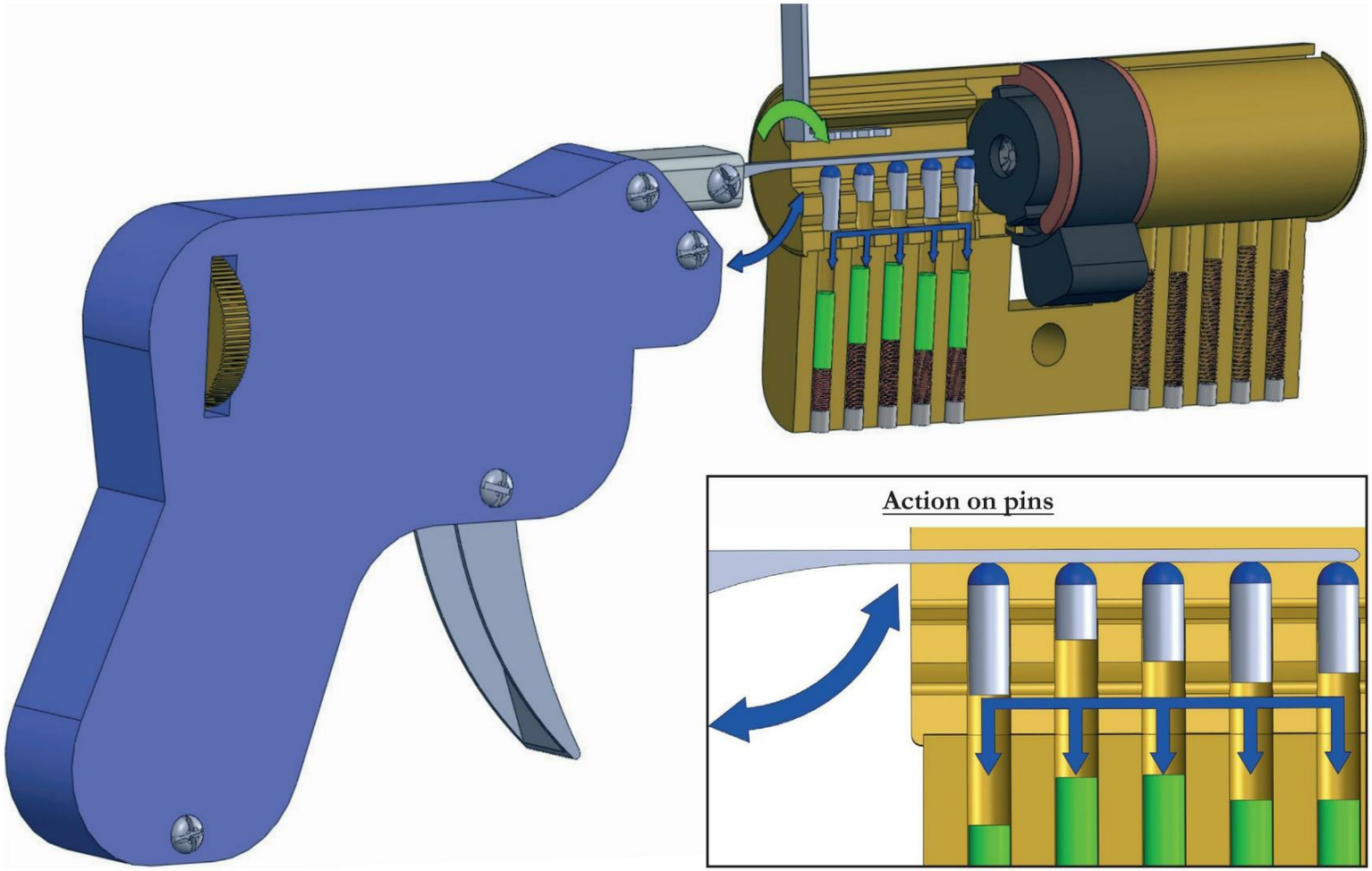
Most mechanical pickguns sold on the market have a thumbwheel for adjusting the force of the spring, and consequently the force of the blow applied to the pins, which means that the tool can be used for different types of locks.

If you decide to invest in this type of equipment, make sure that it is suitable for European locks (if you live in Europe), or that it can be operated in two different positions.

In fact, in most cases, mechanical pickguns are intended for the North American market where the locks are fitted "upside down" with respect to European locks.

In this case, the gun strikes upward and not downward, which means that the tool has to be turned upside down to be used on European locks.

How a manual pickgun works



Tension to be applied with a mechanical pickgun

As opposed to conventional lockpicking, you will have to apply quite a light tension to the plug to enable energy to be transferred under the right conditions, by allowing the key pin to communicate its first impulse to the driver pin, without the driver pin being blocked at the shearline.

To get a precise idea of the appropriate tension for using this tool, the simplest way is to try it on a practice lock where you can best see how it works.

Mechanical pickguns and anti-pick pins

While mechanical pickguns are supposed to be able to circumvent anti-pick pins, they do not perform very well unless you have a lot of practice with it.

It might be necessary to finish the opening using the SPP technique with conventional picking tools.

The other solution is to opt for an electric pickgun, as this tool is very effective on anti-pick pins, as we will discuss later in this chapter.

But first, let's see how you can make you own mechanical pickgun.

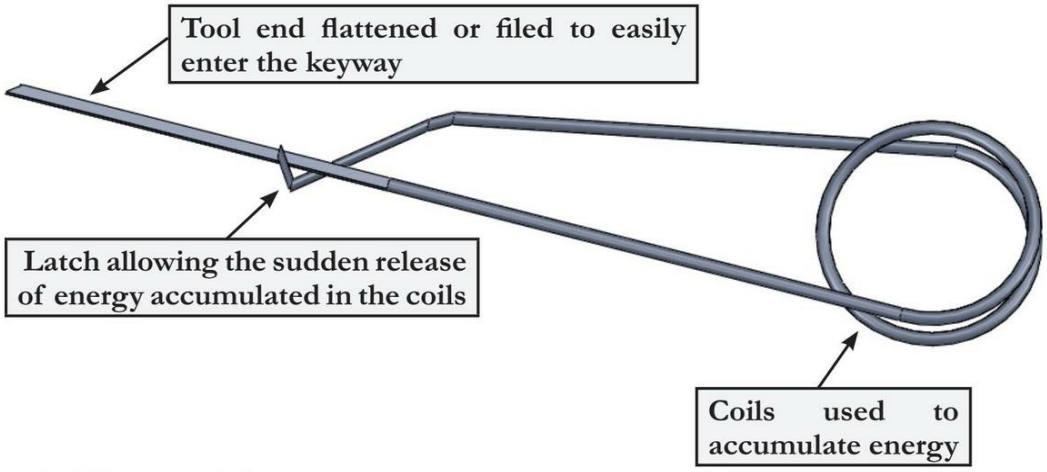
Making a mechanical pickgun

As you have understood, the operating principle of a mechanical gun is fairly simple.

It requires stocking energy and suddenly releasing it to strike the keys pins, to create a gap with the driver pins.

You will easily be able to make a tool using pliers and piano wire, as shown in the following diagram and get your first results. But these will be nowhere near as good as those you would get with a factory-produced mechanical pickgun.

Operating principle of a homemade mechanical gun



2. Electric pickguns

Unlike mechanical guns, these tools do not operate solely on the principle of energy transfer.

Their effectiveness is also based on their ability to produce several hundred vibrations per minute, which are transmitted to a flat tip fixed to the end of the tool. The tip is the same as those found on the mechanical pickgun, which strikes the key pins in the lock at high speed.

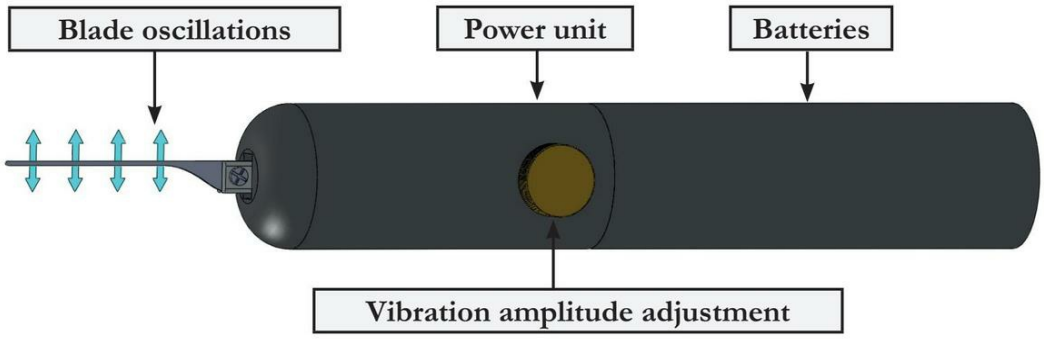
The combinatorial capacity of these tools therefore makes them extremely effective when the lock does not have specific anti-picking protection.

On the other hand, even when you are trying to open complex locks that do have such protection, an electric pickgun usually gives spectacular results.

The only disadvantage of this tool is that the tensioner might fall out, due to the high vibrations to which it is subjected.

A double tip, circular tensioner, is a very effective solution to this problem.

How an electric pickgun works



Applying tension with an electric pickgun

Since the vibrations are low amplitude and very fast, only minimal tension should be applied to the plug and as much care as possible should be taken to avoid blocking the pins, as this would prevent them from being manipulated by the tool.

Furthermore, the tension will also have to be extremely flexible, because bypassing security pins requires the plug to be free to move backward to get past them.

Unlike manual lockpicking, we particularly recommend you use a double tensioner, preferably a circular tensioner in this case, and apply tension alternately to the right and to the left, changing direction as quickly as possible.

Making an electric pickgun

Although there are excellent electric pickguns on the market, you may decide to make your own.

Any commercially available tool operating on a vibration system can be "converted" for this purpose by attaching a pick to the moving part, so that the movement is transmitted to the pick and activate the pins.

You can make your own electric pickgun from razors, toothbrushes, cutters or electric scissors with a fairly good level of success.
Battery-powered tools would, of course, be best, as you would then be able to carry and use your tool under all conditions.

All the effort of making an electric pickgun will then be focused on your pick attachment system.

However, this will be much easier if you have the proper equipment for drilling a metal component and fitting a simple fastener onto it, for example with a small wing nut that will allow you to change your picks regularly. The pickguns picks tend to break quite quickly, due to the very high number of vibrations.

Note: whether an electric pickgun is factory produced or homemade, it is best suited to regular pin tumbler locks. Its effectiveness on dimple locks is very limited, but bumpkeys can be used to overcome this problem.

Chapter 16

Bumpkeys

Bumpkeys, which are also known as 999 keys, are intended for non-destructive opening of pin tumbler locks.
They operate on the same principle as the manual pickgun that we described in the previous chapter.

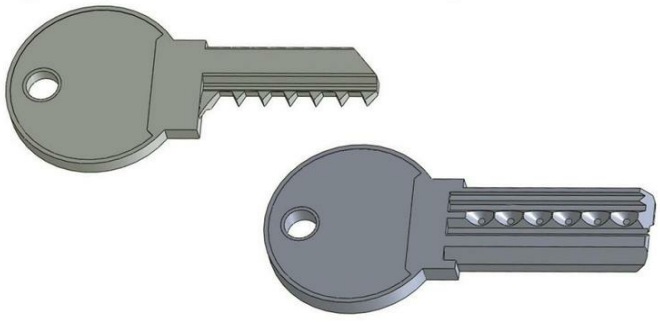
The principle involves striking all the key pins simultaneously so that they transmit their kinetic energy to the driver pins.
This creates a gap at the shearline between the key pins and driver pins, causing the lock to open.

However, despite the similarity of their opening principle, the success rate of bumpkeys remains higher than that of the pickgun because it is possible, with the appropriate keys, to open locks with very complicated keyhole profiles, as opposed to with a pickgun, which can only be inserted and used effectively in the simplest profiles. And as previously mentioned, bumpkeys will be far more effective than electropicks on dimple locks, for example.

To achieve the desired effect, the keys are cut to their maximum depth at each pin location, with the teeth of the key sufficiently ramped to strike the pins at an angle.

On pin tumbler lock models, bumpkeys are therefore keys where all the "teeth" are cut as deep as possible, which explains why these keys are sometimes called 999 keys, because nine depths are generally possible for a pin on a regular pin tumbler lock. Whereas, in the case of dimple lock pins, as the height of the key is less than the height of regular pin tumbler lock keys, the pins can, in principle, have only four to six depths.

999 keys for regular pin tumbler locks and dimple locks



Shape of bumpkeys cuts

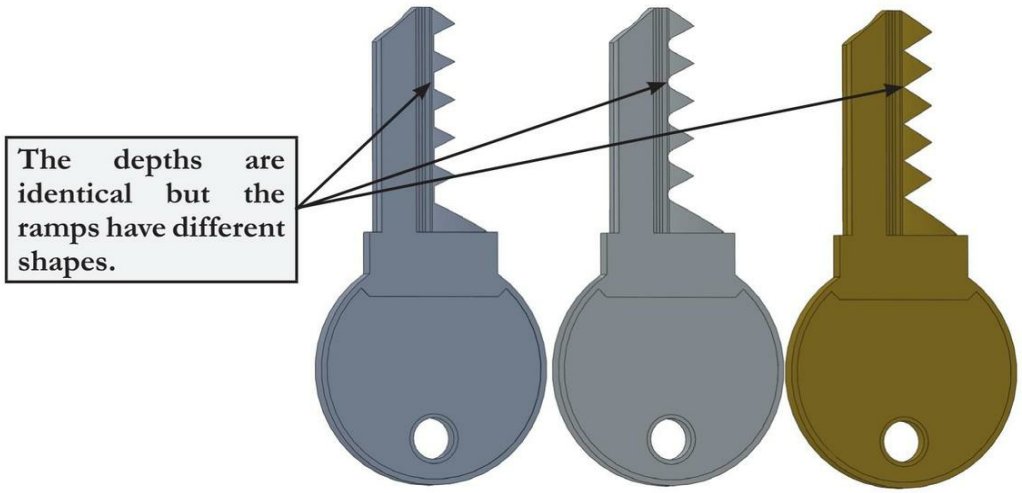
While the depths of bumpkeys are always equivalent to the maximum possible depth of the lock targeted, the shape of the ramps is also really important.

We will see that when bumpkeys are used, we strike them with a plastic hammer to act on the pins inside the lock.

It is therefore the ramps of the key that will hit the pin to transfer the energy necessary to push the driver pins past the shearline.

That is why, depending on the key model encountered, some ramp shapes will be more useful than others for opening the lock, because they will strike the pins more effectively.

Set of bumpkeys for the same keyway profile

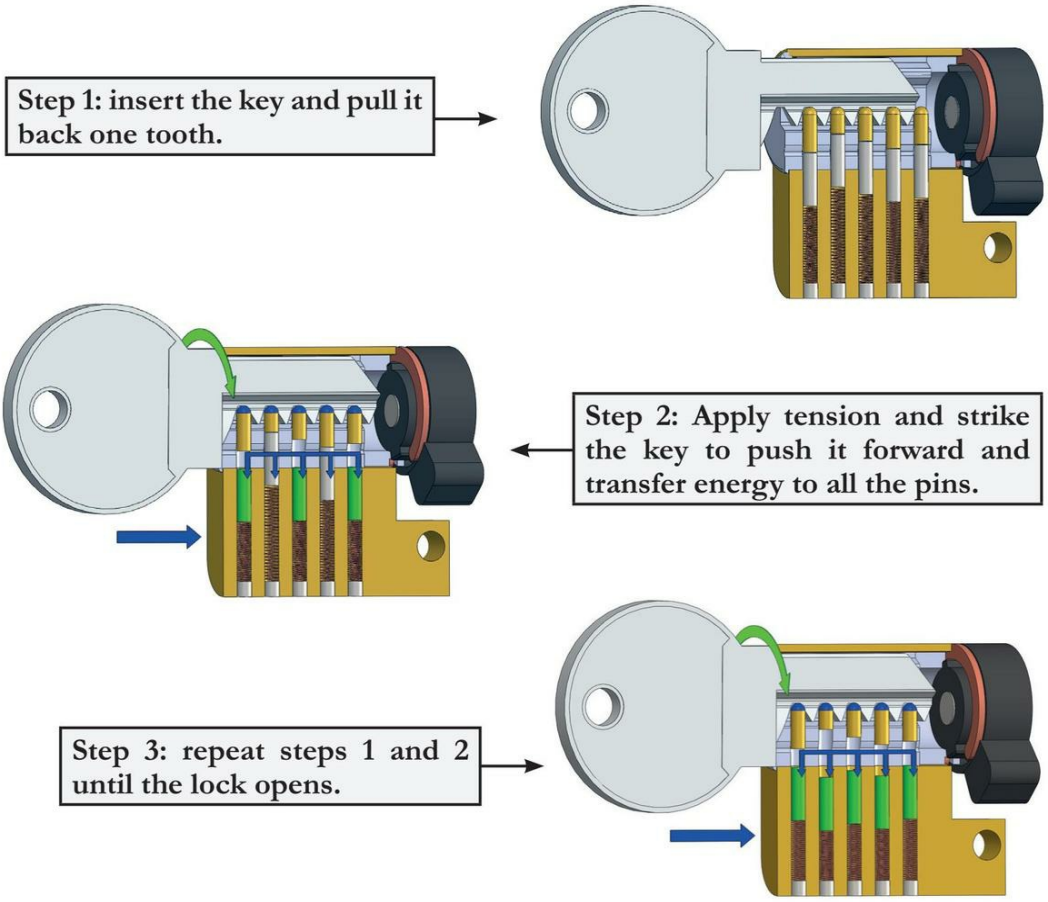


Using bumpkeys

Two opening methods can be used successfully with bumpkeys.

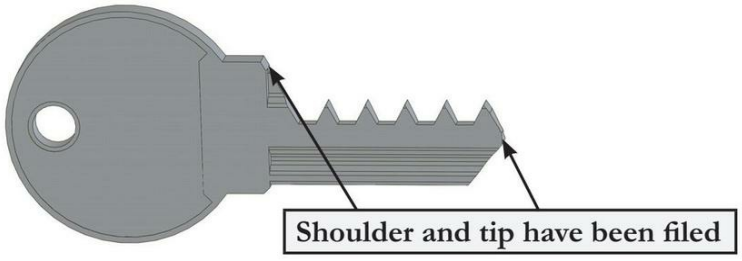
The first one, called the "pull" method, involves pulling the key out one notch and then striking it on the head to hit the pins and transfer sufficient energy to push the driver pins below the shearline. At the same time you must apply a very light tension for the plug to actually rotate when the gap occurs at the shearline.

Illustration of the "pull" method



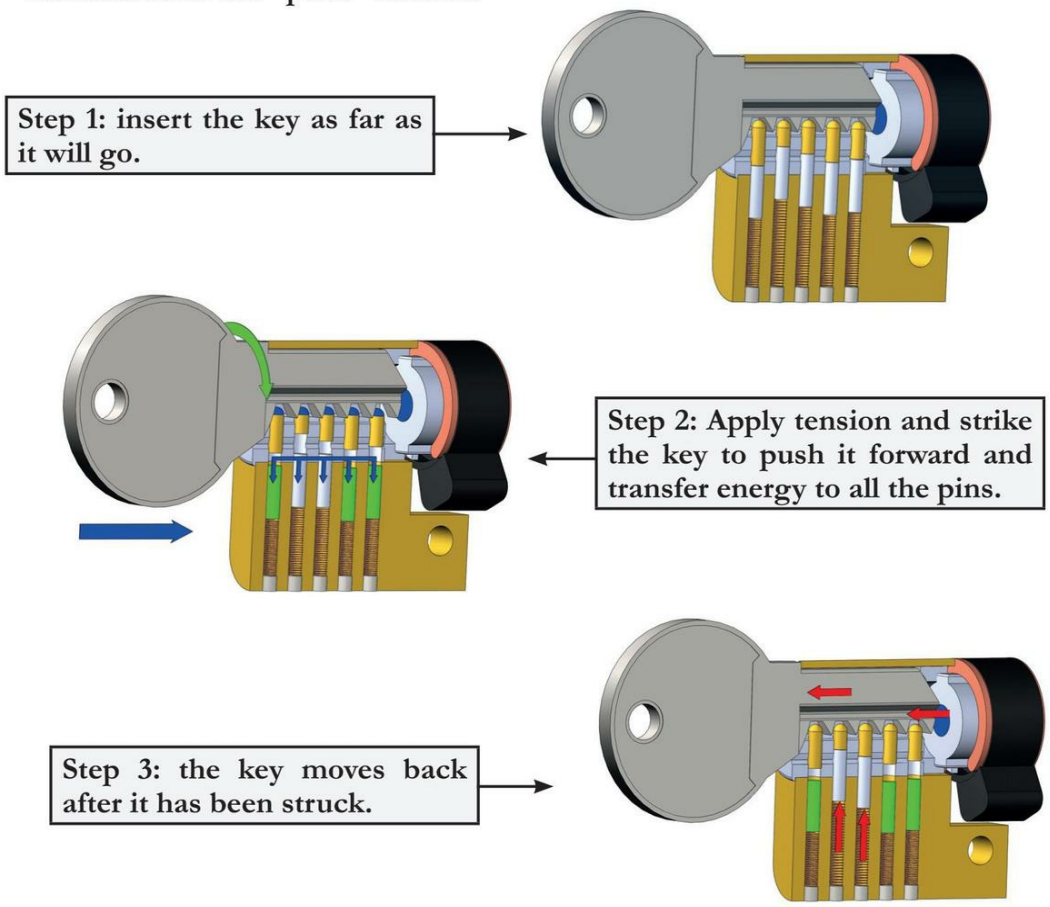
The second method, called the "push" method, involves using a bumpkey with its shoulder and tip slightly filed down to allow it to go a little further into the lock than a standard key. When you strike the key, its teeth will hit the pins and create the gap necessary to allow the plug to rotate.

