LOCKPICKING PRIMER

NSF ATE INTERNSHIP

AUGUST 2020

Prepared by: Leslie Ramos

PHYSICAL SECURITY

Lockpicking has existed for as long as the invention of locks themselves, which dates back roughly 6,000 years ago. Initially locks, such as simple knots made of rope or other materials, were used for tampering detection. Over time, new technologies developed for locks to be made with wood and metal leading to mechanical improvement, eventually becoming the locks we know today, used for security purposes.

DISCLAIMER

GROUND RULES PER THE OPEN ORGANIZATION OF LOCKPICKERS (TOOOL)

1. Only pick, or attempt to pick, that which you own.
2. Do not pick any lock that you may rely on (ex: lock to your house or car)
3. The possession of lockpicking sets is generally legal throughout the United States but exceptions do exist. Local municipalities may differ so check with your local code office.

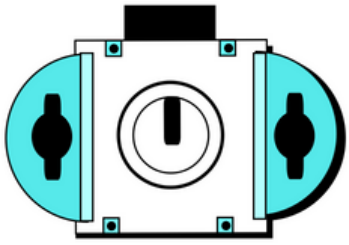
TOOOL provides a brief overview of the possession and ownership of lockpicks by state at their website, https://toool.us/laws.html

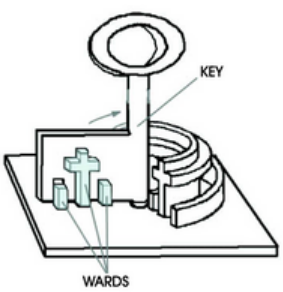
WHAT YOU'LL NEED

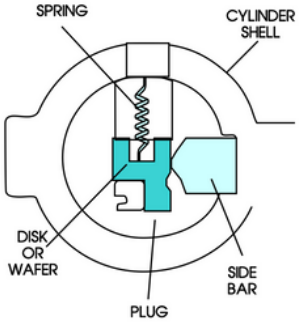
1. Lockpick set
2. Test lock(s)

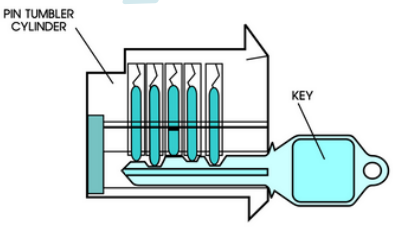
LOCK MECHANISM TYPES

1. Pin cylinder locks (aka pin tumbler)
2. Lever locks
3. Wafer locks or disk tumbler locks
4. Warded





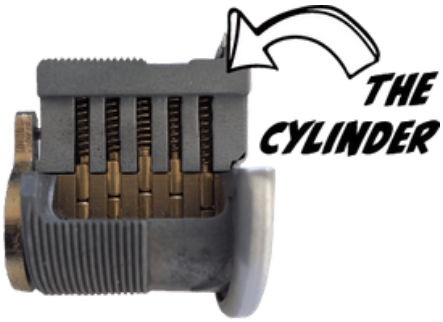




(Most common in the US)
*Primary focus of exercise

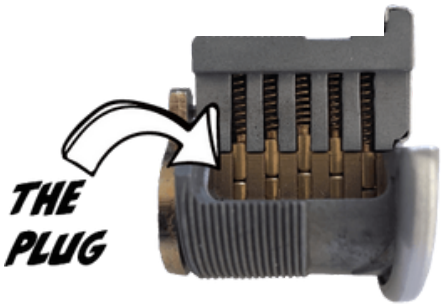
OPERATION

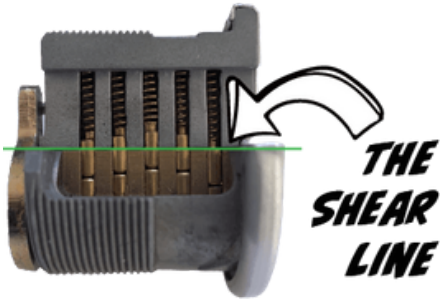
6 primary components that we effect while lockpicking



The cyclinder, part of the lock houses the rest of the components, aka shell, housing, or body of the lock. It is what slides into a door or padlock, creating the upper limit of shear line. Consider this as the "top paper."

