EECS 388

Introduction to Computer Security

Lecture 26:

Physical Security: Locks and Lock Picking

December 3, 2024
Prof. Halderman

What is Physical Security?

Physical security defenses are mechanisms that create barriers to unauthorized physical access

Examples: locks, latches, safes, alarms, cameras, guards, guard dogs, doors, windows, walls, ceilings, floors, fences, door strikes, door frames, and door closers

Physical security is a computer security concern because all computing devices exist in the physical world

Many powerful attacks are only possible with physical access

If an attacker gains physical access to your server room or network wiring closet, is your data still safe?

Destructive vs. Nondestructive Entry

Destructive entry

uses force to defeat physical security and leaves obvious **evidence**

Example:

Methods that involve crowbars, saws, bolt cutters, sledge hammers

Apparent that a breach occurred, so you can start remediation

Expensive to prevent, but can invoke tools for recovery (e.g., insurance) and deterrence (e.g., police)

Nondestructive entry

compromises security without leaving obvious signs of a breach

Example:

Under-the-door tool

Lock picking, etc.

More sinister threat.

Can be vastly harder to recover from

[Why?]

Different Door Knobs

Under-the-Door Tool (UDT)

https://www.youtube.com/watch?v=O74Q1VTz4j4#t=48

Locks

Since ancient times, one of the cornerstones of physical security. Often a symbol for security itself

Trust in locks is mostly unwarranted.

Most can be easily bypassed with nondestructive methods, often in seconds with readily available tools

A pair of paperclips is all an attacker needs to pick many widely used locks

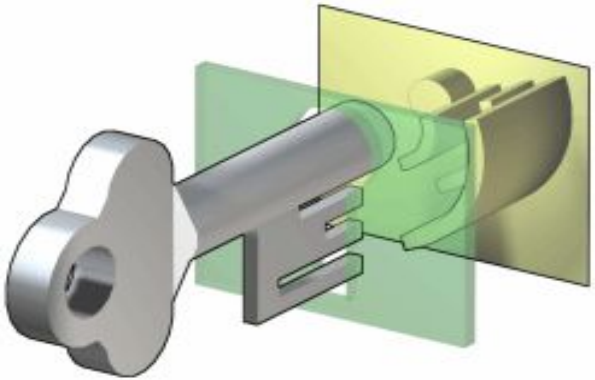
["Locks keep honest people honest"?]

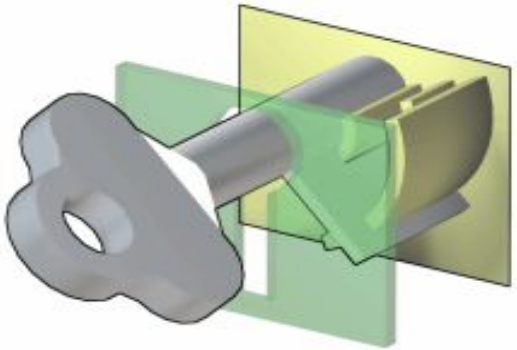
Kinds of Locks: Warded Locks

Kinds of Locks: Warded Locks

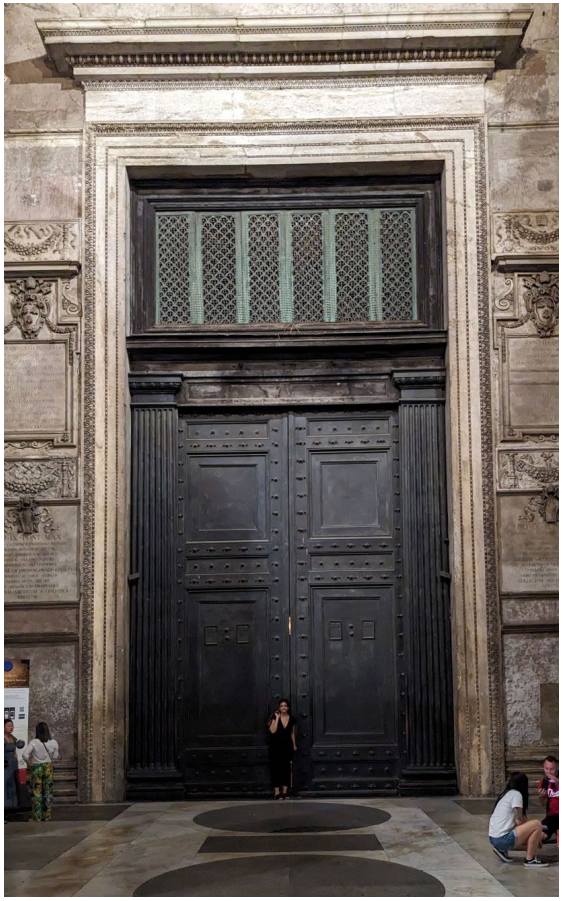
Warded locks used since ancient Rome. Weak security