Bumpkey modified for the "push" method



With this technique, the tip of the key contacts the coupling when the head of the key is struck. The key will then move back one or two millimeters to be struck again after it has been fully inserted, due to the reverse force exerted on the key by the pins.

Illustration of the "push" method



Using a bumpkey hammer

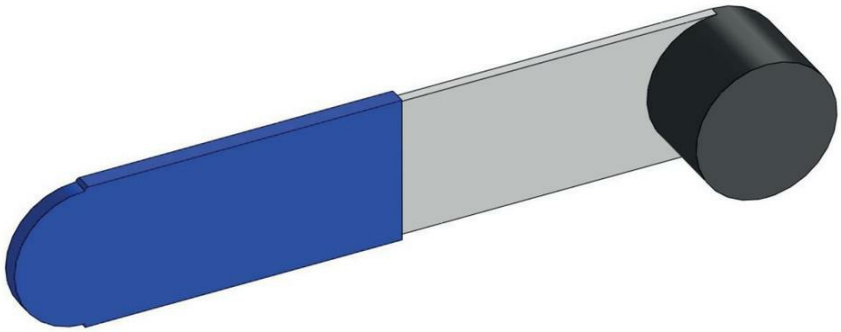
Regardless of the method used, several taps are often required before the lock can be opened.

The tool used to strike the key, and transfer its energy to the key and then in turn to the key pins and driver pins, is then extremely important.

A hammer generally consists of a relatively flexible handle to which a rigid plastic head is attached.

In fact, this type of tool allows you to easily vary the amplitude and force of the strike, while transferring correctly distributed kinetic energy to the key head.

Bumpkey hammer



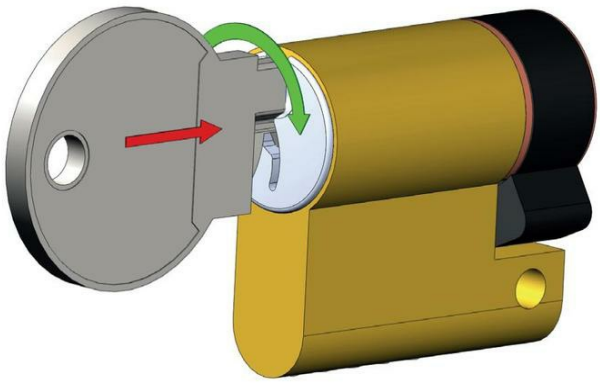
Note: although these hammers have been specifically designed to correspond to the force needed to strike the bumpkeys, you can also successfully use your own home tools such as screwdriver handles, soup or coffee spoons, etc. and more generally any tool with which you can strike the key sharply on the head and which will allow you to vary the amplitude of the blows.

What tension should you apply with the bumpkeys?

You cannot apply tension to the plug with a tensioner, since there is a key in the lock.

The key must play this part itself by exerting tension to the right or to the left, thus triggering the rotation of the plug mechanism as soon as the driver pins are in position below the shearline.

Applying tension by rotating the key



To start opening a lock, the key must be rotated slightly: just sufficiently to apply tension to the plug if the driver pins drop below the shearline, but not too much, otherwise the driver pins will be too tightly wedged between the plug and the shell and unable to move freely under the kinetic energy boosted by the impact of the key pins.

During bumping, this tension will have to be constantly adjusted according to how the bumpkey feels in the lock, and you should not hesitate to increase it intermittently, as soon as you feel the plug turn a few degrees.

The instant during which the gap generated by the transfer of energy between the key and driver pins is actually very short, because the driver pins are immediately pushed back by their respective springs. The most difficult part is therefore turning the key at the precise moment that the pins separate.

Bumpkeys and anti-pick pins

If the lock has anti-pick pins, you will be able to open it successfully with the help of bumpkeys, but when you feel that the plug rotates a few degrees more, indicating that an anti-pick pin is positioned on one of its false notches, you will, as with manual lockpicking, have to minimize the rotational force exerted on the plug, so that it comes slightly backwards the next time you strike the bumpkey, thus allowing the pin to set correctly at the shearline.

Using bumpkeys - Conclusion

The bumpkey technique gives many professionals the possibility to open locks very quickly, mainly on models known for their excellent resistance to lockpicking (including dimple locks).

Obviously and despite the very simple way in which it works, it is a relatively difficult technique to master on complex locks, just like lockpicking, because it involves varying the tension exerted on the plug, as well as the amplitude of the strike, according to how it feels to you, a feeling that you can only acquire with practice.

The main disadvantage of this technique is the need to have at least one bumpkey to match the profile of each lock to be opened.

As a general rule, you will have everything to gain from owning sets of bumpkeys for certain common profiles (universal right and left profile and some common models in your area) that will at first be sufficient to deal with many situations, but later on you should acquire specific profiles, according to your needs.

We should also note that the effectiveness of this technique is based on opening a lock by transferring kinetic energy from the key pins to the driver pins, which implies that the force exerted on each pin should be perfectly equivalent.

In fact, this technique works much better on new locks than on old mechanisms that have become dirty over time or deteriorated with use, and which then tend to require a slightly different force from one pin to the next to effect the same movement within the lock. In this case, the bumping technique loses much of its effectiveness and it is better to use impressioning or lockpicking to open the lock.

To maximize your chances of success, whether the lock is new or deteriorated, it is a good idea to spray the lock with a lock-special lubricant before you start bumping. Spraying will allow the key and pins to move more easily and catch less on the few rough edges you may encounter in the lock, caused by wear and tear and the gradual introduction of dust and small foreign bodies.

Chapter 17

Key impressioning

Impressioning is a non-destructive opening technique that is used to make a working key from a lock without taking it apart and without knowing the key bitting in advance.

Although relatively unknown to European professionals, impressioning has many advantages over lockpicking (besides being my favorite public technique).

- Operators can obtain a working key that can open or close the lock with a double turn and which can be copied manually or mechanically.
- They can take a break and come back later without losing the work that has been done (unlike lockpicking where all pin positioning is lost if you release the tension on the plug).
- The method is not more complicated on a dimple lock than on a regular pin tumbler lock, even if the cylinder contains a large number of pins.
- Anti-pick driver pins have virtually no effect on impressioning.
- It sometimes takes longer to open a lock with this method than with lockpicking but the results are far more reliable. If impressioning is done correctly, it is almost always guaranteed to work.
- The finished key can be passed on to another operator to perform further work if necessary.

The fact that this technique is not very well known is probably due to Hollywood films, which have always portrayed lockpicking, rather than impressioning.

Apart from this anecdotal aspect, it is, in my opinion, a technique that is as effective as lockpicking, if not more, and the fact that it is less popular is in no way justified by the following few disadvantages, which probably explain why it is so infrequently used:

- Impressioning requires a key blank that matches the target lock.
- It is best to use blanks made of brass rather than steel.
- You should have a good magnifying lamp or at least excellent sight.
- It takes a fairly long time to impression a lock and a trained operator will need between ten minutes and one hour and a half to make a working key, depending on the lock model and its combination.

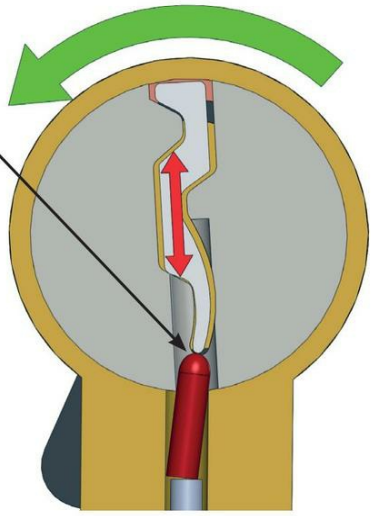
However, these few complications should not discourage you, because, apart from the fact that mastering the technique of impressioning will make you stand out in your profession, it will truly give you the confidence that you can open almost any door!

Operating principle of impressioning

The principle of impressioning is extremely simple.
A new blank, held firmly with a small vice grip, is inserted into the lock and a slight rotational force is applied to block the key pins in shear between the plug and the shell, then the blank is rocked up and down.

The pins caught between the plug and the shell slightly mark the blade of the blank, just as a needle would mark a smooth surface.

Rocking the key up and down makes marks on the blank as it hits the blocked pin.



N.B. It is best to use brass blanks to obtain clear marks, as the pins, which are also made of brass, mark brass blanks better. Alternatively, more common steel blanks can also be used.

The marks produced by the pins on the blank are then filed as they appear, allowing you to gradually replicate the cuts of the working key.

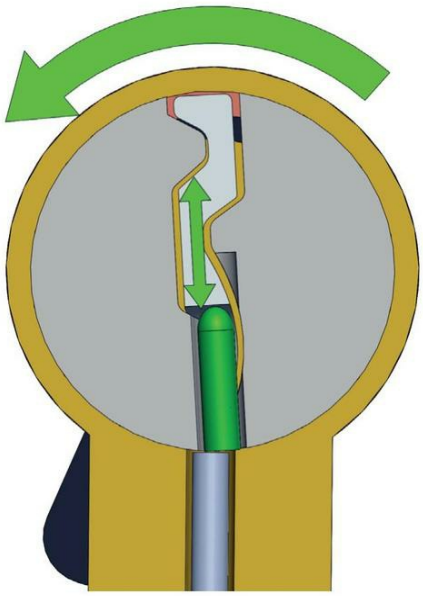
When the teeth of the key are cut deep enough to allow the pins to reach the shearline, the pins stop marking the blank because they are no longer caught in shear between the plug and the shell and are therefore free to move at the same time as the key.

Sectional view of a pin set at the shearline by impressioning

When a pin is at the shearline, it has a slight clearance that allows it to move up and down at the same time as the key.

Doing so, the pin no longer marks the key when you rock the key up and down.

Warning: if the key has been filed too deep, the driver pin will be blocked between the plug and the shell again and new marks will appear.



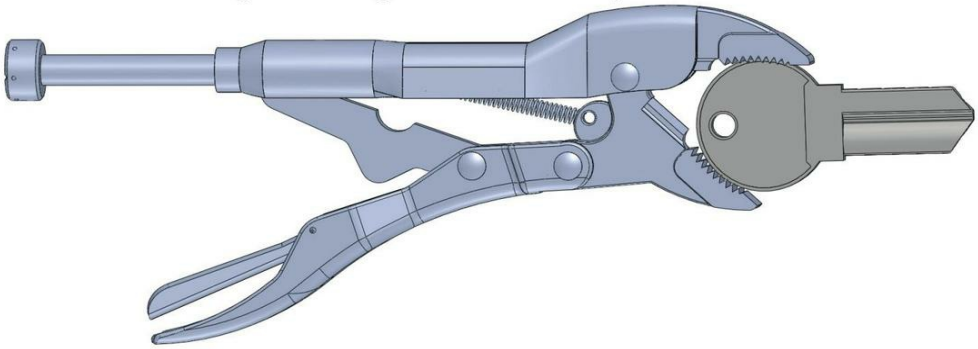
Equipment required for impressioning

- A good quality fine-grit half-round file (2 to 4) for making cuts in your key blank
- A small locking vice grip or a dedicated impressioning handle with a good grip generating a lever effect on the impressioning blank
- A brass blank suitable for the target lock
- A desk or pocket magnifying lamp to help you read the impression marks on the key blade

Impressioning procedure

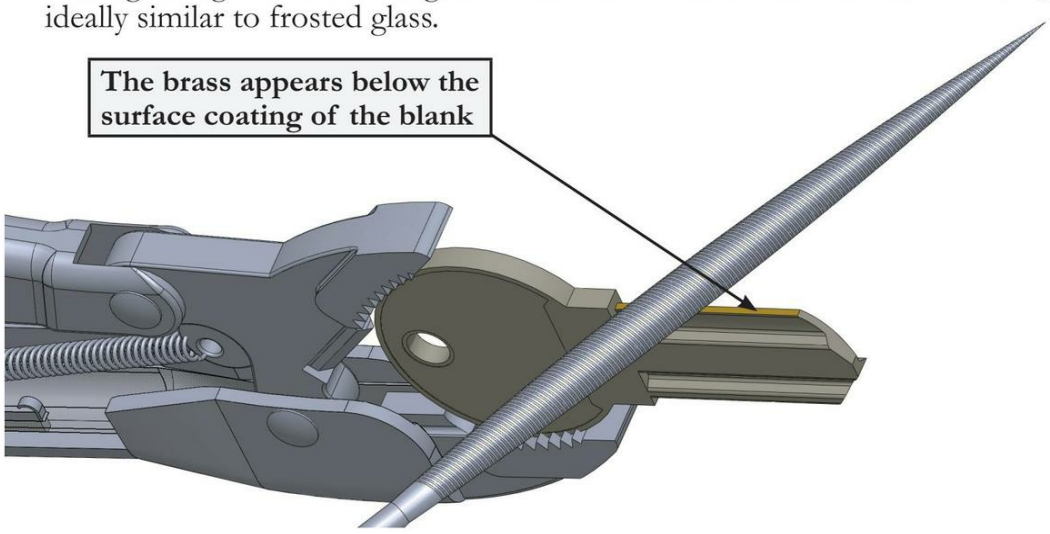
Step 1: Secure the blank

Clamp the key in your vice grip so that it cannot move. You will then find it easy to handle and have the right leverage to manipulate the blank in the plug and make the impressioning marks on the key:



Step 2: Prepare the blank

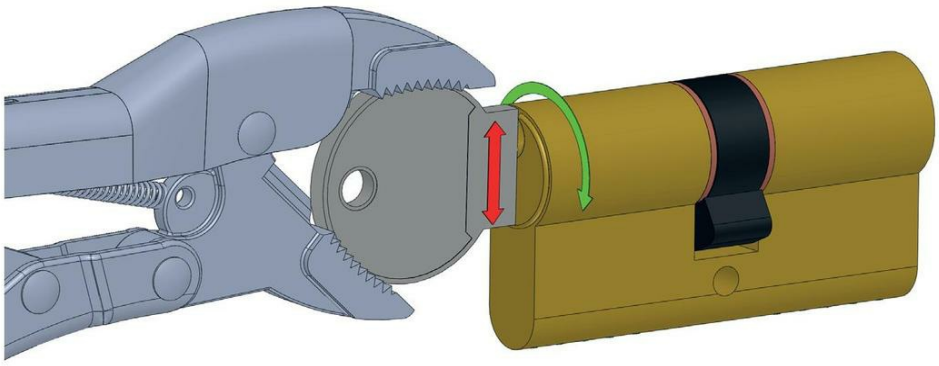
Slightly file the key blade using the flat part of the file to clean off the surface coating along the entire length of the blade and obtain an even surface, ideally similar to frosted glass.



Step 3: Make the marks

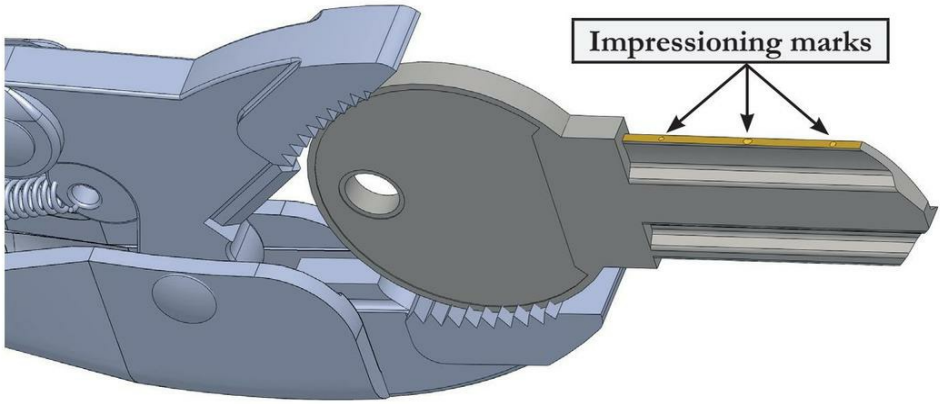
Insert your key into the lock and rotate it slightly **with one hand,** then rock it gently up and down two or three times with your vice grip **with the other hand**, bearing in mind that you will probably have to perform these movements dozens of times before you obtain a working key and that you do not want to risk breaking your blank.

Then apply a rotational force in the other direction and repeat two or three up-and-down movements **using both hands** as before.



Step 4: Look at the marks

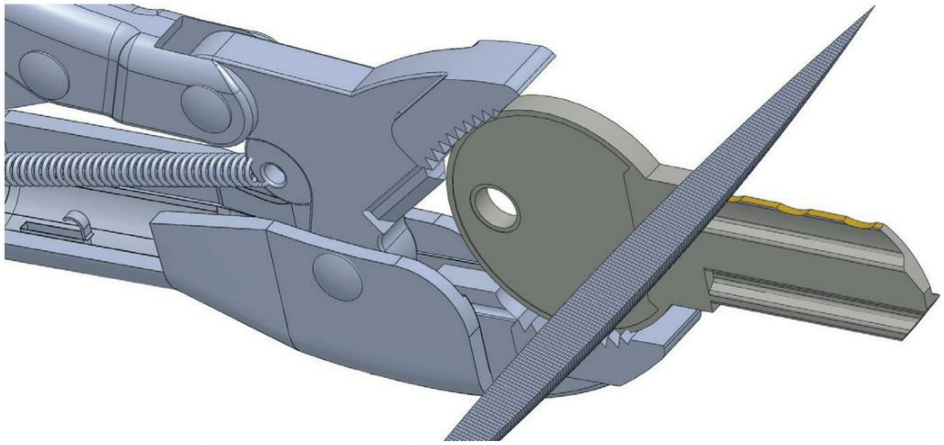
Release the tension, then carefully remove your key from the lock and look at the blade. You should be able to distinguish the marks made by the pins. To see them clearly, turn your key in all directions to see it in the best possible light and at every angle. The marks may appear as tiny shiny spots or as dark spots.



Step 5: File the marks

File each marked location down to a depth of approximately 0.2 mm. Of course, you should only file the blank where the marks are, without touching the rest of the blade.

Golden rule: if you are not sure about a mark, do not file it!



Note: use the full length of your file. If it is in the right position, it will not overlap adjacent pin locations.

When you file a mark, two things happen:

- The depth changes, allowing you to retest the key with a slightly different bitting.
- The mark that was there before you filed it is erased, leaving a blank surface ready for receiving another mark in the same place.

Step 6: Make the key

Repeat steps 3 to 5 as many times as necessary, to recreate the key bitting corresponding to the pin setting in the lock. You will know that your key is finished when you insert it into the cylinder after filing it and see that it now rotates the plug freely as soon as you exert a rotational force.

A few impressioning tips:

1. Avoiding blocking the key in the lock

When making a key, the deeper the cuts, the more likely it is that you will get stuck in the lock.

As soon as you feel that your blank begins to catch when you take it out of the lock, be sure to round off the top of the ramps of the teeth with the flat side of your file, as illustrated earlier in Chapter 5, where we describe creating a key from a disassembled lock.

Another cause of the key becoming blocked in a lock is, of course, when your blank breaks. In this case, if the key has been cut properly, the pins will not block the removal of the key and an extractor or even a relatively thin pick can help you remove the broken piece of a blank quite easily.

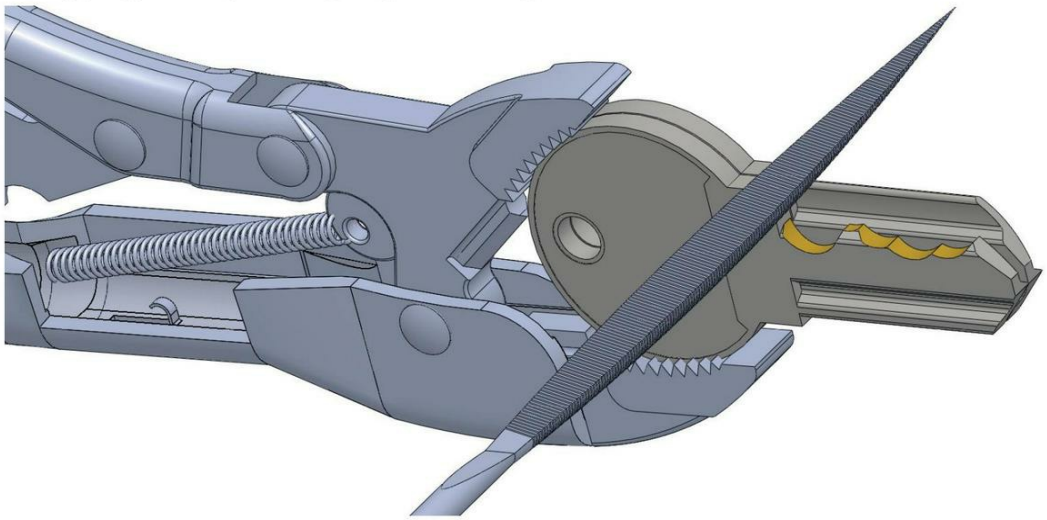
2. Copying the key during impressioning

While you are marking the blank, the repeated movements to the blank through the vice grip sometimes end up breaking it, especially if the first pin requires a relatively deep key cut.

If you apply the correct force when you wiggle the key around inside the lock, you will feel that the key is beginning to break and you can anticipate this problem by immediately pulling your blank out of the plug.
To ensure that you do not lose the work you have done so far and to be able to carry on later with an unstressed blank, simply clamp the blank that is about to break in exactly the same position next to a new blank and replicate your work on the latter.

Obviously, this technique also gives you the possibility of making a duplicate of the key once the lock is open.