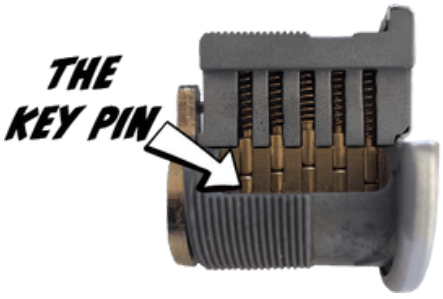
The plug surrounds the keyway, rotates freely within the housing, creating a rotational shear line. Consider this as the "bottom paper."

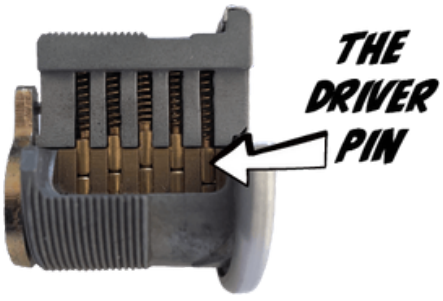




The shear line is where the plug and and hull casing meet. The goal of lockpicking is to manipulate the pins so that driver prins are above the shear line and key pins are still within the plug, allowing rotation and unlocking.

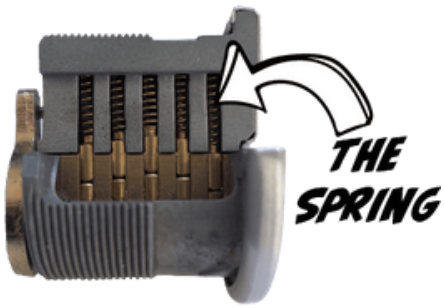
The opening of the lock that the key may be inserted into is called the keyway, where you are able to see pins. The lower pins makes contact with the key upon insertion.





The top pins are called the driver pins because it is driven down by the springs, responsible for obstructing shear line and providing the locking action. Unlike the key pins, the driver pins are usually same length. Consider this as the "pencil."

The springs have two jobs: forcing everything down into the plug and push the key pins against the key, which helps read the cuts of the key. Without springs, the pins could get stuck anywhere in the pin chamber.

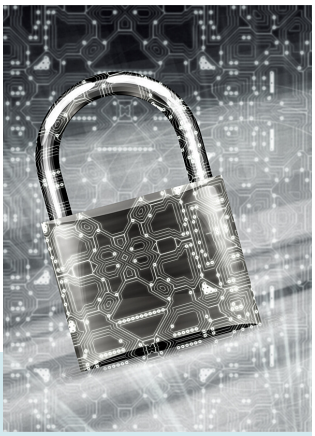


PROCESS

For demonstration purposes, the lock will be held with the left hand and picked with the right hand.

1. Begin by holding the lock in a comfortable manner in your left hand with the torque wrench inserted.
2. Wrap your left thumb around the bottom of the lock to provide support and your left index finger straight up to provide tension to the torque wrench.
3. Holding your pick as you would a dart, grasping it with your index finger and thumb, insert it into the lock all the way to the back.
4. As you get near the back of the lock, begin applying tension with your left index finger on the torque wrench.
5. When the pick is at the back begin to draw the pick forward, pushing down gently against the key pins as you continue to provide even pressure on the torque wrench.
6. The process of pushing and pulling the pick against the pins is called raking. If the lock does not open within three to four rakes, release tension on the torque wrench and try again as it is possible that a pin has been pushed too far and is binding.

DIGITAL SECURITY



The “analogue hacking” of a lock is deciphering how a device works and bypassing prohibited access, allowing for better understanding of security. Lockpicking can be thought of as a physical model to a core digital security concept – cryptography, which is the art of writing or solving codes.

Symmetric Cryptography - This can be explained as having a box with a lock. Key holders have access to unlock and lock the box. An example of this is the caesar cipher.

Asymmetric Cryptography - An example of this is if you wanted to plan a surprise party for a friend. Invitations are sent to the people you want to invite. Their addresses in this case are the public keys. When they send their RSVPs back to you, the private key is your mailbox as you’re the only person that can open your mailbox and read your mail.