Obstructions in the lock (**wards**) engage protrusions on *incorrect* keys and prevent turning





Security comes from *everyone else* having the *wrong* key, not from verifying that you have the right key



Kinds of Locks: Combination Locks

Combination locks use a numeric code instead of a key

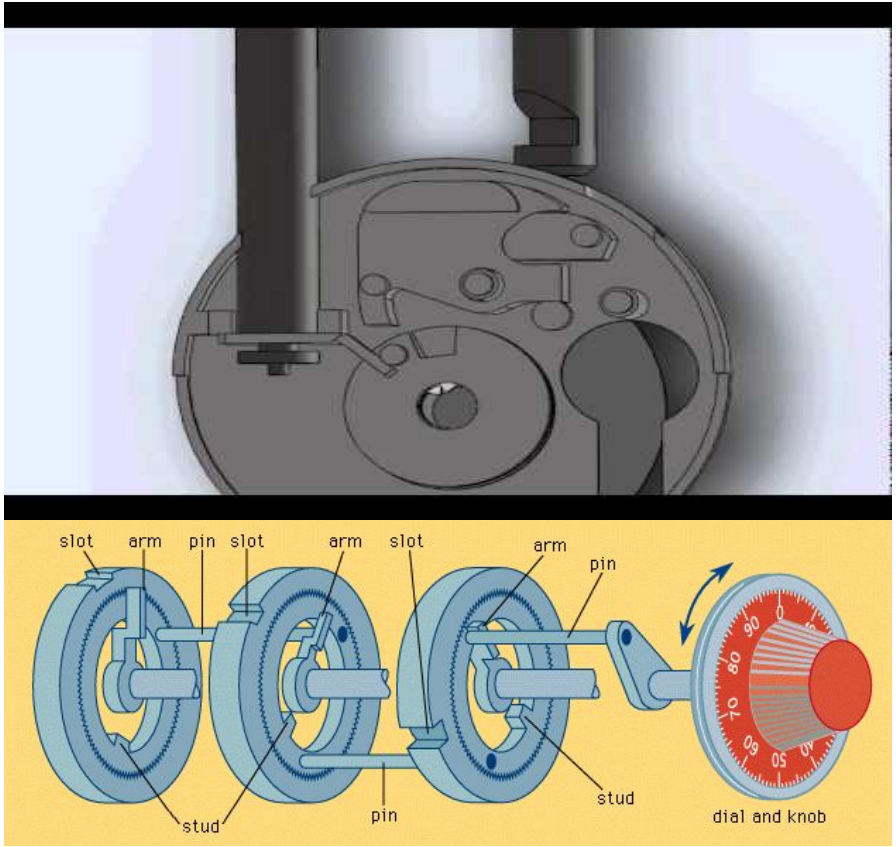
Theory: Given ***N*** dial positions, ***M*** numbers in the combination, have N^M possible combinations.
E.g., 40^3 = 64,000 combos

Inexpensive locks have high error tolerance, will accept numbers ±1.5, so only need to try ≈2000 combinations