Copying the key during impressioning



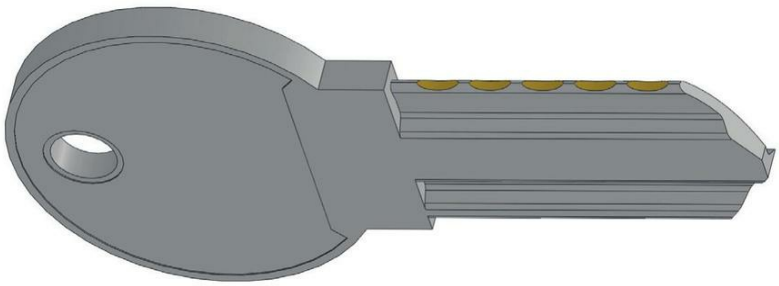
3. Preparing your blanks for impressioning

If you are often faced with identical lock models that you regularly open by impressioning, it will be to your advantage to prepare your blanks in advance, so that you know exactly where to look for the marks produced by the pins.

To do this, proceed as explained in the chapter on how to make a key from a disassembled lock, by marking the position of the pins on a new blank inserted in an empty plug and then starting to file very lightly at this location.

When you start impressioning, you will immediately know where to look for the impressioning marks, which will save you a lot of time.

Key prepared for impressioning on a specific model of lock, so that you can more easily locate the pin marks



4. Impressioning dimple keys

Thanks to the thickness of dimple key blanks and the lowest possible number of depths in a lock of this type (usually 4 to 6 possible depths, as opposed to 9 or 10 for regular pin tumbler locks), the impressioning technique is particularly easy on dimple locks.

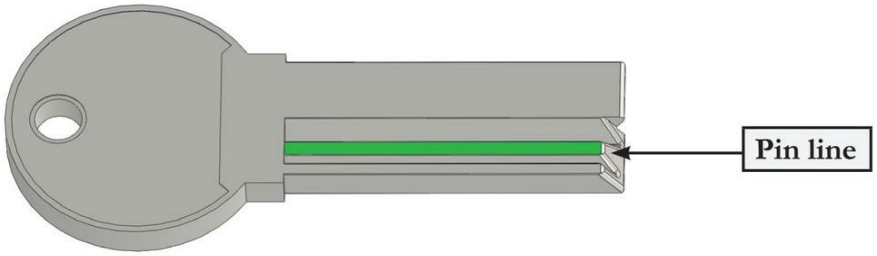
It can seem, however, more complicated because of the shape of the cuts.

While it is absolutely possible to cut the key using a "Dremel" type tool with a round diamond burr, it is equally possible (and actually recommended) to cut the key using the same half-round file used for regular keys.

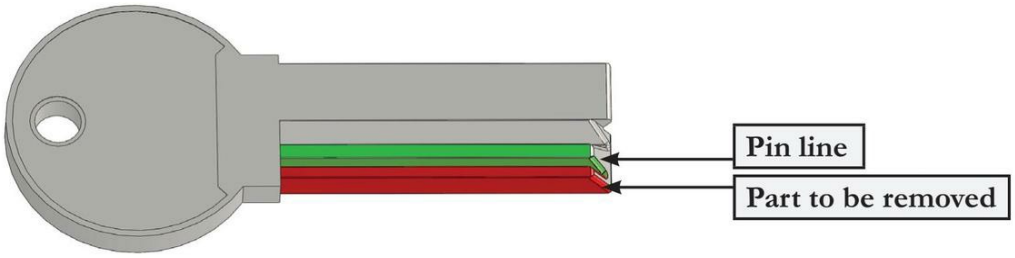
In this scenario, you may want to prepare the blank beforehand to make it easier to file the impression marks.

1. Start by locating the pin line on the new blank, observing how the blank acts in the lock, or a key cut from the same model of lock.

Dimple key with a single pin line

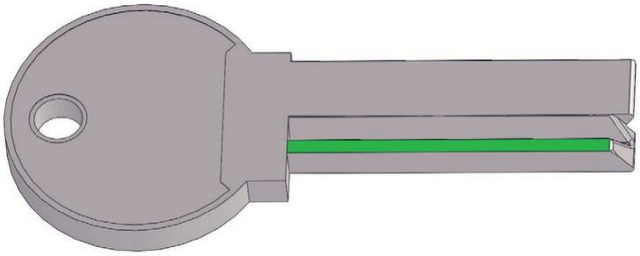


2. When you have located the part of the blank that is not needed, file it away starting from the outside and working toward the pin line.



You will then get a truncated blank that you can use to make your impression. You will easily be able to position your file against the pin line and impression the key.

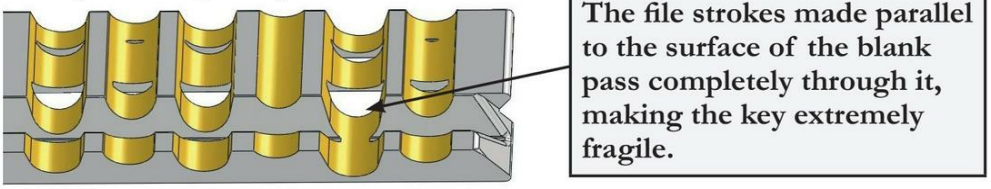
Example of a dimple blank modified to facilitate impressioning



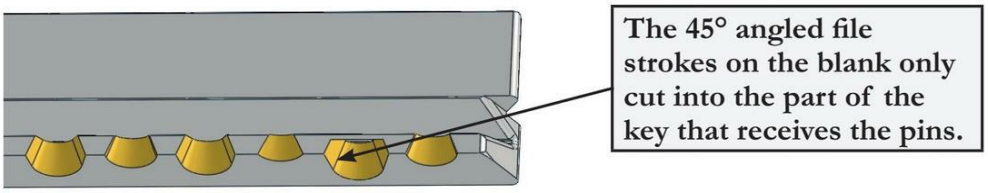
Warning: if the lock you are working on has side pins, you will not be able to remove the portion in question unless they are only single-action control pins that will not block the lock, since the missing material will allow them to sit below the shearline.

When your blank has been prepared, one last precaution to be taken is to file the location of the pins at an angle of about 45° and not parallel to the surface of the blank, so as not to weaken it too much.

Badly cut dimple key blank:



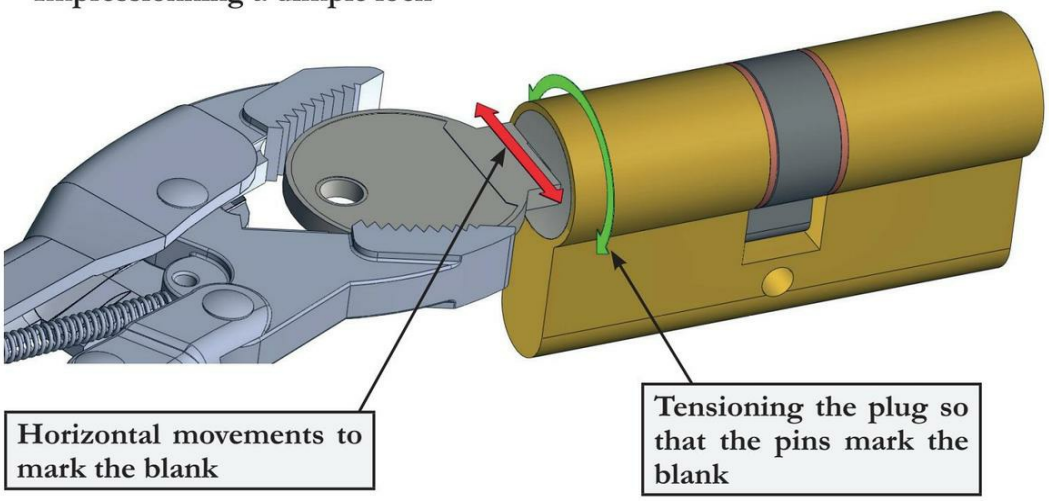
Well cut dimple key blank:



Marking dimple key blanks

As opposed to impressioning keys for regular pin tumbler locks, where an upward movement is used to mark the pins, the horizontal configuration of a dimple lock is more suitable for marking by horizontal movements, from left to right and from right to left, always using one hand to apply tension on the key to make the pins binding and using the other hand to rock the key right and left.

Impressionning a dimple lock



Chapter 18

Soft keys

1. Self-impressioning technique

Soft keys use the same principle as impressioning. This is called self-impressioning, because the key bitting is formed automatically without any need to file the blank.

The self-impressioning technique is based on the use of a modified key, the blade of which, usually made of steel or brass, is replaced by a much softer material.

Aluminum foil, wax, soap, or a combination of these can be used.

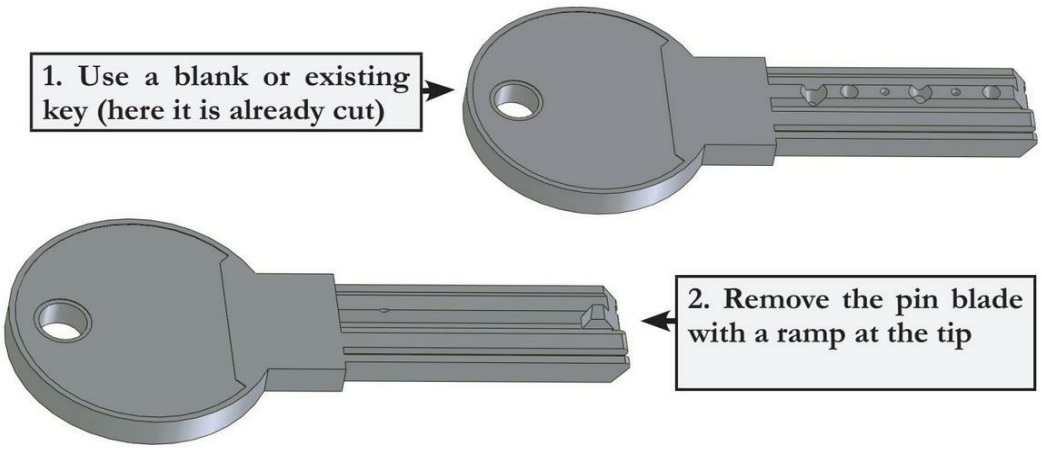
Because of their shape, and the limited number of possible depths, dimple locks are the most suitable for this technique.

Self-impressioning method

Step 1: cut the blank

Choose a key or a blank that matches the profile of the target lock and hollow out the blade at the pin location, leaving a few millimeters at the end of the key to make it easier to insert in the lock.
Remember to create a ramp at the back to allow the key to be removed without getting stuck.

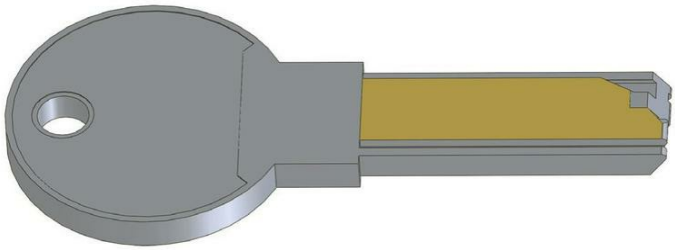
Blank modification process



Step 2: insert soft material

Fill the cavity you have made with wax, soap or plasticine.

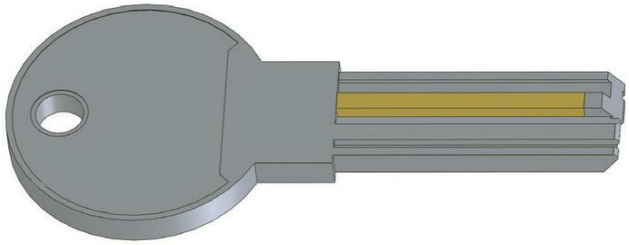
Wax-filled blank



Step 3: create the profile

Using a pointed tool, scrape the sides of the blade to obtain a profile similar to that of the original blank. You can also use an empty plug to insert the key in; this will remove the extra material.

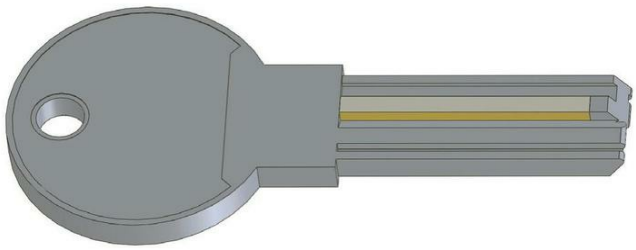
Extracting the soft material until the original profile is obtained



Step 4: finish off the blank

To prevent soft material from getting lodged in the lock, glue a strip of self-adhesive aluminum foil over the modified blade.

Gluing aluminum foil to the modified blade of the blank



When you have completed this laborious preparatory work, the procedure is very simple:

Insert the key into the lock and rotate it alternately right and left for a few minutes, applying firm tension to each side and making sure that the tension does not end up breaking the key.

Alternatively, you can tension the blank and apply a rapid vibratory movement to the key head, e.g. with the chuck of a self-disengaging power screwdriver.

During the self-impressioning process, the pins mark and alter the surface of the key to form the key bitting.

As opposed to traditional impressioning, you must not remove the key from the lock once you have inserted it, as you risk distorting the bitting generated by self-impressioning and lose the work you have done.

When the bitting has been formed, the plug suddenly rotates as if you have just inserted the original key and you can turn the key several times in any direction.

Warning: this key can, however, usually only be used once. In fact, as explained previously, its bitting will probably change and be undecodable once you have removed it. You will therefore not be able to copy it onto a real blank.

2. Foil-impressioning technique

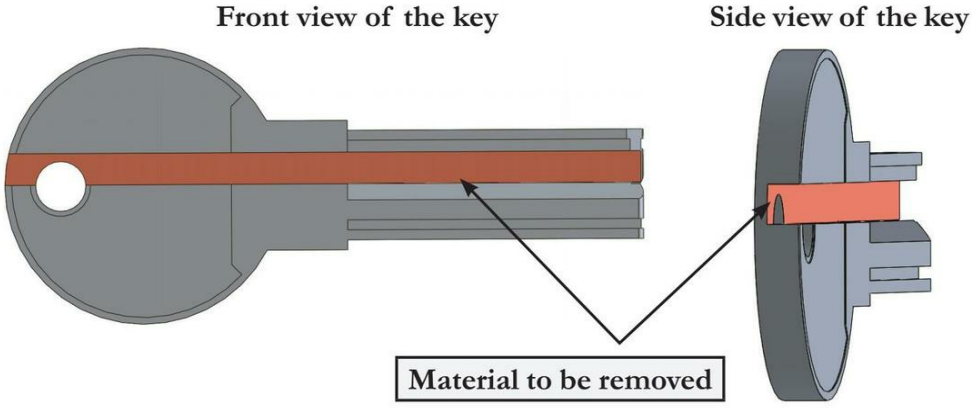
Foil-impressioning is based on exactly the same principle as the self-impressioning technique and allows you to open locks that are known for their excellent level of security even more quickly.

Foil-impressioning method

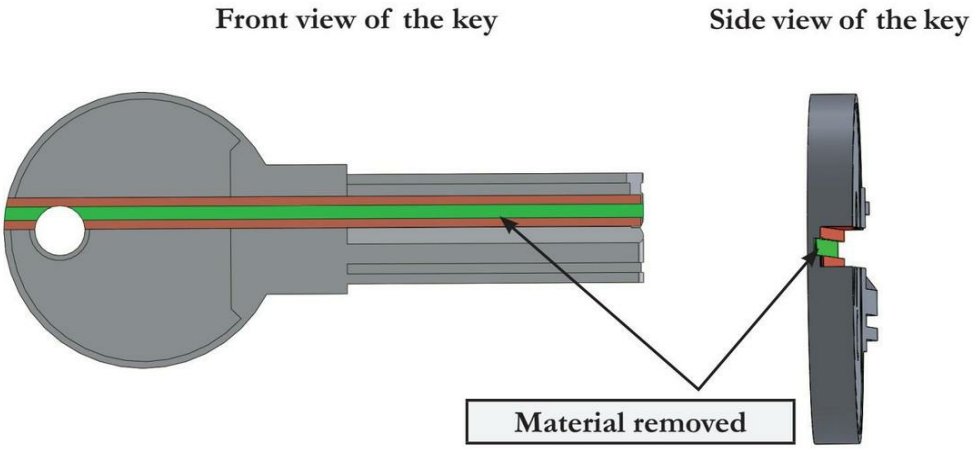
Step 1: cut the blank

Choose a blank that matches the profile of the lock and completely hollow out the blade at the pin location over the entire surface of the key including the key head and wider than the width of the pin blade.

Cutting the blank



When you have done this, dig out a deeper groove of the same width as the blade exactly where the blade was previously located.
(Leave behind as little material as possible, without cutting through the key).

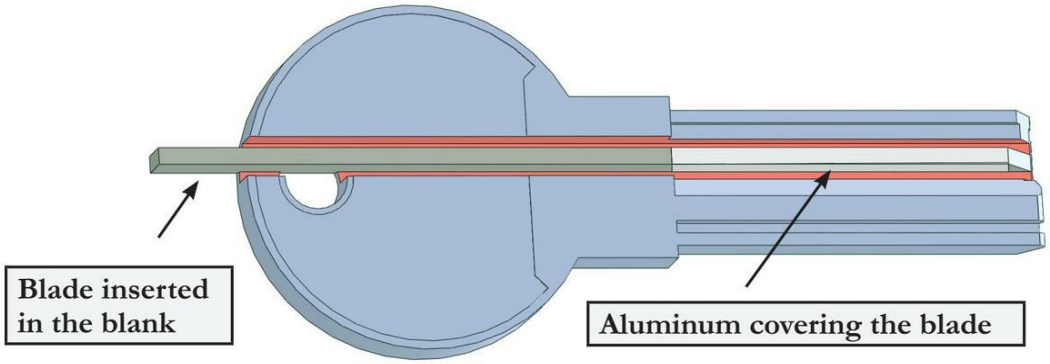


Step 2: prepare the blade

Insert a removable metal blade where the blank blade used to be. Its height and width must be the same as those of the original blade and it must have a pointed tip to push back the pins when it is inserted.

Then cover that new blade with thick aluminum foil at the pin location and check that you can slide the metal blade out of its aluminum cover.

Inserting an aluminum-covered metal blade into the prepared blank



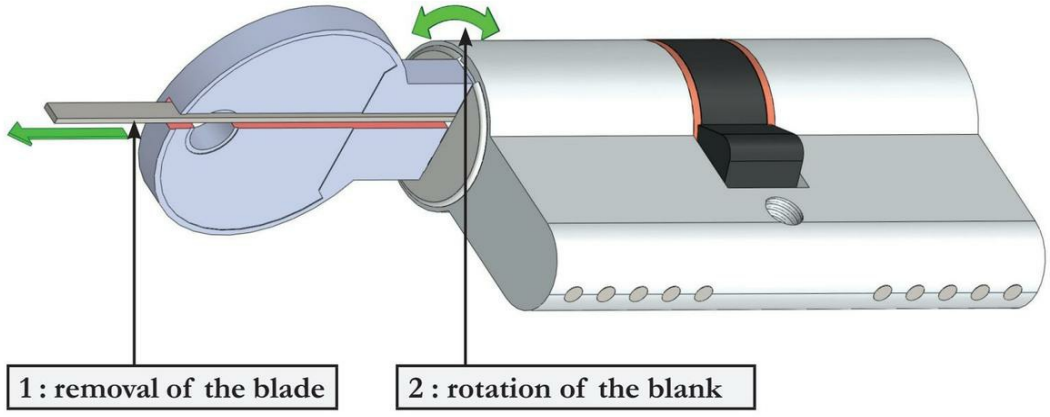
Step 3: finishing off the foil-impressioning process

Once you have prepared the blank, hold the blade firmly in position in the keyway and insert the blank into the cylinder.

Then remove the metal blade inserted in the blank so that only the aluminum remains in contact with the pins and rotate the blank a few times right and left to operate the self-impressioning of the key.

As a general rule, it will be impressioned in less than a minute because the structure of the blade, which consists solely of one thickness of aluminum foil, changes shape very quickly, depending on the stress exerted by the pins.

Opening a dimple lock by foil-impressioning



Notes and additional information about soft keys

Although soft keys are extremely useful because of the speed with which they can open some complex dimple locks, this technique is still quite tedious to use, because it is not always easy to prepare the blank.

Don't forget that it is usually impossible to decode and copy a soft key once it has been removed from the lock.

Another disadvantage of soft keys is that they do not work easily when the key bitting is too deep or too shallow.

This is because self-impressioning requires the superfluous material from the blade to move into the keyway, but the keyway usually fits tightly against the blank.

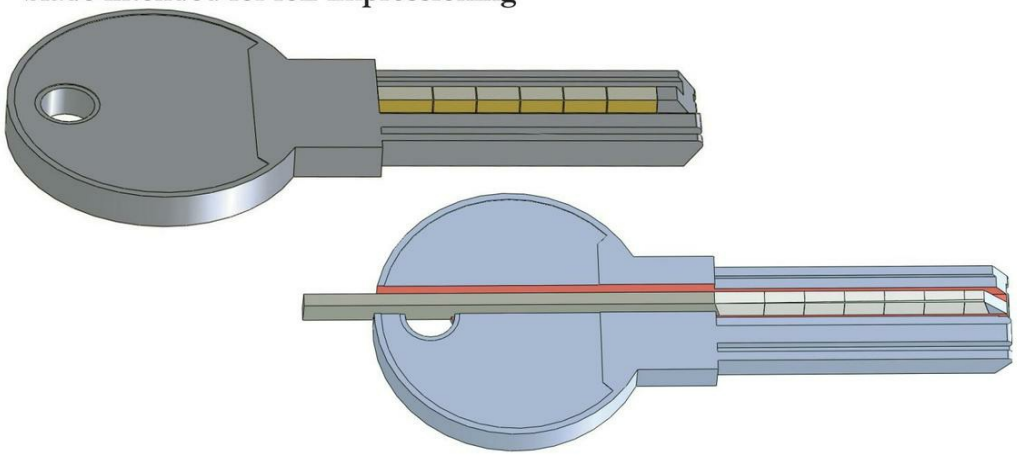
As a result, there is not always enough room for the soft material to be extruded from the blade and form the bitting for deepest cuts.

Therefore, to resolve this problem, it would be best to lightly file the surfaces of the blank adjacent to the blade to leave more room for the soft material to be extruded and form the key bitting.

Similarly, the marks made by a pin on the key blade may transfer over onto the imprint of the next pin and distort the key bitting.

That is why it is sometimes a good idea to cut the soft material into as many "portions" as you have pins. Consequently, if one portion is distorted, this will not affect the other portions of the blade.

Incisions made in a key blade intended for self-impressioning and in a key blade intended for foil-impressioning



If, despite the incisions in the soft material, you are unable to self-impression the targeted lock, it may mean that one of the teeth of the key is actually too deep to be formed in this way.

In practice, we often see that the deepest hole in a dimple key almost goes right through the key.

To work in this configuration, soft keys would have to be machined so that a full cut can be made at the key blade, which would pose a major problem with regard to the strength of the blank, especially because the blank has to be wiggled inside the plug to self-impression the lock.

Conversely, a "zero" cut pin is also a problem, because the soft material tends to become slightly deformed on insertion, potentially making the key bitting too low at this location. The problem can, in some cases, be remedied by applying a "cold spray" to the blade just before inserting it, to temporarily "freeze" the wax to harden it when it is inserted into the lock.

So if you are trying to open a lock by self-impressioning, and your attempts are unsuccessful, switch to impressioning or lockpicking instead, since one or more pins are probably in the minimum or maximum position and this is the reason for the problems mentioned above.

Chapter 19

Bypass methods

Although the main goal of this book is to study the different non-destructive methods of lock picking encountered by opening professionals, some security systems can also be bypassed by opening them without causing any damage and without even having to use special tools to simulate a key.

These methods, known as "Bypass" methods, can be divided into two categories:

1. Techniques aimed at directly reaching the blocking components of the lock (deadbolt or spring bolt), without having to tackle the security devices that usually operate them.

2. Techniques that take advantage of a major security flaw in the closing device, which allows it to be opened via a non-destructive method, without having to pick the lock.

That is why this chapter includes several bypass techniques that are designed to avoid destroying or picking the devices targeted.

1) Opening day-latched doors

The best-known bypass technique is without doubt the "X-ray film bypass" method used successfully by most professionals worldwide to open a door that has been closed but not locked.

In this case, rather than trying to deal with the cylinder, the operator pushes the spring bolt back by sliding a piece of X-ray film or a metal strip into the door rebate.

As the spring bolt is beveled, inserting X-ray film pushes it back into its housing, freeing the door and allowing it to open.

To use this technique, **the X-ray film must be slid at an angle from the top or bottom of the door**, where the gap is usually wider and then gradually slid along until it comes into contact with the spring bolt on the lock. At this point **it is best to push the X-ray film flat against the spring bolt.**

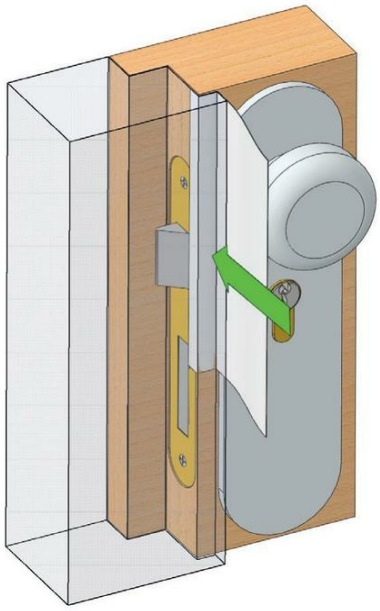
When the door is fitted with anti break-in angle plates, you would be well-advised to lubricate your X-ray film to allow it to move more freely in the gap.

1. **Flexible X-ray film pressed against the bolt**

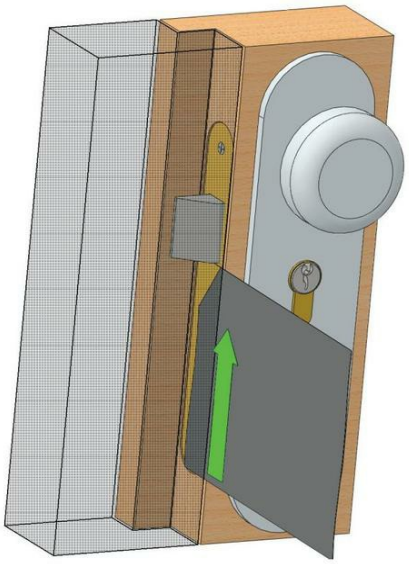
Firmly push the X-ray film flat against the spring bolt, ensuring that it is not at an angle and pulling the door repeatedly while steadily pushing the film.

Contrary to popular belief, kicking the door should be avoided because, apart from the bad impression it makes on your watchers and the noise it generates, the door is pushed at the bottom, whereas in fact we need a pulling movement at the lock location.

The spring bolt will then be able to gradually enter its housing, causing the door to open.



2. **Rigid shim at an angle against the bolt**



When the gap between the door and the frame permits, it is preferable to use metal plates rather than X-ray film.

In fact, their rigidity helps to retract the bolt very quickly, as long as they can be inserted into the rebate.

Similarly, a simple rigid wire 1 to 2 mm thick and bent into a Z-shape, can also serve this purpose.

An alternative, halfway between using X-ray film or metal foil, is to use rigid plastic foil that will allow you to apply more force than the X-ray film and give greater flexibility than the metal foil.

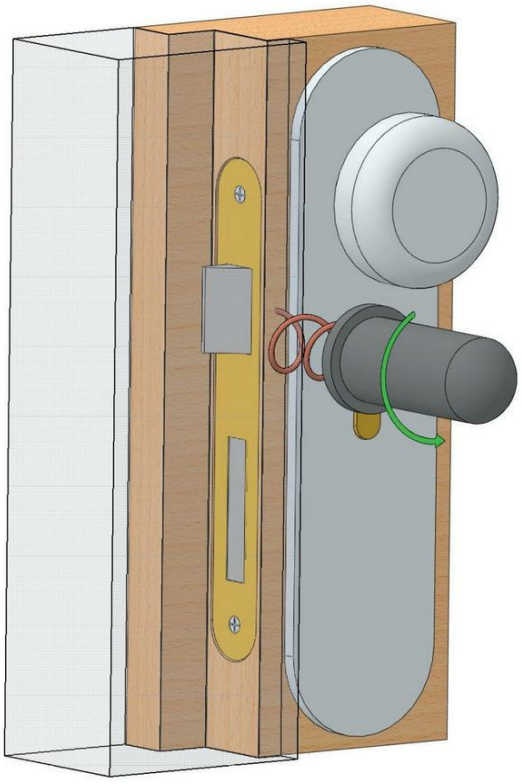
The plastic of soda bottles is therefore perfectly suited to this use and has the considerable advantage of being easy to find in any waste bin. This can come in very handy if you have inadvertently forgotten some of your equipment. But be aware of the impression this may give, as opposed to the use of more professional tools.

Finally, if you have to open day-latched doors regularly, there are other tools that can help you unblock them.

In this case, for example, use piano wire twisted into a corkscrew shape that can be "screwed" between the door and the frame without causing any damage, and is even compatible with most double rebated doors.

3. Inserting twisted piano wire to bypass a single or double rebated door

Using twisted piano wire is probably the most appropriate solution for opening day-latched doors when they have a double rebate or properly adjusted rubber gaskets.



2) Unblocking outward opening doors

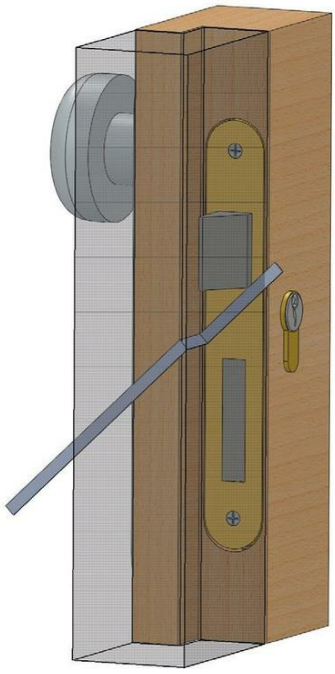
If the door to be unblocked opens outwards, it is more complicated to use the bypass methods to open it.

In fact, to be able to access the bevel of the spring bolt to retract it, you have to go behind it, before bringing the tool back towards you to operate the bolt.

Thin, rigid wire is particularly appropriate for this situation.

Using piano wire to release an outward opening door

After the piano wire has passed through the rebate, it should be placed at an angle beneath the spring bolt and then pulled towards you with a lever effect, so that the spring bolt goes back into its housing.



3) Bypassing panic doors

When you are confronted with an outward-opening door to a building that is open to the general public, it is highly probable that it is a panic door, with a bar on the inside that can be opened by simply pushing the bar.

In this configuration, the simplest solution for unblocking the door is to drill a hole in the metal door plate, by the bolt, then insert a bent wire that will hook onto the bar and simply pull it towards you to activate the panic bar and open the door.

4) Unlocking day-latched doors without accessing the bolt

If you do not manage to unlock the door by pushing back the bolt, several additional solutions are possible.

However, they require the use of destructive techniques that are not the subject of this book and we will therefore only mention them briefly.

One technique involves unscrewing or pulling off the pull handle (or blind plate) to see if you can access the square end of the handle.

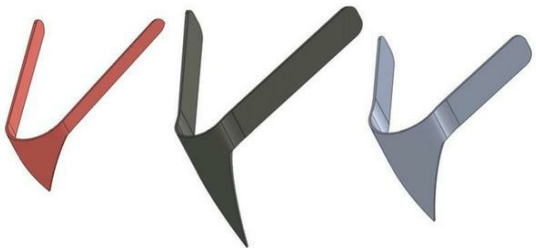
If you can access it, just grasp it with some pliers and turn it to open the bolt.

If you cannot access it, you can also use an under-the-door tool, that will, as its name states, go under the door to manipulate the handle from inside the room. It is particularly effective in offices and hotel rooms.

5) Using shims to open padlocks

Similarly, the X-ray film method can be applied to some locks with the help of shims, i.e. metal blades cut into the shape of a triangle that can be bought commercially, or aluminum cut from soda cans with a pair of scissors.

Three padlock shim models



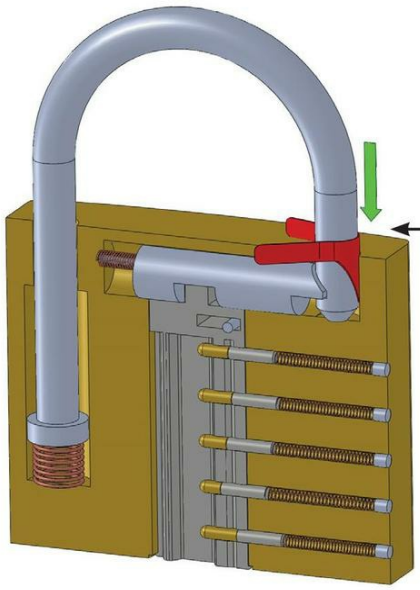
To open a padlock, the shim is slipped between the shackle and the body of the padlock and then rotated around the shackle to retract the bolt.

The major disadvantage of this technique is that it only works "easily" if the target padlock has only one locking bolt, which is now less and less frequent.

However, when working on relatively old or bottom-of-the-range padlocks, you will only waste a few seconds trying this technique, which will sometimes allow you to almost "miraculously" open a padlock. You can also open double-bolt padlocks with two shims, even though the chances of success are lower.

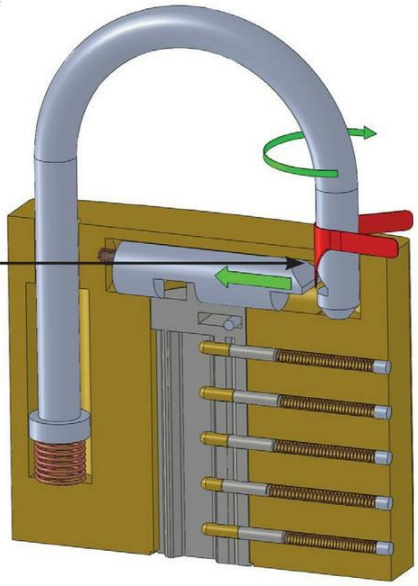
Illustration of the shim technique

Step 1: insert the shim



If the clearance between the shackle and the body of the padlock allows, insert your shim from the outside of the shackle, pushing it down as far as it will go.

Step 2: rotate the shim and open the padlock



When you have inserted the shim, rotate it around the shackle of the padlock, toward the inside of the shackle, and force it to retract the bolt of the padlock when you encounter resistance. If you are successful, the padlock will open.

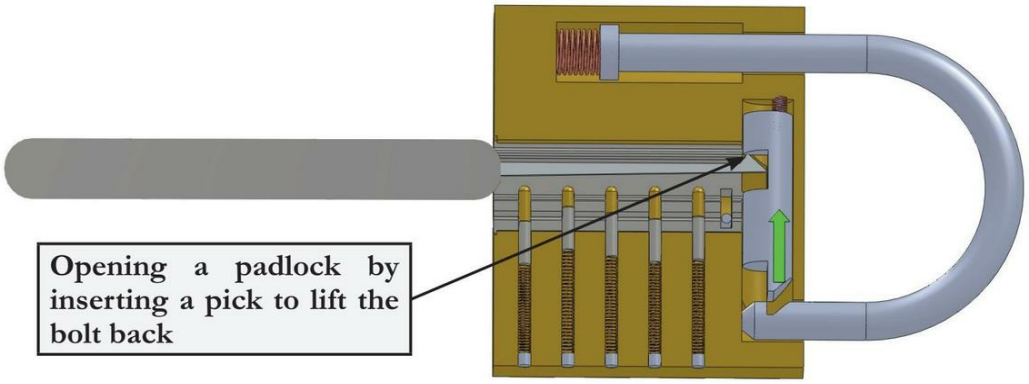
You can help it by pressing the shackle down as well (releasing the friction on the spring bolt)

6) The Silly Technique: Bypassing a padlock through the keyway

I call it the *Silly Technique*, because it really shouldn't exist such an easy way to open a padlock without the key, and it's silly manufacturers still produce padlocks with this flaw.

Some padlocks that have only one locking bolt can be opened by "catching" the bolt inside the keyway with a strong, pointed pick.

Opening a padlock through the keyway



As with shims, the disadvantage of this technique lies in the fact that modern padlocks are often protected against this security flaw by using two bolts instead of one.

Once again, when you are working on poorly designed padlocks, you will never waste more than a few seconds trying this technique, which will very quickly succeed if the padlock does not have protections against this type of bypass.

7) The comb technique

This method, which is particularly suitable for padlocks, is halfway between lockpicking and bypassing.

It takes advantage of a major design flaw in some padlocks and locks that would be easy to overcome by lock makers, but which is found in locks and padlocks from major manufacturers, including some top-of-the-range ones.

Operating principle of the comb technique

The comb technique simply consists in inserting a comb-shaped tool, whose spacing and number of teeth correspond to the spacing and number of pins inside the lock.

Set of combs for dealing with the majority of cases encountered

When the teeth of the comb come into contact with the pins, the comb is moved downward in the keyway to push the key pins back into the shell, while the tips of the teeth reach the shearline.

When this has been done, there is nothing else to prevent the plug from turning.

Using this method obviously requires a combination of two parameters:

1. There must be enough room in the wells of the shell for them to accommodate the spring, the driver pin and the key pin, which is why this technique is often more suitable for padlocks than for cylinders, because the depth of the wells is generally proportionally greater.
2. It must also be possible to insert into the profile a comb with teeth that are long enough to reach the shearline. This excludes many keyhole profiles that are not straight enough to slide a comb into and move it downward.

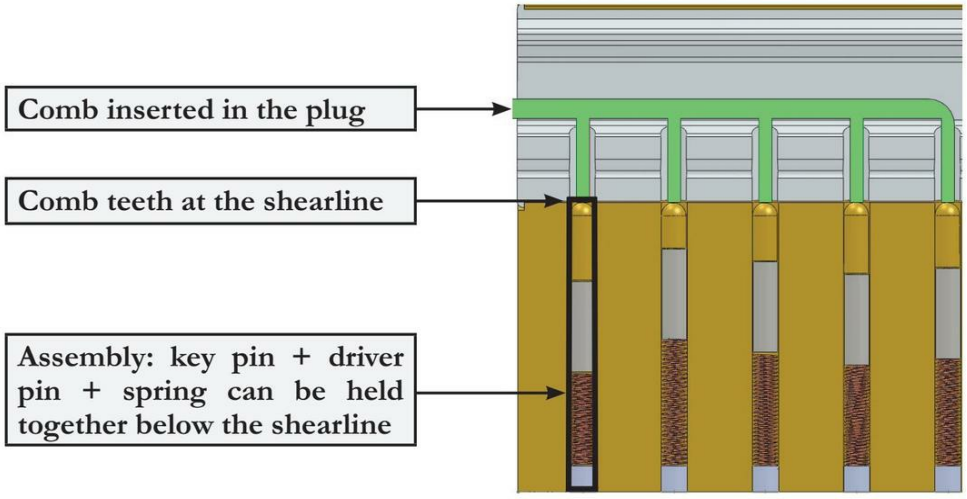
Large padlocks are therefore the preferred targets for using combs, because the wells are very deep in proportion to the diameter of the plug (the useful length of the pins). In addition, the profile is generally large and rather straight.

This technique can also be used to open some top-of-the-range regular pin tumbler locks, which would otherwise take a long time to pick, due to the many anti-pick features they contain.

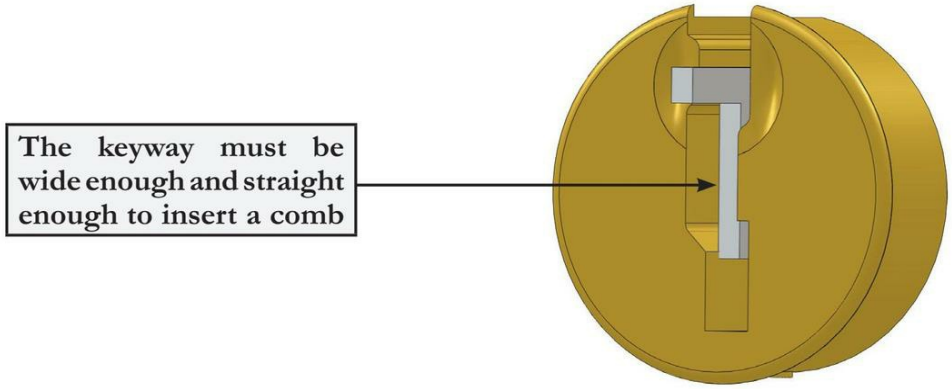
Note: the chances of this technique being successful sometimes depend on the pin setting in the target padlock or lock. A given model may therefore be susceptible to the technique in certain cases but not in others, depending on its key bitting.

Conditions for using a comb

Condition 1: the wells must be deep enough to accommodate the springs, driver pins and key pins



Condition 2: the key profile must have enough room and be straight enough to insert the comb



If you are going to use this technique on a regular basis, you will need several models of combs with a varying number of teeth, varied spacing and of different heights that can be used on different models of locks or padlocks.

Commercially available comb kits are, in this respect, highly suitable and include most of the pin spacings encountered in locks that can be "combed".

If you wish, you can easily make your own tools with hacksaw blades, using (for marking purposes) an empty plug corresponding to the profile for which you want to make your comb.

To do this, start by inserting a metal blade into an empty plug and mark the location of the pins with a pointed tool.

Then cut out the metal from the unmarked area until the teeth of your comb are flush with the plug, ensuring that all the teeth are the same height.

Procedure for opening a lock or padlock with a comb

Once the comb is inserted, and after moving the key pins down below the shearline, your comb can, in theory, be used as a simple key, by exerting a rotary force to open the padlock or lock targeted.

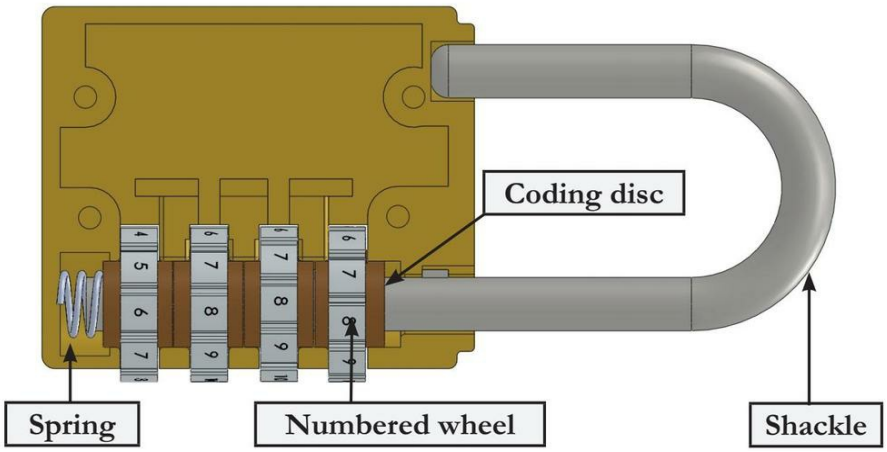
It is, however, preferable to use a tensioner to turn the plug, because the thinness of the comb often makes it relatively fragile and your combs could break after they have been rotated a few times.

8) Decoding combination padlocks

Still between lockpicking and bypass techniques, we will now look at some of the methods used to quickly decode combination padlocks.