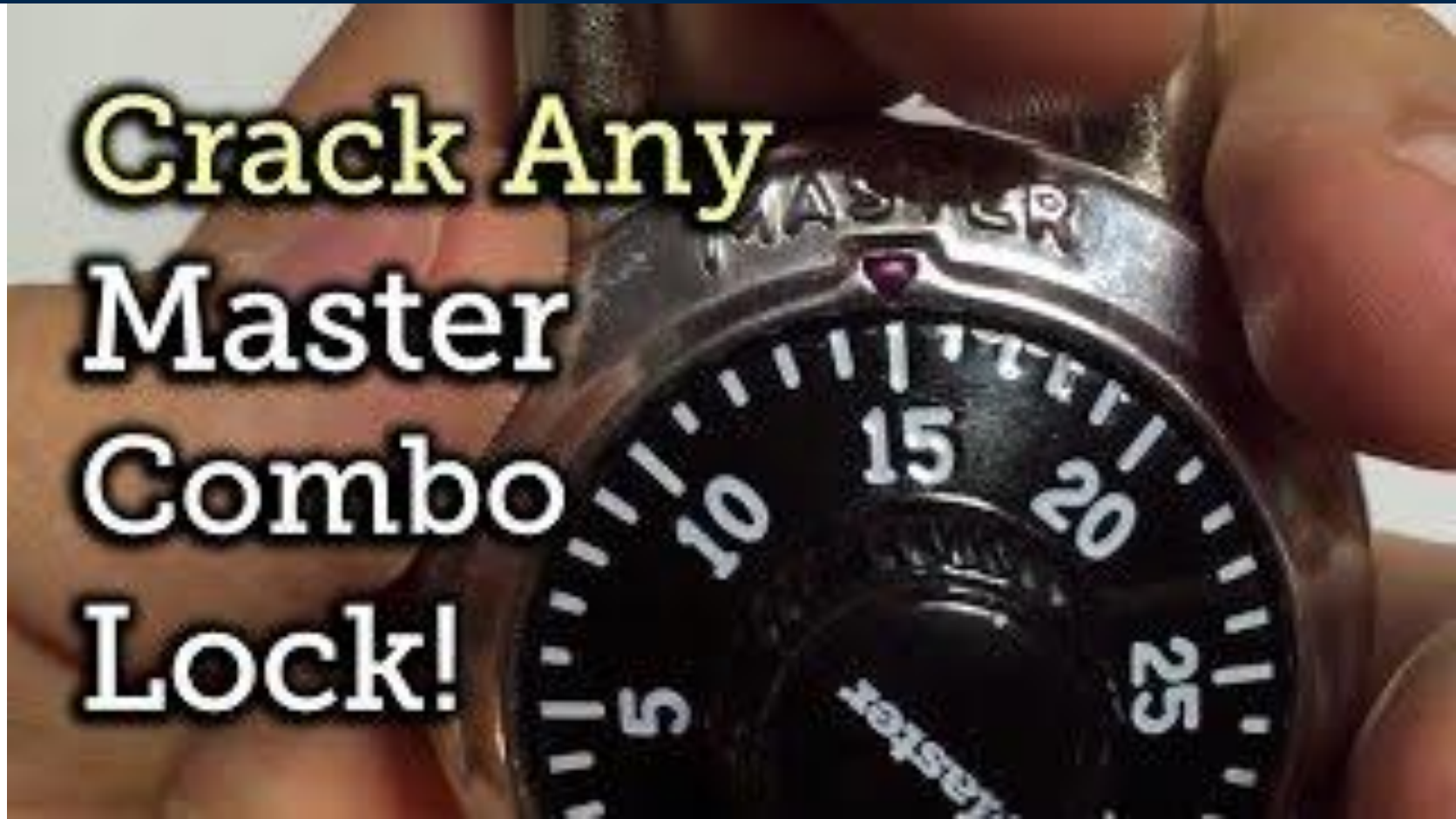
Can reduce to only **eight** by noting the critical gear points and applying math