However, before going any further, let's start by looking at how these padlocks work in practice:

Sectional view of a combination padlock



Shackle

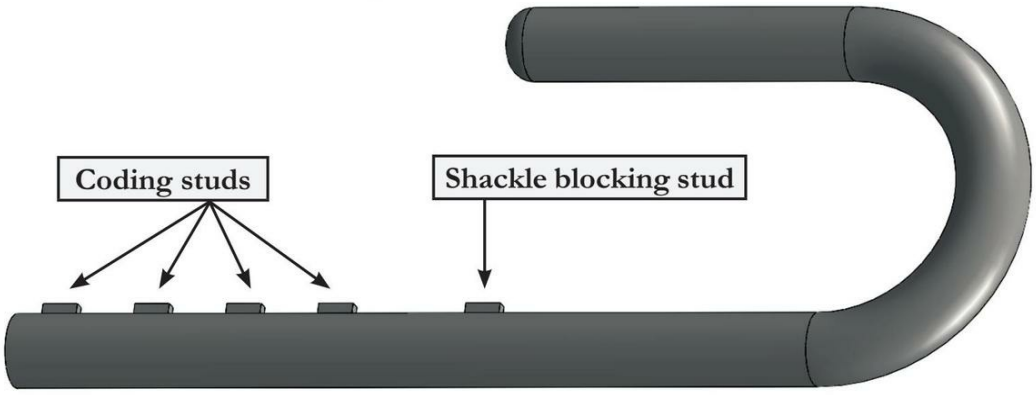
The shackle of a padlock is a moveable part, usually made of hardened steel, and it is designed to lock a system.

On combination padlocks, the part of the shackle remaining inside the padlock is fitted with as many studs as there are numbered wheels.

The studs are protruding pins aligned on the same axis and arranged at theoretically identical intervals along the shackle of the padlock.

As with the alignment of pin wells in a lock, these intervals are, in reality, not perfect, as shown in the diagram below. One of the techniques used to decode such padlocks is based on this imperfection.

Shackle of a combination padlock



Coding discs

The axis of rotation of the coding discs inserted in the numbering wheels is the shackle of the padlock.

The discs have several protrusions on the outside that allow the discs to engage with the numbered wheels.

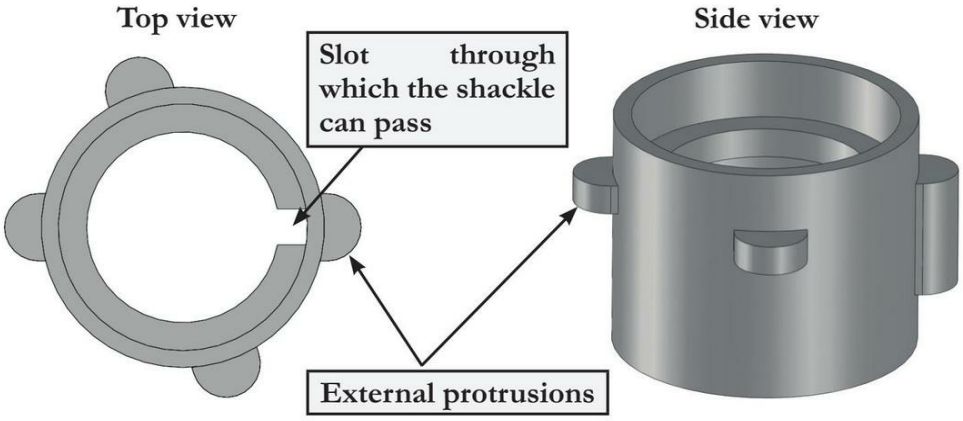
One of these protrusions is higher than the others: it allows you to change the padlock code when the padlock is open and the shackle is pressed down.

The system acts as a guide and allows the numbered wheel to be disengaged from the protrusions on the outside of the coding discs while the code is changed, and the coding disc and its corresponding numberer wheel can then be re-engaged once the new code has been selected.

The coding disc has a slot on the inside through which the stud can pass when these two components are aligned.

When all the slots in the discs are aligned with the studs, the shackle can be opened or closed.

Coding disc

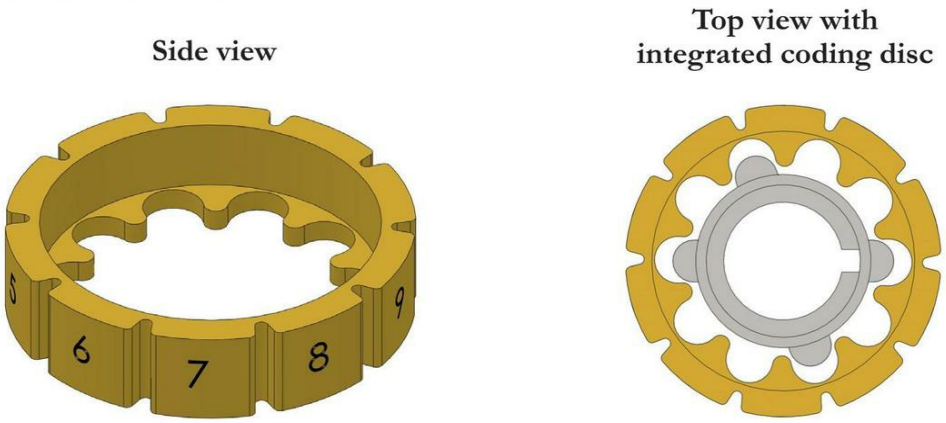


Numbered wheels

The numbered wheels used to set the padlock code.

The inside of the wheel is notched to interlock with the coding discs that fit inside them.

Numbered wheel

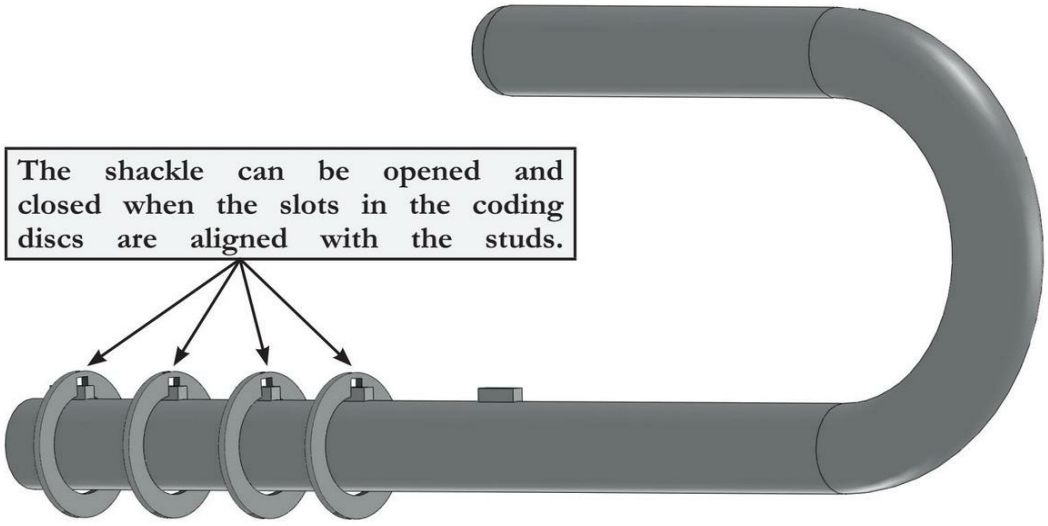


Principle of opening combination padlocks

We will focus on the two parts of the padlock involved in opening it: the studs located on the shackle and the coding discs.

Only when all the inner slots of the coding discs are aligned with the studs on the shackle will the shackle be free to slide along the coding discs, allowing the padlock to be opened and closed.

Schematic diagram of the coding discs position when the padlock is open

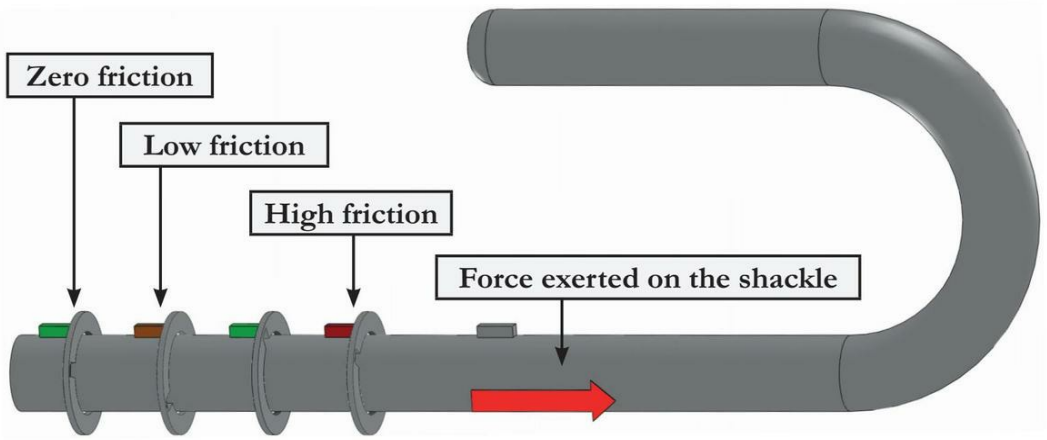


Decoding code padlocks relies on the faults inherent in the machining of the padlock components, which is also the case when picking pin tumbler locks.

In fact, if all the studs on the shackle were equidistant, pulling the shackle outwards while trying at the same time to turn the wheels would generate friction equivalent to all the coding discs on the studs.

In reality, the differences of a few tenths of a millimeter in the spacing between the studs cause some of them to come into friction with coding discs before others, as shown on the diagram on the next page.

Diagram showing friction between studs and coding discs



To open the padlock, you must therefore pull the shackle, while turning the most resistant wheel.

As the shackle stud is in friction with the coding disc, when the slot arrives aligned with its stud, you will feel a slight click as the shackle lifts and the friction slackens for a moment.

Now, move on to the next wheel, i.e. the one that now offers the most resistance, and repeat the same process until all the slots in the coding discs are aligned with the studs: the padlock is now open.

If you do not feel a click, you can use a variation on the previous technique to find when the second wheel becomes harder to turn whenever you test a position on the first.

As soon as it becomes more difficult to turn the second wheel, this proves that the first wheel is in the right position and all that remains to be done is to continue this process until the padlock opens.

There is another technique that can also be used successfully, provided that the models you want to open do not have any special protection.

In this case, simply insert a pin between the shackle and the body of the padlock and then move the pin downward, pressing it against the coding disc.

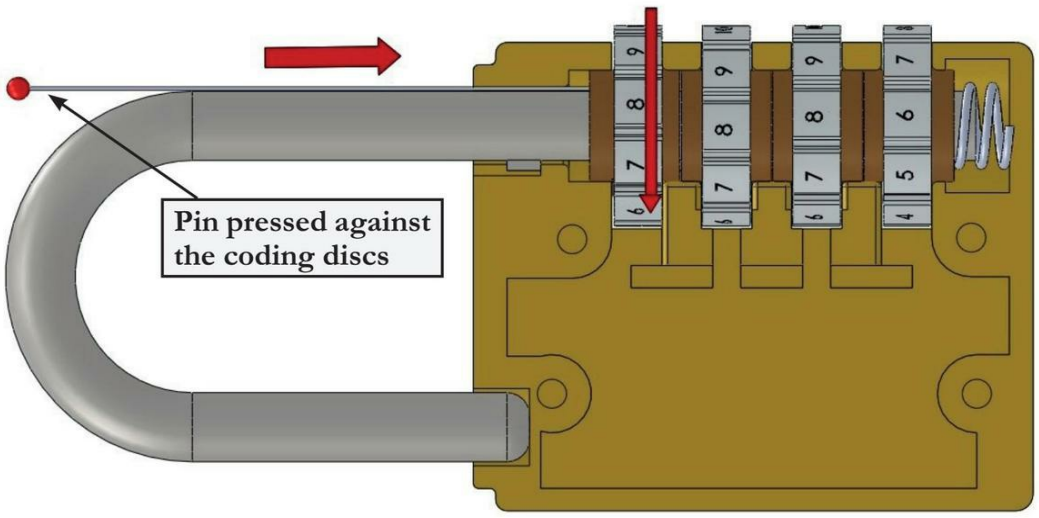
Now use the numbered wheel to turn the coding disc until the pin is aligned with the slot, which you will easily feel, as the needle will be able to enter the slot and pass down to the next coding disc, on which you should repeat this process.

Once the pin can move freely down the padlock shackle, this means that all the stud slots are aligned.

As the slots are aligned with the pin and not with the studs, simply remove the pin and turn all the numbered wheels together, so that the slots in the coding discs are aligned with their respective studs, thus opening the padlock.

This technique is extremely fast and efficient, but more and more manufacturers are aware of the flaw and are inserting washers on top of the coding discs, which prevents this decoding method from working.

Decoding a combination padlock by inserting a pin



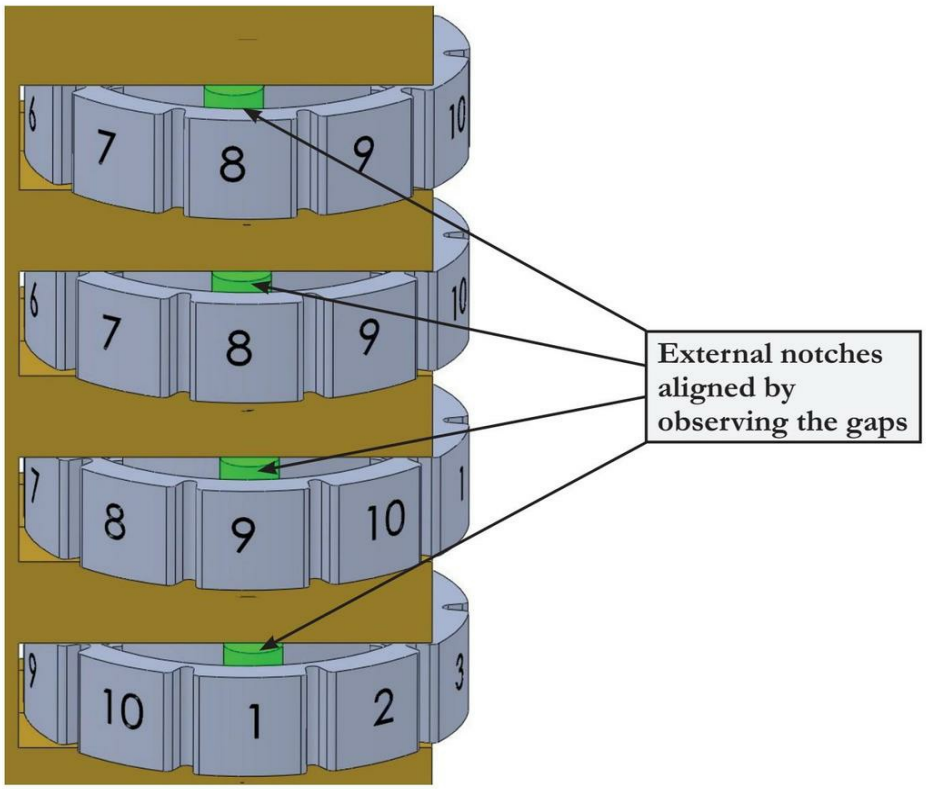
A third technique for decoding combination padlocks involves carefully observing the gap between the body of the padlock and the numbered wheels.

The coding discs located inside the numbered wheels are, in fact, all machined identically.

Therefore, bearing in mind that one of the external notches is higher than the others to allow you to change the padlock code, if you can see this notch by turning the numbering wheels, simply align all the notches on the coding discs so that all the stud slots are also aligned along the padlock shackle.

Then, all that remains to be done is to turn the numbered wheels of the padlock together to finally align the slots with the corresponding studs, which successfully opens the padlock.

Opening by observing the coding discs



Chapter 20

Wafer locks

Wafer locks work on a principle similar to that of pin tumbler locks and are generally found on systems requiring only a low level of security.

You will therefore see them on drawers, cupboards, suitcases, mailboxes, etc.

These locks are also found on medium security applications and more particularly on vehicle doors and ignition.

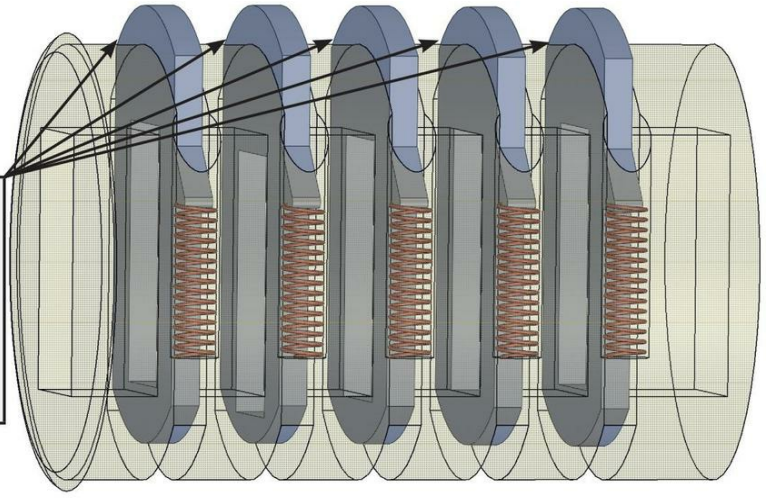
In the latter case, the locks are often of better quality than common wafer locks, but they are still relatively easy to open.

How a wafer lock works

Wafers located inside the lock are metal plates whose height is equal to the diameter of the plug.

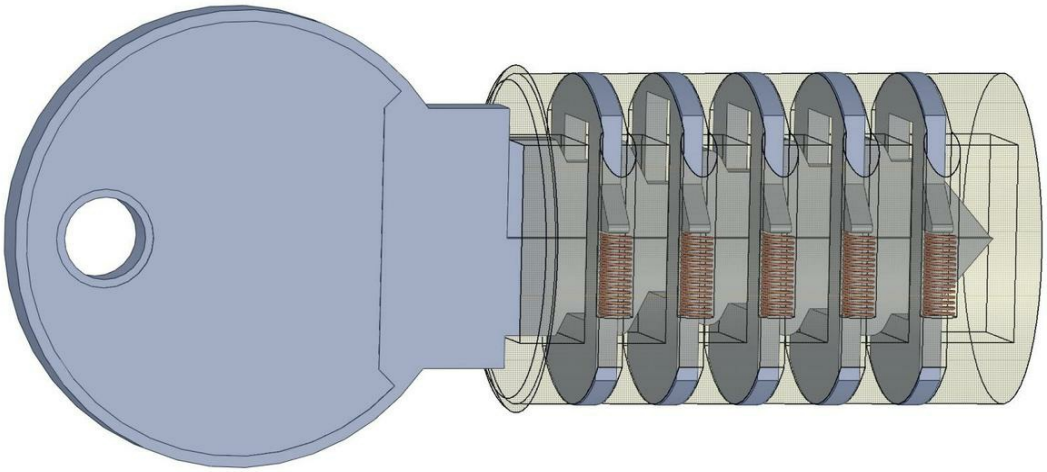
Like the pins, they are double action blocking components, pushed out of the circumference of the plug by springs, so that they partially fit into the shell, thus preventing the lock from opening.

Transparent view of a wafer lock plug at rest



The wafers, pushed by their springs, come out of the plug and enter the shell, preventing the plug from turning.

Representation of a wafer lock with its key



The wafers, constrained by the key bitting are positioned at the plug/shell shearline at the top and bottom, allowing the lock to open.

Wafer lock opening methods

1. Conventional lockpicking

Since wafers work on a similar principle to pins, wafer locks are susceptible to the same opening techniques, except for bumpkeys, which do not really work on this type of lock.

In this respect, the easiest way to pick a wafer lock is usually to use a pick and tensioner, although you can also successfully use the impressioning technique.

Please note that while these locks can be opened by single pin picking, their poor quality usually allows opening them quickly by raking.

However, to make locks more difficult to pick, manufacturers sometimes alternate wafers at the top and bottom of the lock.

In this case, the tensioner can be placed in the middle of the keyway, or must be short enough to be placed in front of the wafers without touching them, as is the case when picking a pin tumbler lock with the tensioner positioned to apply tension in front of the pins.

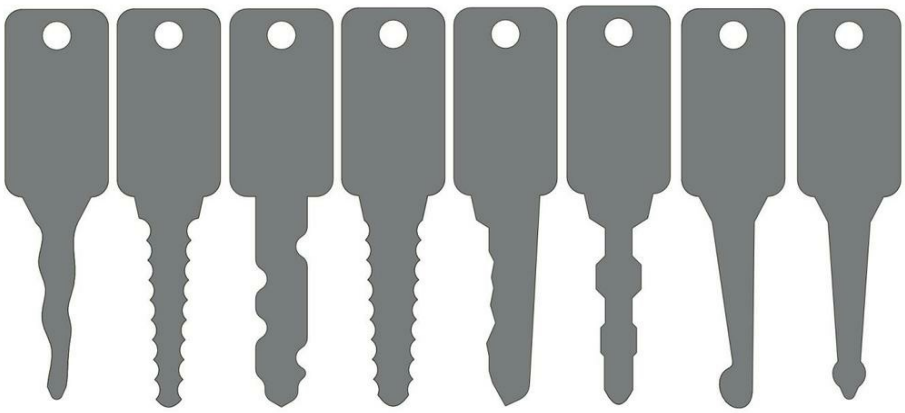
2. Using simulators or jigglers

Due to their manufacturing process, the key profile of wafer locks is often relatively wide, allowing dedicated tools to open this type of locks easily. These tools, known as jigglers, can be used just like a key, without a tensioner.

They are used in the same way as dedicated raking picks and therefore need to be jiggled around in the cylinder, except that the jiggler must simultaneously act as a tensioner. This implies that the back-and-forth movements of the tool are associated with a rotational force exerted on the cylinder.

As jigglers are specifically designed to replicate a maximum number of combinations, you will have to try each jiggler in the lock until it opens.

Set of dedicated wafer lock jigglers



3. Decoding techniques for wafer locks

Even though it is very easy to pick and impression wafer locks, you will find that decoders are useful for your work, especially for vehicle locks when you need to replicate a key.

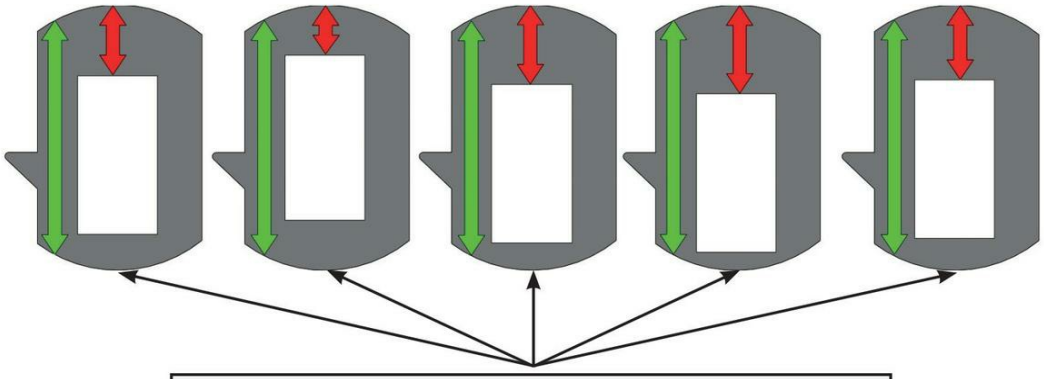
In fact, impressioning, although very effective, takes longer than lockpicking or decoding.

In this context, using a decoder will help you make a new key more easily and more quickly than impressioning, for instance.
Wafer locks are very easy to decode because all the wafers of a given cylinder are the same size and only the openings allowing the key to pass are positioned at different heights.

To use the decoder, it is then only necessary to push the wafer until it comes into contact with the shell to determine the key bitting, either by reading it directly if the tool is appropriate for use with a specific model, or by calculation for a generic decoder.

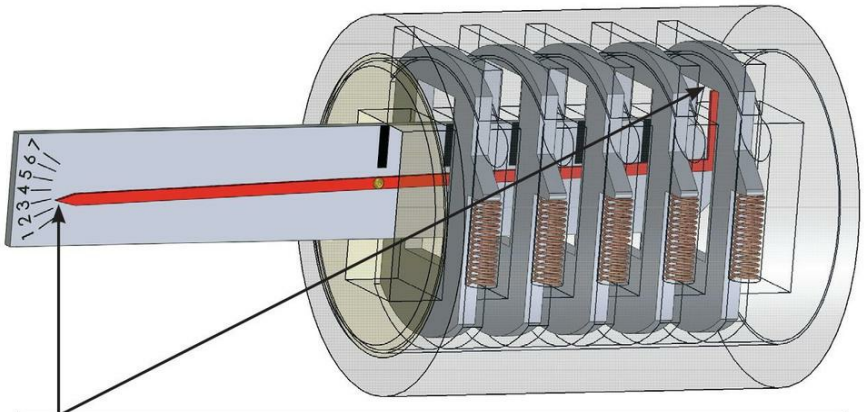
How a wafer lock decoder works

Diagram 1: operating principle



All the wafers are the same size and only the keyhole openings are positioned at different heights.

Diagram 2: using a decoder



The decoder accurately measures the height of each wafer to find the lock combination, allowing you to replicate the key after decoding.

Chapter 21

Lever locks

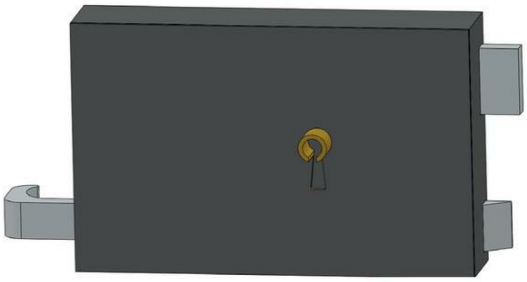
Lever locks are easier to recognize than to open, as they are pretty big locks with long keys with teeth at right angles to the key barrel.

Single-bitted keys have teeth only on one side, whereas double-bitted keys have teeth on both sides.

Single-bitted locks are found less and less in large cities because of the reputedly low level of security of mainstream models, but mainly because of their relatively high price and maintenance constraints (installation, replacement, etc.).

They are therefore more frequently found in the countryside, but they are also found as double-bitted locks in reinforced doors, security cabinets or safes, as they then offer a fairly high level of security.

Single-bitted lock and corresponding key



Double-bitted lock and corresponding key

How a lever lock works

The levers inside the lock are metal plates that prevent the stump from moving if the right key is not used.

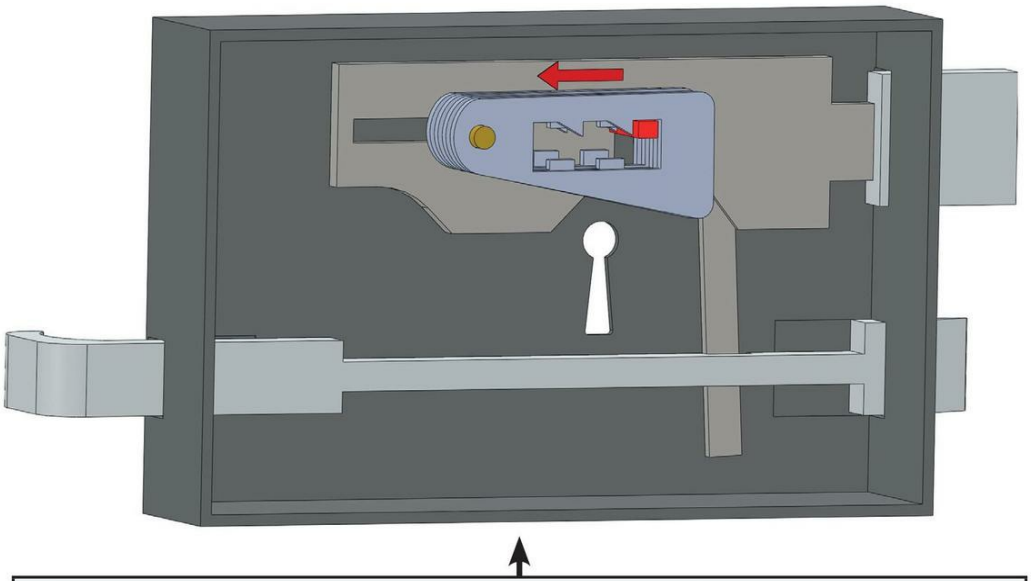
As the stump is fixed to the bolt, it prevents the bolt from moving, as long as it cannot itself move freely through the levers.

The stump is only free to move when the key is turned and raises all the levers to the correct height, allowing the bolt to move and the lock to open or close.

Note that in most cases, one of the teeth on the key is not intended to act on the lock levers.

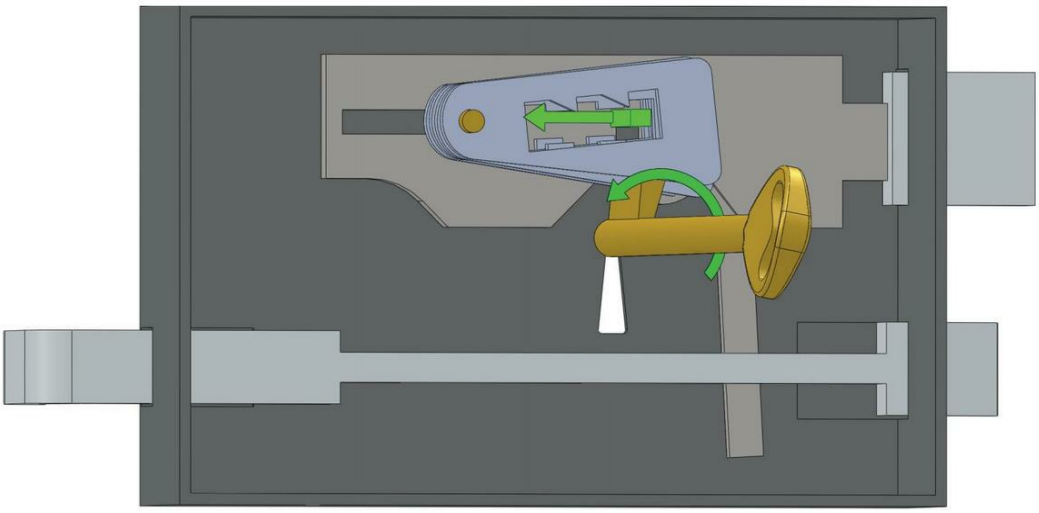
It is simply used to exert a tensioning force on the bolt notch in the opening or closing direction, whereas the other useful teeth align the levers to allow the stump to move.

Sectional view of a lever lock at rest



The stump (in red here) attached to the bolt cannot be pulled back, because it is blocked by the lever alignment, which prevents the lock from unlocking.

Opening a lever lock



When the correct key is inserted, it drives the bolt with the last tooth, while the other teeth raise the levers to the correct height, freeing the stump (in green here).
The bolt is then free to move and the lock can be unlocked.

Lever lock opening techniques

1. "Saint Peter's keys sets"

"St. Peter's keys sets", sometimes erroneously called "Skeleton keys", are sets of a few dozen keys whose bittings have been calculated to simulate a maximum number of existing combinations. You will need several sets to cover the different models of lever locks, depending on the length of the bit, its height and the number of levers.

These sets are very effective on single-bitted lever locks, because they often have pretty large manufacturing tolerances, and very few effective bittings.

They are used as if they were standard keys by generating a rotational movement in the opening direction. However, it is advisable to "wiggle" these masterkeys around in the lock to replicate as many combinations as possible.

Representation of a "Saint Peter's keys set"

2. "Hobbs picks" or two-in-one picks

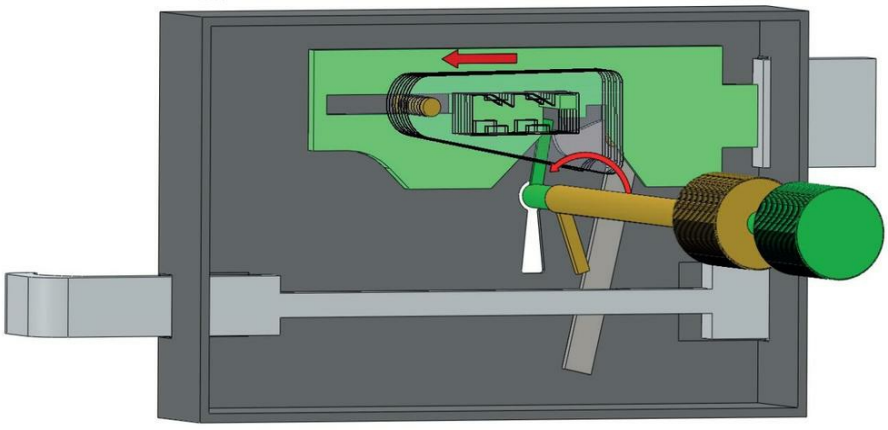
Hobbs picks, which are named after Alfred C. Hobbs, who is thought to be their inventor, are tools that combine a tensioner and a hook, and are used to pick a lever lock in the same way as you would pick a pin cylinder lock.

These tools can be used on both single-bitted and double-bitted lever locks on reinforced doors or safes.

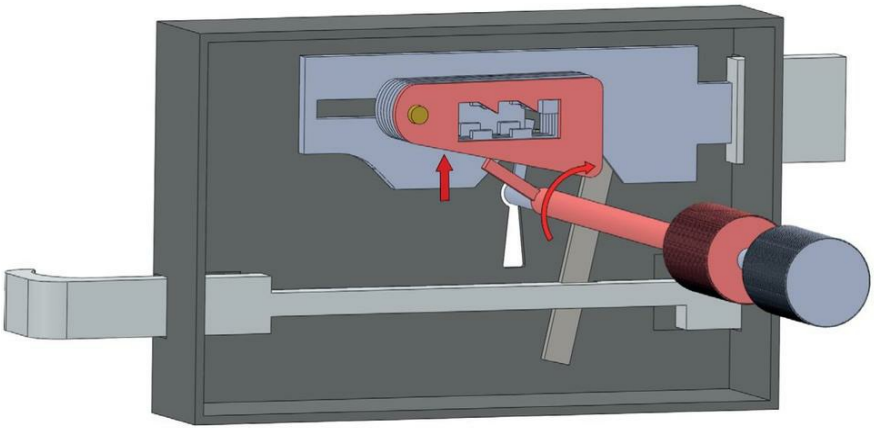
The opening method is similar to that used for single pin picking on pin tumbler locks: tension is applied to the bolt with the tensioner, while the feeler explores the levers and operates them to find the one that binds most and to put it at the right height, thus gradually freeing the stump.

How to use a Hobbs pick

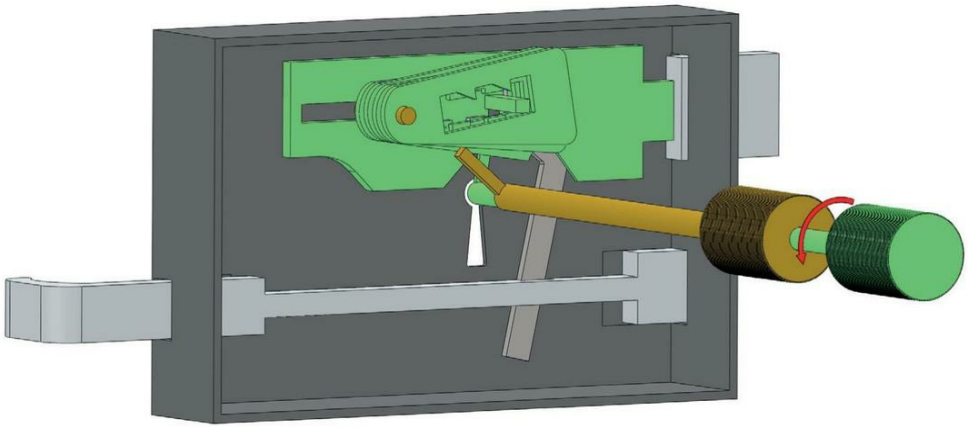
a) the tensioner applies tension to the bolt



b) the feeler gradually aligns the levers to allow the stump to pass



c) when all the levers are aligned, the tensioner opens the lock



3. Impressioning

The equipment and impressioning procedure required for a lever lock are the same as for a pin tumbler lock, except that the file will be flat and thin enough to cut the teeth of the key.

The blank key will be preferably be made of brass so that it will be easier to mark and file. When you are impressioning, the marks will be easier to distinguish if you cover the blank with soot (using a lighter or a candle).

You must, however, be careful to ignore the traces on the tooth that drives the bolt, because it is always marked by the bolt.

4. Self-impressioning

For lever locks, and more specifically double-bitted locks, self-impressioning tools are probably the most effective. They can open even the most complex models in less than ten minutes.

These tools have sliding pins that act as teeth, which are inserted in a key specially made for this purpose with a shank that includes a long screw that makes it possible to tighten the pins.

A separate tensioner is often used, allowing for a precise control of the movements.

The tensioner applies tension to the bolt, which blocks the levers that are not at the correct height.

The vertical movement of the tool pushes the pins in contact with the blocked levers, moving those pins by a few tenths of a millimeter. Tension is released and the process is repeated over and over until the stump passes freely (and the lock opens).

Chapter 22

Warded locks

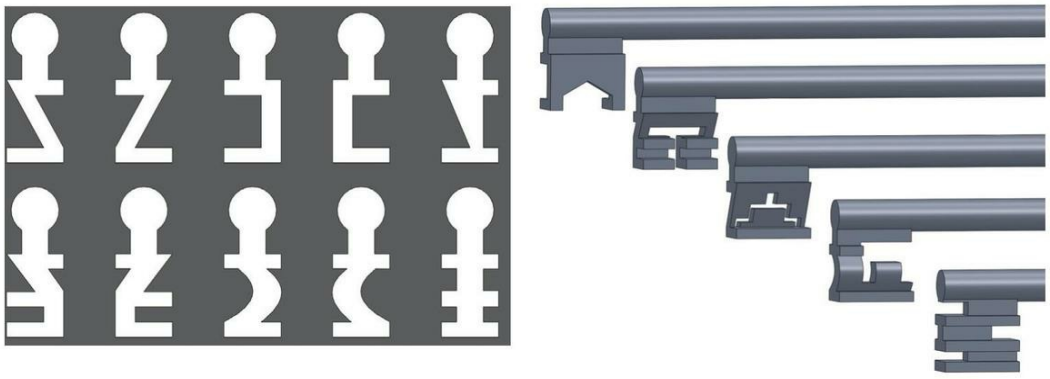
From the outside, warded locks look very similar to lever locks but often differ from them by a more elaborate keyhole profile.

However, these locks have the lowest level of security of all access control systems.

They are frequently used on old doors or basement or attic entrances, but should never be used for security applications.

Warded lock keys are the ancestor of lever lock keys and they can as well be single-bitted or double-bitted.

Representation of keyhole profiles for warded keys and some warded keys



How a warded lock works

The only security features present in this type of lock are internal or external wards, which are actually only physical obstacles to inserting and/or turning the key.

The wards, which are fixed, are therefore single-action components. This means that they do not need to be positioned in a specific place to allow the system to be unlocked (unlike levers and pins, which, let's not forget, are double-action components).

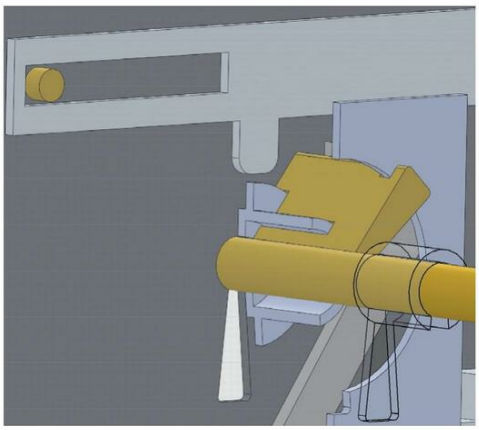
Therefore, when the key does not have the necessary cutouts to allow it to pass through the wards, the bolt cannot be engaged.

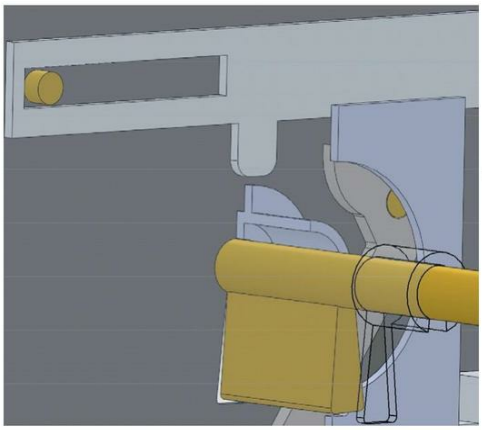
However, if these openings are deeper or wider than necessary, the operation of the key will not be hindered.

In fact, the only action of the key in the lock is to drive the bolt, which is pretty straightforward, provided that the key has adequate cuts to successfully engage in the keyway, which constitutes an external ward, and that it does not come into contact with any internal wards the lock may contain.

Representation of the action of a key in a warded lock

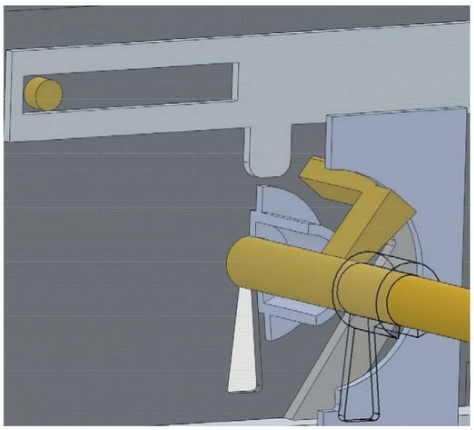
1 : the correct key with the correct cuts can enter the lock and operate the bolt.





2 : a key that does not have cutouts corresponding to the wards cannot be turned and therefore cannot operate the bolt.

3 : a skeleton key can enter the lock and operate the bolt as long as it is not blocked by the wards.



Warded lock opening techniques

As explained at the beginning of this chapter, these locks do not have a very high level of security and can easily be opened by various means, without any need for destructive techniques.

In this respect, the most widely used methods are based on:

- The use of bent wires to operate the bolt
- The use of sets of "masterkeys", also known as "skeleton keys"
- The use of existing keys to be modified to pass through the target wards

Although effective, these methods are often laborious because the locks are often old and hard to handle with a wire, whereas the use of modified keys or "sets of skeleton keys" requires you to have sets of keys for many profiles.

A good alternative to these techniques is to use impressioning, by applying a layer of soot, candle wax, or a thin layer of self-adhesive wax to your blank.

The wards will scratch the surface of the key and then you simply need to file away these marks gradually for the key to eventually be functional.

Impressioning warded locks is child's play compared to impressioning lever locks. In fact, as the wards are fixed, the markings are highly legible.

In addition, since the wards are single-action components used only to prevent the key from entering or turning, the key will work even if the cut is too deep, so you can get away with quick work.

Chapter 23

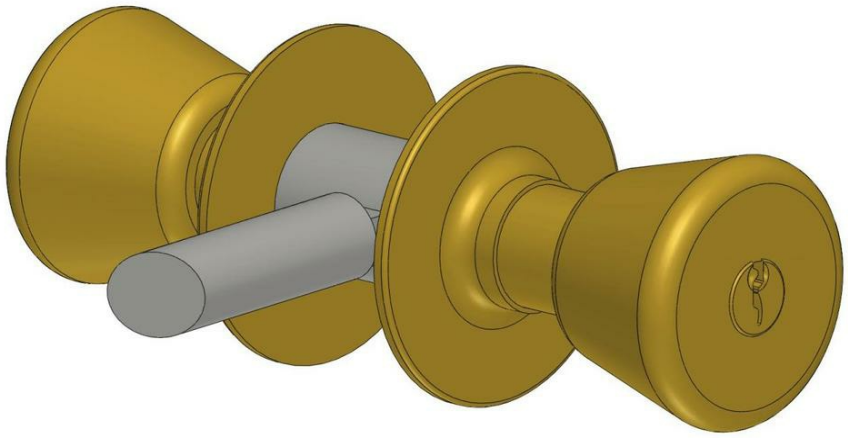
Tubular locks

The term "tubular locks" is often used to refer to two different types of locks: tubular thumbturn locks and tubular key locks.

1. Tubular thumbturn locks

These locks, which are widely used in some areas of the United States as well as in hotels and countryside houses in Europe, are simply regular pin tumbler locks with a plug that is integrated into the door handle.
They are therefore susceptible to the same lockpicking techniques as conventional regular pin tumbler locks.

Representation of a regular pin tumbler lock known as a "tubular" lock



2. Tubular key locks

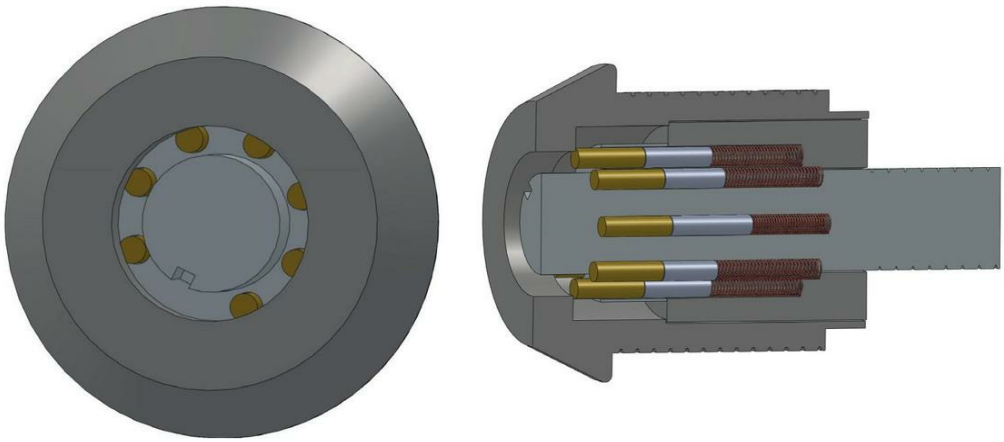
Tubular key locks, which are widely used on anti-theft devices for laptops, bikes and motorbikes, are small pin tumbler locks that can be opened with tubular-shaped keys.

The blocking components of these locks, which operate on the same principle as conventional regular pin tumbler locks, are pins set around a circle that coincides with the diameter of the key.

Even if these locks sometimes have anti-pick pins, they are quite easy to open in most cases with non-destructive methods because, as opposed to a conventional regular pin tumbler lock, all the key pins are directly accessible.

Representation of a tubular lock

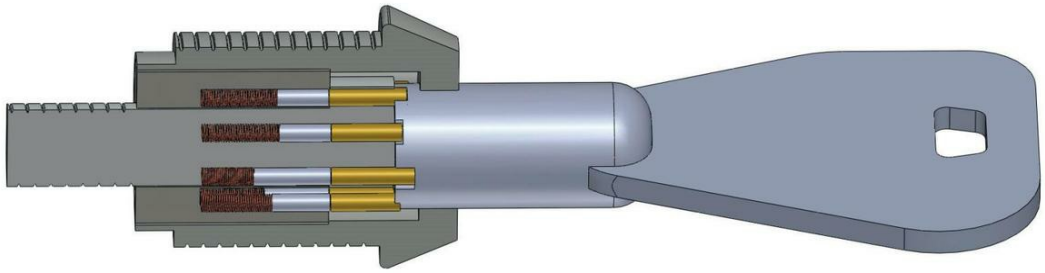
Front view **Side view (transparent)**



The pins blocked in shear between the plug and the shell prevent the lock from opening, in the same way as with a regular pin tumbler lock.

When the correct key is inserted, its bitting at the end of the key allows the pins to be aligned on the shearline and the cylinder to open.

Representation of a tubular lock with its key

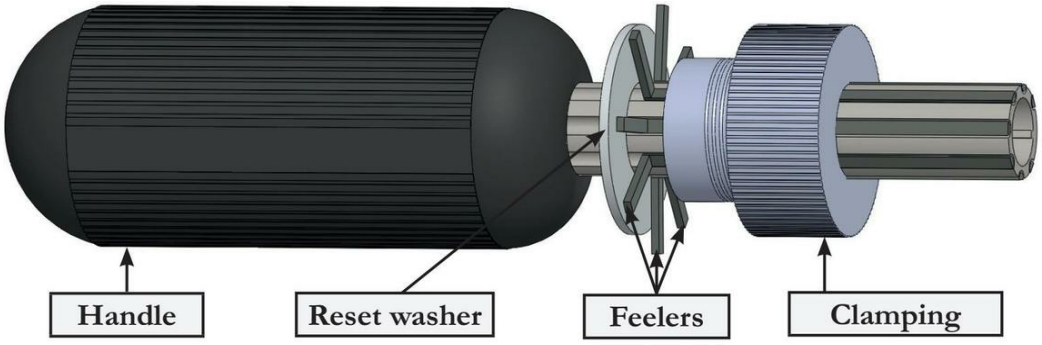


Tubular lock opening techniques

1. Picks for tubular locks

Tubular locks are, in principle, only used for medium security applications because they can be opened quite easily with a special tool known as a "tubular pick" or an "umbrella tool".

Representation of a tubular pick for tubular locks



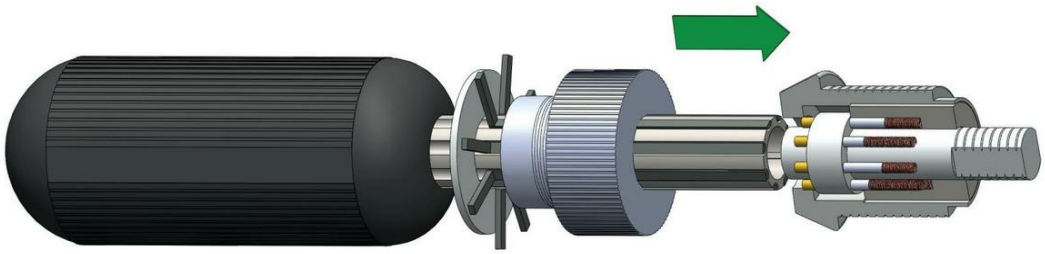
A tubular pick is very simple to use on tubular locks.

However, they require the use of a specific tubular pick that corresponds to the number of pins inside the lock and to the diameter of the plug.

A set of three tubular picks, with diameters of 7 mm, 7.5 mm and 7.8 mm, makes it possible to deal with the vast majority of tubular locks encountered in the field.

To use this tool, a few simple actions will suffice:

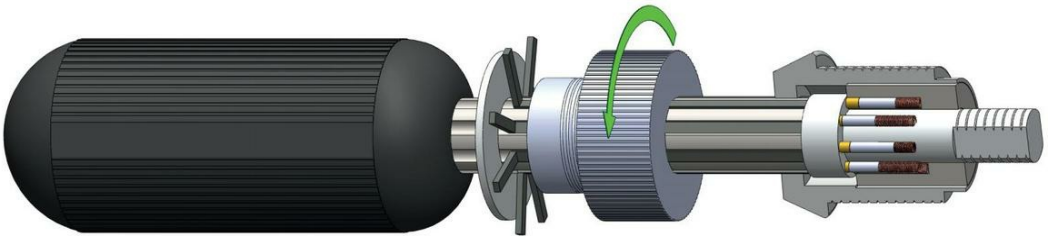
Step 1: reset the feelers and insert the tubular pick in the lock



You can reset the feelers with the "reset washer" which pushes all the feelers to the end of the tool.

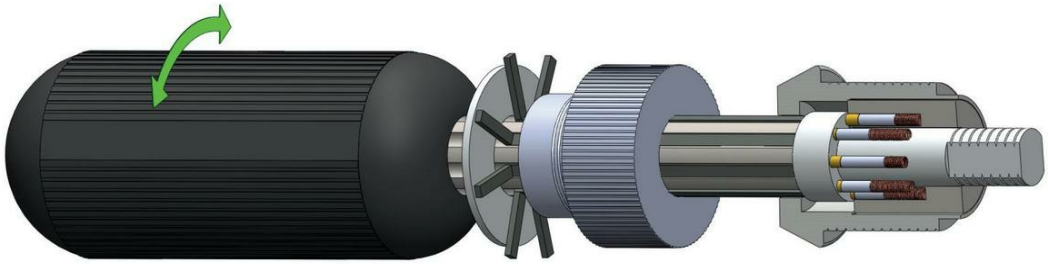
Then tighten the clamping wheel to maintain this position and insert the tubular pick all the way in the lock.

Step 2: loosen the feelers



After inserting the tubular pick until it comes into contact with the back of the lock, loosen the feeler clamping knob to allow the feelers to move under the effect of friction along the body of the tubular pick

Step 3: start self-impressioning



When the feeler clamping knob has been adjusted to allow the feelers to hard slide along the body of the tool, alternatively turn the tool a few degrees to the right and left, which will gradually push the tubular pick feelers back, until the self-impressioning technique allows you to obtain the key bitting.

Step 4: form the bitting by self-impressioning

As with key impressioning on a regular pin tumbler lock, when the pins reach the shearline, they stop pushing back the feelers, which then remain in place.

The bitting is formed gradually without any particular effort, until the lock opens.

When the bitting has been formed, if you carefully tighten the feeler clamping knob, you will be able to make a new key to match the lock.

You can make this duplicate key by decoding the bitting, using a card provided for this purpose, or by simply attaching the tubular pick to the vice of a tubular key duplicating machine, as if it were the original key to be copied.

2. Conventional lockpicking

Besides using tubular picks for picking tubular locks, these can be picked in a more traditional way with a tensioner and a hook, as with any pin tumbler lock.

However, the specific shape of tubular locks will require the use of a special tensioner, which is often difficult to hold in the lock.

On the other hand, although front access to all the pins makes this type of cylinder fairly easy to pick, you should note that whenever a key pin overlaps a driver pin, you will have to repeat the entire lockpicking process.

You will therefore need to pick the lock seven or eight times, depending on the number of pins it contains, to obtain a full rotation.

So, if you do not have a tubular pick, and to avoid having to pick the lock several times, remember to pack the plug with aluminum foil once it has been picked.

Packing the aluminum foil tightly against the pins inside the shell will reproduce the shape of the key and you will only have to insert a tensioner forcefully into the middle of this mass for the plug to rotate freely.

Chapter 24

Pump locks

The name "pump" or "pump effect" comes from the fact that when you insert the key, you feel the force of the spring or springs in the lock that tend to push the key back and serve to reset the tumblers after the key has been removed.

These locks are quite similar to tubular locks because, as with the latter, the correct bitting needed to unblock the lock is formed at the end of the key and the blocking components are all visible and accessible from the keyway.

In reality, pump locks differ from tubular locks only in their presumed higher level of security.

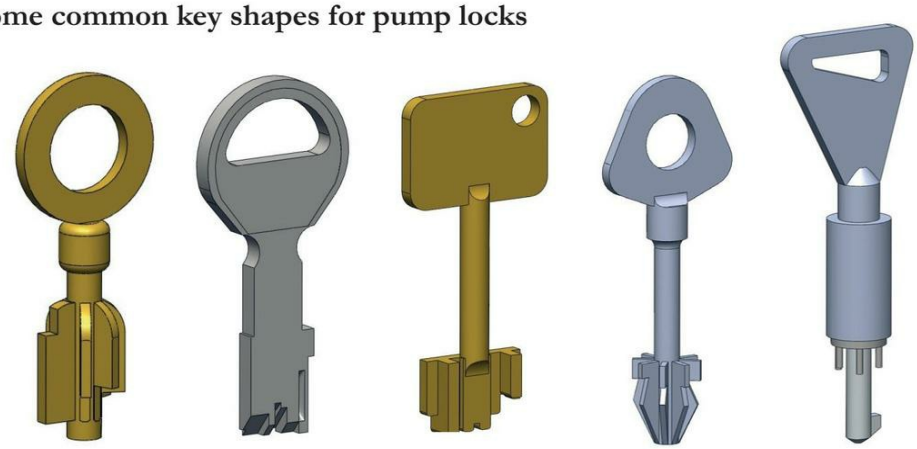
A tubular key lock is actually a simplified form of pin tumbler pump lock, often used for applications that require only a low level of security, whereas a "conventional" pump lock would normally be used for entrances that require a relatively high level of security.

As far as the internal mechanism is concerned, pump locks can be subdivided into three categories:

1. "Pins" pump locks
2. "Sliders" pump locks
3. "Tilting wards" pump locks

Pump lock keys can be round, star-shaped or have a wide, flat tip; they all have in common that the bitting is formed at the end of the key and not along its length.

Some common key shapes for pump locks



1. "Pins" pump locks

These locks are based on the same operating principle as the tubular locks discussed in the previous chapter, to which we invite you to refer to for more detailed explanations.

In fact, although we have chosen to describe tubular locks separately from pump locks, we categorize them this way because we want to grade the security levels of the locks we describe. Given that the machining quality of "real" pump locks is better than that of tubular locks and that they can also be recognized by their key shapes which are different from those of "conventional" tubular keys.

2. "Sliders" pump locks

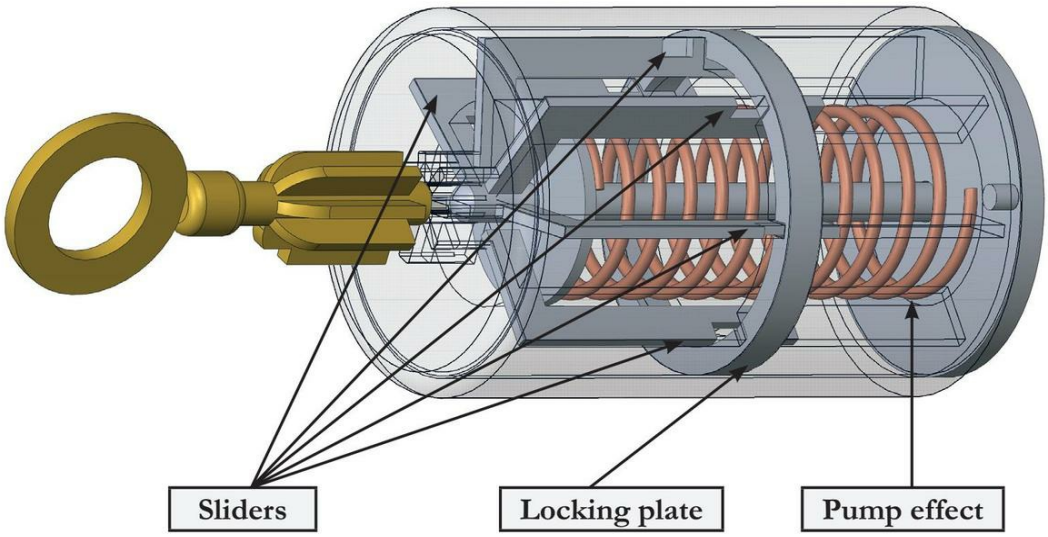
The blocking components on these locks are metal notched sliders. The sliders are made in one piece, unlike the pins which always consist of a key pin and a driver pin.

The metal sliders, which have false notches on the most advanced models, slide when the key is inserted until their notches are aligned with the blocking components known as "locking plates".

It is important to understand that in this type of lock, the locking plates are fixed components that are integral with the shell and circle the plug like a circlip.

If you do not have a key, or if a key does not have the right bitting, the sliders fill the cuts in the locking plates, which prevents the plug from turning, because as soon as you try to turn the key, the sliders stop against the locking plates.

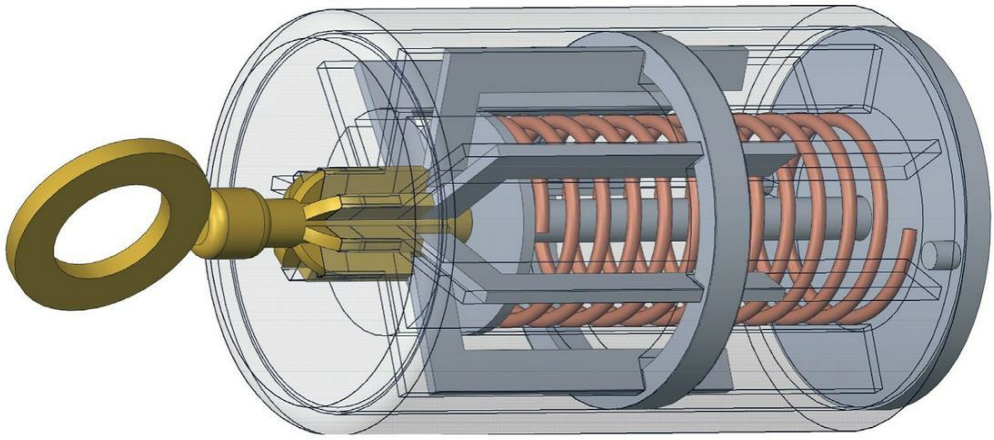
Initial alignment of the sliders with no key inserted



This diagram shows the sliders that sit in the cuts of the locking plate, preventing the lock from opening.

Conversely, when the correct key is inserted, the notches in the sliders are aligned with the locking plates, allowing the plug to rotate:

Alignment with corresponding key inserted



As can be seen in the diagram above, the bitting formed at the end of the key allows the notches on the sliders to be aligned with the openings on the locking plate. The lock can then be unlocked and the plug set in motion, while the locking plate and shell remain stationary.

3. "Tilting wards" pump locks

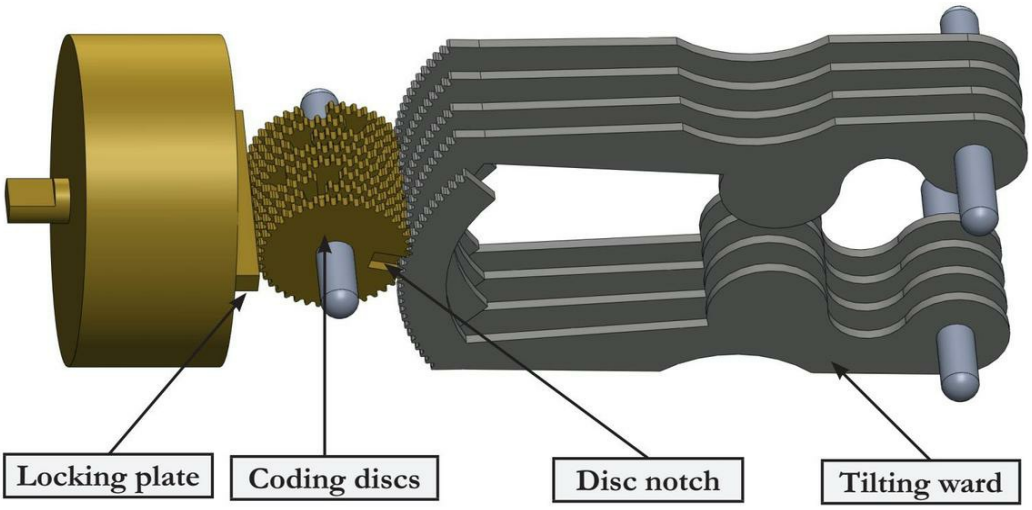
It is difficult to describe these locks because the design of each model is unique. They are, however, still called "pump effect" locks because, when the correct key is inserted, the plug is pushed forward against the action of the return spring.

As opposed to more conventional pump locks, where the components blocking the system are accessible from the front, inserting the key will, in this case, operate a lever or gear system, which will align the blocking components under the spring effect, so that the locking plate located at the back can enter.

These locks have generally an excellent level of security and will very often be difficult to pick using non-destructive opening methods, beacause it is very difficult to feel whether the coding discs are aligned along the locking plate.

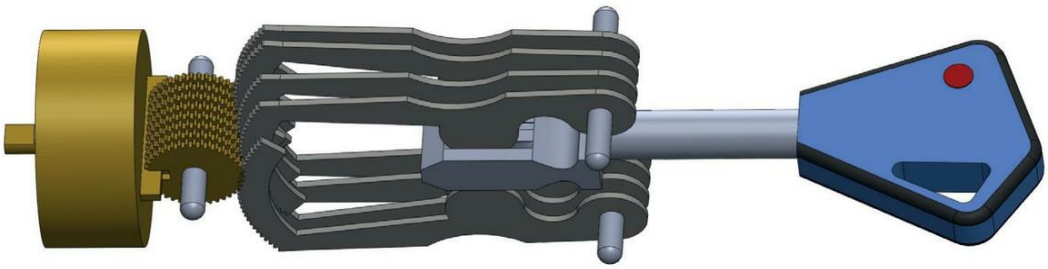
Representation of the internal mechanism of a tilting wards pump lock.

1. Lock in resting position



When the lock is at rest, as in the above diagram, the tilting wards are set to zero by a spring system (not shown, to make the mechanism easier to understand).

2. Lock with corresponding key inserted



As can be seen, each of the eight key cuts presses against the protrusion on one of the tilting wards, which causes it to rotate on its axis, driving the corresponding coding disc which is then positioned in such a way that its notch is aligned with the locking plate.

When all the discs are set, the locking plate is aligned with the coding discs and therefore interlocks with the rest of the plug, allowing the mechanism to be unlocked.

Pump lock opening methods

1. Umbrella tools

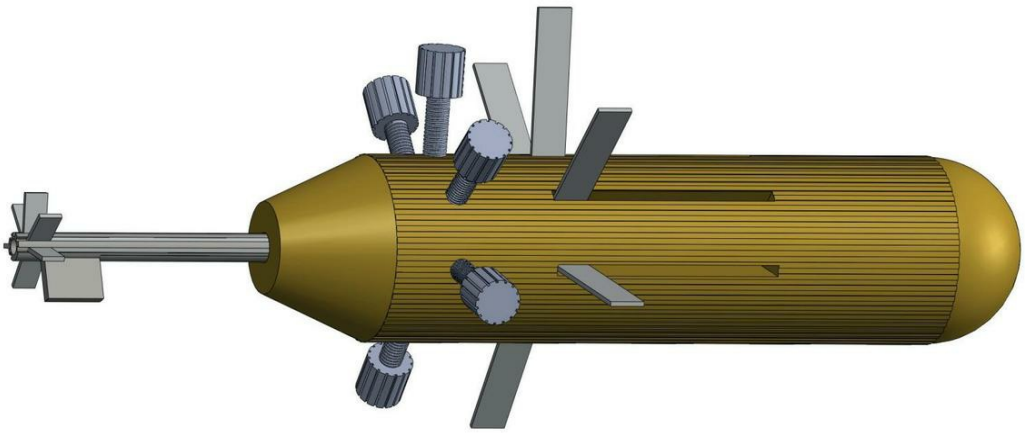
Pump (pin or sliders) locks are characterized by blocking components that can all be seen and accessed from the outside.

Tools that can individually act on each blocking element, without interfering with the others, can be used in this configuration. Umbrella tools are particularly suitable for these types of lock, similarly as for tubular locks.

It is, however, essential for the umbrella tool to be specific to the target lock model, bearing in mind that in most cases, the single-pin picking technique will be needed, using the tool handle as the tensioner, while at the same time using the feelers to position each element.

It can take up to one hour to pick such a lock, depending on its quality, the effectiveness of the umbrella tool and the experience of the operator attempting to open it.

Representation of an umbrella tool suitable for a sliders pump lock



Some umbrella tools can be used for self-impressioning, as in the case of tubular locks, which will be very useful from the operator's point of view, because they will allow the lock to be opened quickly and easily, even by an inexperienced lockpicker.

However, the main drawback of self-impressioning tools is that when it fails to open, very little clues are given to understand why it failed, and how to eventually open the lock. Thus, we highly recommend to avoid self-impressioning tools, and instead use picking umbrella tools, which are far more reliable.

2. Conventional lockpicking

It is, of course, possible to pick pump locks with two suitable metal rods (a tensioner and a feeler).

However, if you choose this option, the circular configuration will require you to pick the lock between 5 and 8 times to complete a full rotation.

Conversely, an umbrella tool will allow you not only to complete one or more rotations without any difficulty, but also to decode the corresponding key, as soon as the lock is open.

That is why a professional wishing to use non-destructive opening techniques on this type of locks would be well advised to work with suitable tools, while the amateur may do with basic, but admittedly, far less effective equipment.

Chapter 25

Disc detainer locks

Using disc detainer locks

These locks are widely used on security padlocks and bicycle and motorcycle security locks.

In fact, in most cases, due to their design, they can only be rotated in one direction, which explains these rather specific uses.

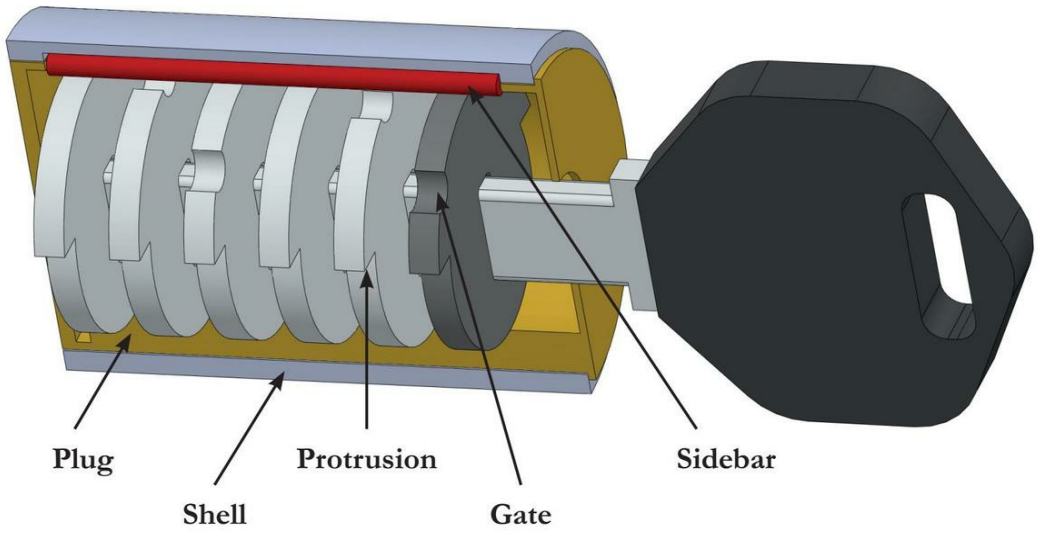
There are, however, a few rare models of top-of-the-range disc detainer locks, which rotate in both directions and are therefore used in conventional access control systems.

How disc detainer locks work

In terms of the design of this type of lock, the plug contains a stack of discs with a notch (also called "gate") and a protrusion on their circumference and a central hole into which the key is inserted.

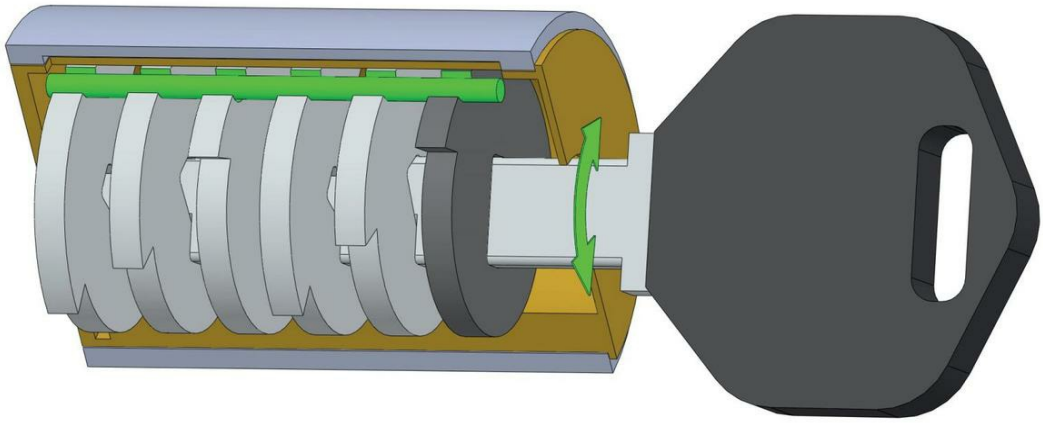
Without the right key, the plug cannot be rotated because a sidebar is blocked between the plug and the shell

Representation of a disc detainer lock in the closed position



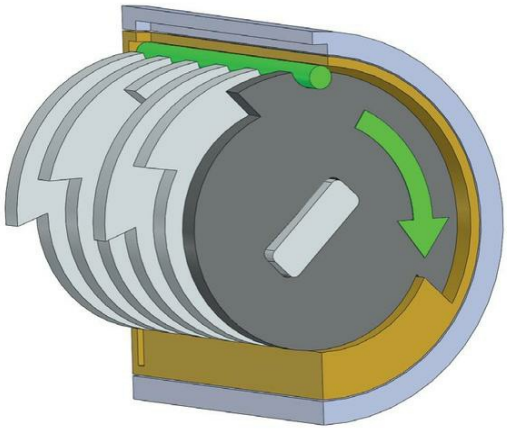
When the correct key is turned, the gates in the discs are aligned to allow the sidebar to drop into them. The sidebar then moves down inside the plug and no longer prevents it from rotating.

Representation of a disc detainer lock with a key inserted and turned



When the key is inserted, a first rotational movement moves only the discs. then as soon as the protrusions on the discs engage the plug, the combination is tested by pushing the sidebar against the discs.
The plug can then rotate as long as the gates are aligned with the sidebar.

Interlocking of the discs and plug when the gates are aligned



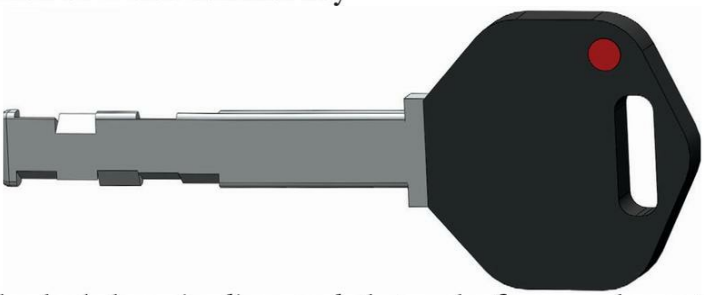
There is therefore always at least one tensioning disc among the discs which interlocks with the plug when its gate is aligned with the sidebar.

The tensioning disc is often either the first or the last disc in the lock.

Before picking this type of lock, you must first determine which is the tensioning disc, bearing in mind that it is often the first or last disc.

To find the position of the tensioning disc, the best solution is to look at a key corresponding to the same cylinder model. The location of the tensioning disc will be indicated by the absence of an angular cutout.

Representation of a disc detainer key



Given that the lock has six discs and that only five angular cuts are visible, we can deduce that the tensioning disc is, in this case, the first disc.

Disc detainer lock opening method

These locks require special tools, which, on the one hand, allow a certain amount of tension to be exerted on the plug by applying constant tension to the tensioning disc, while, on the other hand, allowing the other discs to be manipulated separately to align their gates with the sidebar.

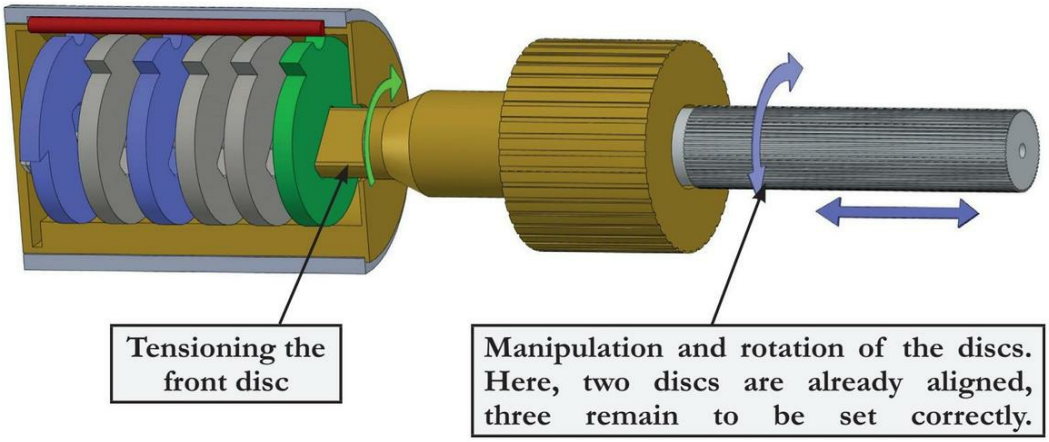
Although it is theoretically possible to pick these locks with two bent wires, dedicated two-in-one tools are generally used.

Representation of a disc detainer pick tool

Obviously, each type of lock requires a tool that is appropriate to the shape of the keyway, the position of the tensioning disc and the number and thickness of the discs present.

Note: the feeler should generally be thin enough to slide between two adjacent discs and move from one to the other.

How to pick a disc detainer lock



The lockpicking procedure is similar to single pin picking tumbler locks: tension is applied to the tensioning disc with the body of the tool and then the feeler is used to manipulate each disc to feel which one "rubs" the most.

For better success rate, it is advised to always turn all the discs by 90° Clock-Wise (with a blank key or a rectangular piece of metal), and pick the discs by rotating them Counter Clock-Wise.

A disc is in correctly set when you hear a "click" and/or feel that there is no more friction on that disc.

The sensations you feel when you pick disc detainer locks are very different from those you feel when you pick pin tumbler locks. They take longer to learn, including bottom-of-the-range models. This also explains why these locks are becoming more and more widespread and are sometimes chosen for high security applications.

In any case, it is advised to use a modular disc detainer pick allowing to tension from the first disc or from the last disc upon need. These are definitely the most versatile tools.

Chapter 26

Magnetic locks

Magnetic locks are mostly intended for high security applications.

These systems differ from all the locks previously studied in that the key is never directly in contact with the blocking components that it merely attracts, repels or positions.

The magnetic components in the lock can be pins, mobile components or magnetized discs, as the key itself is fitted with magnets.

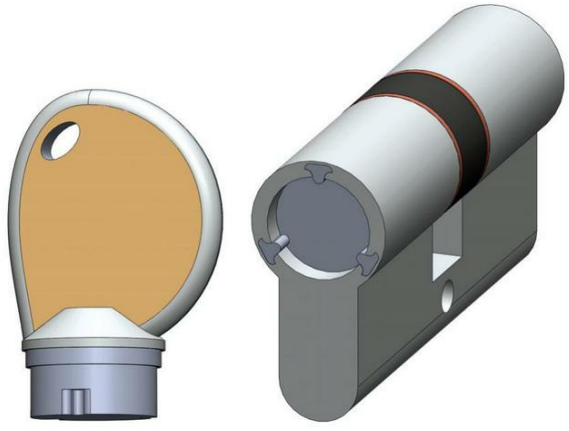
As on other lock models, when the correct key is inserted, the blocking components attracted by the magnets on the key enter the plug to allow it to rotate, or change their positions to allow a sidebar to enter.

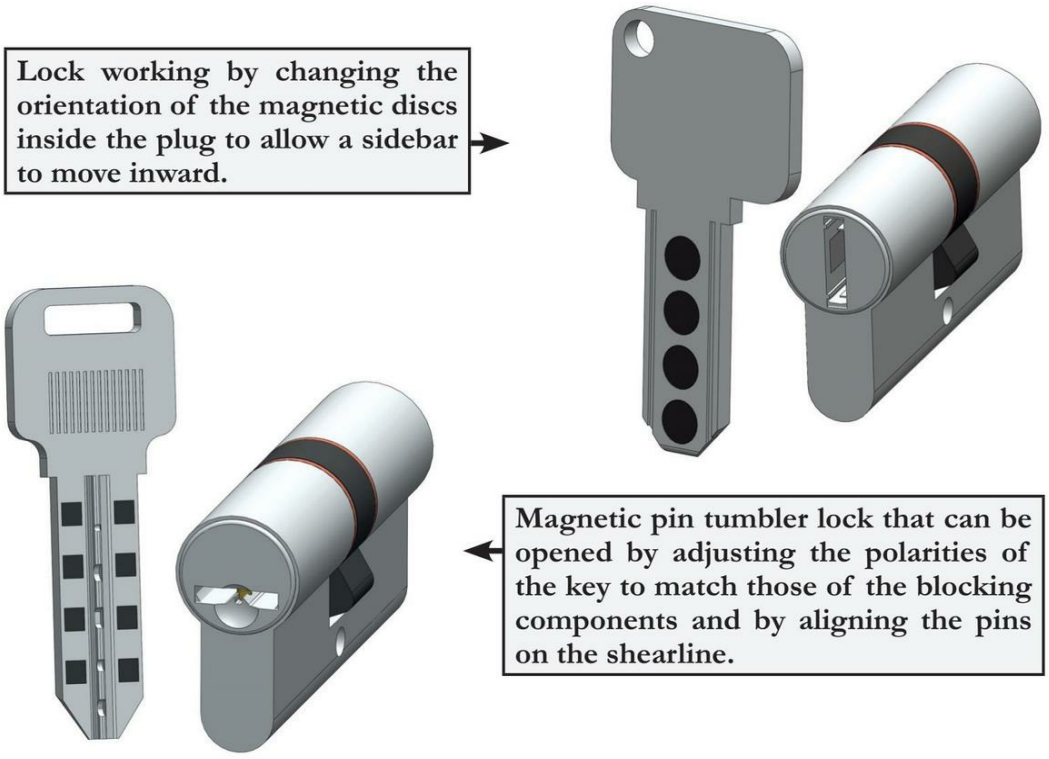
On some models, the combination is achieved by acting in a binary manner on the North or South polarity of the magnets, but there are also more complex models based on the orientation of the magnets inside the plug, or others, reacting to the strength of the magnetic force of the permanent magnets embedded in the key.

The rectangular or round keyway is usually wide enough to allow the manufacturer to make blanks into which magnets will be set, which would be difficult to do with complex profiles.

Representation of the few existing models of magnetic locks and their corresponding keys

Magnetic lock with no access to the inside of the plug. The blocking components are activated when the key touches the surface of the plug and attracts or repels certain blocking components located inside the lock (similar to a tubular lock, but magnetic).





Opening method

Due to the variety of magnetic lock models, there is no universal opening method.

Each model must therefore be treated on a case-by-case basis, starting by determining the type of lock (with pins, discs, sliders, etc.) and then by deducing a method specific to the targeted lock from the opening method for this type of lock.

Picking this type of high-security lock is, however, a challenge, especially as there are no specially designed tools available for opening them available on the market.

It should also be noted that, some magnetic lock models have yet to be picked, which tends to demonstrate the high level of reliability and security of this type of lock.

Chapter 27

Variable position warded locks

Using variable position warded locks

These locks are usually used for applications with a fairly high level of security, due to their manufacturing quality and presumed complexity.

How variable position locks work

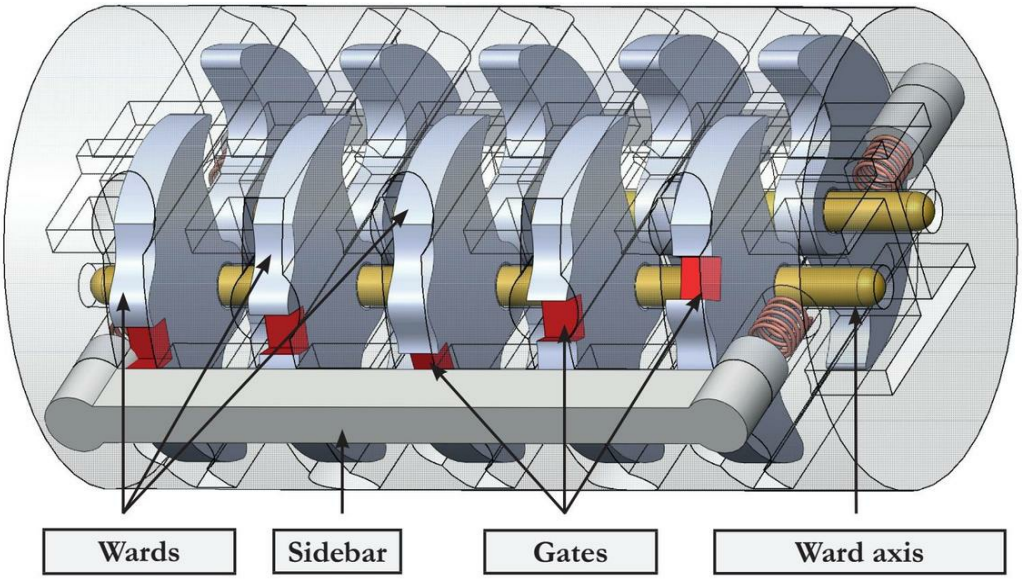
As with magnetic locks, the many varied locks based on the principle of variable position wards makes any generalization on the configuration of this type of mechanism very difficult.

Nevertheless, the operating principle is always the same.
It is based on aligning the ward gates located inside the plug to allow a sidebar to drop into those gates, after being initially blocked between the plug and the shell to prevent the lock from opening.

Sometimes this concept of variable position wards is combined with a traditional pin system or a pump system.

Representation of how a variable position warded lock works

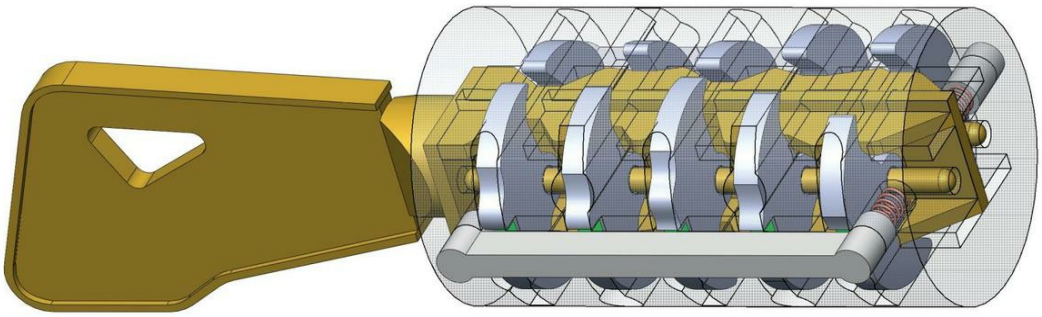
1 : Simplified representation of a lock without a key



As you can see in the diagram on the previous page, if no key is inserted, the wards are positioned by means of a spring system (not shown here to make it easier to see the mechanism).

In this case, the gates are not aligned and the sidebar is caught between the plug and the shell, preventing the mechanism from unlocking.

2 : Simplified representation of a lock with its key



When the correct key is inserted, its cuts tilt the wards until their gates are facing the sidebar, which can then freely enter the plug and allow the lock to be unlocked.

Variable position warded lock opening methods

As with magnetic locks, due to the variety of models, there is no universal method for the non-destructive opening of this type of lock.

Each model must again be treated on a case-by-case basis. Bearing in mind the complexity and machining quality of this type of lock, even if lockpicking with "conventional" tools were still to be considered, only the use of the appropriate umbrella tools for the model targeted will give a useful result, along with impressioning techniques.

Conclusion

I hope that this book has given you a comprehensive overview of the way in which the main mechanical access control systems work and the non-destructive methods that can be used to open them.

Obviously, the non-destructive opening of some high-security locks requires equipment and skills that sometimes exceed your current skill set. In such cases, more practice is the key to achieve your goal (or finding another way in of course).

Nevertheless, when faced with more traditional locks, the regular use of lockpicking, decoding or impressioning techniques will give you the ability to open most locks you will encounter.

Whatever the situation, you must master a wide range of essential techniques to be able to find the most satisfactory solution to the problems you face.

Don't be afraid by difficult locks. There is (almost) always a solution. It takes time, practice, commitment, but the result is always there.

Take your time, do your homework, take the time to study some locks, make your own tools, practice again, and never give up.

Have Fun!

Alexandre *FrenchKey* TRIFFAULT