See: https://youtu.be/09UgmwtL12c

Try it yourself! Tool: https://samy.pl/master/



Defeating Combination Locks



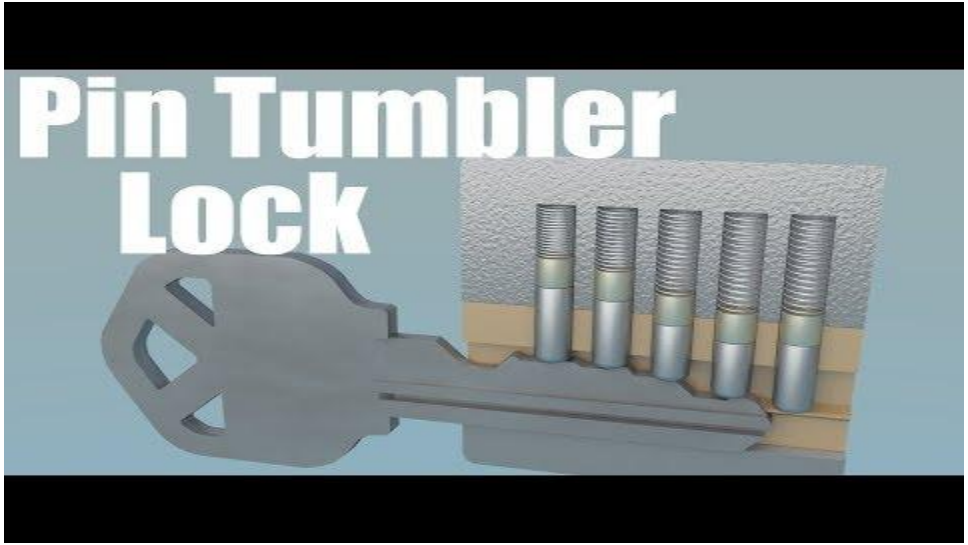
See:
https://youtu.be/09UgmwtL12c

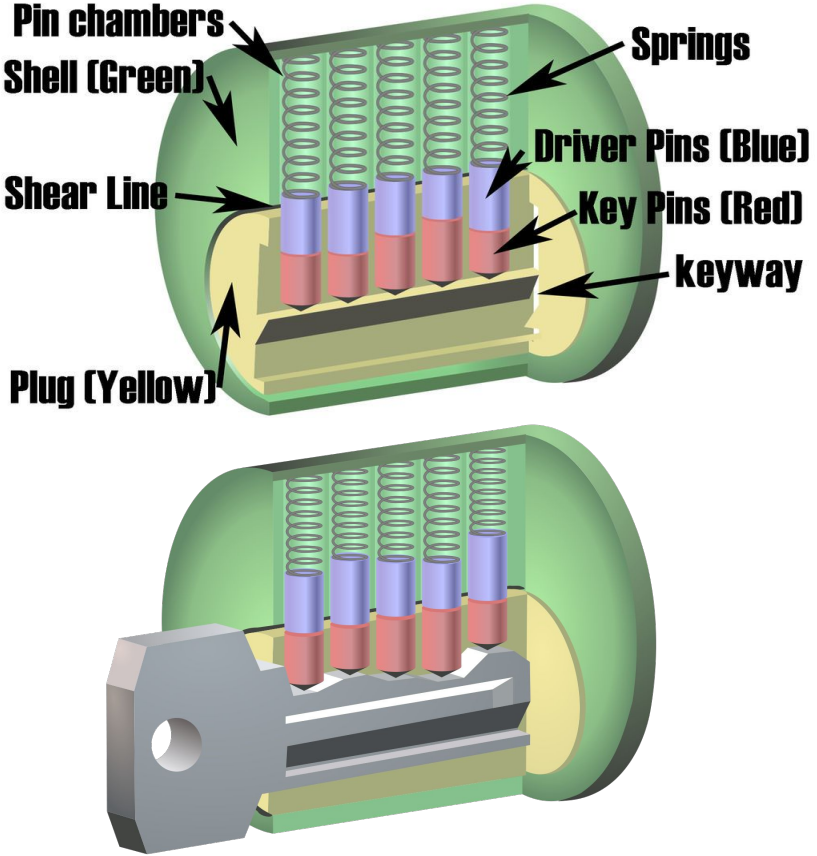
Tool:
https://samy.pl/master/

Kinds of Locks: Pin Tumbler Lock

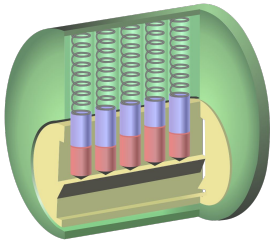
Most modern locks are **pin tumbler locks**, invented by Linus Yale in 1848

Clever mechanism verifies that *your key* has the *right shape*

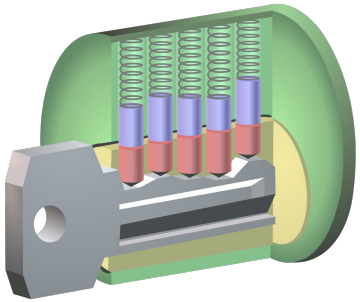




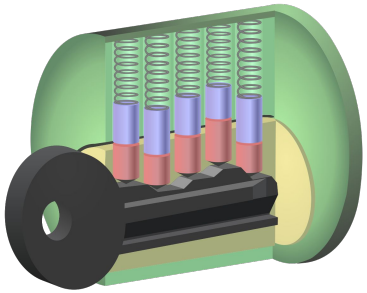
How Pin Tumbler Locks Work

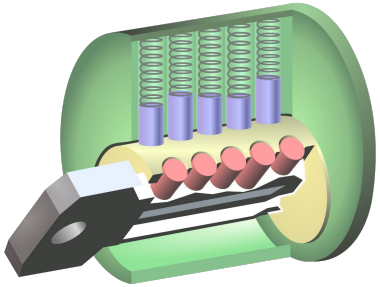


1. When a key is not present, the pin stacks are pushed down by the springs so that the driver (top) pins span the plug and the outer casing, preventing the plug from rotating



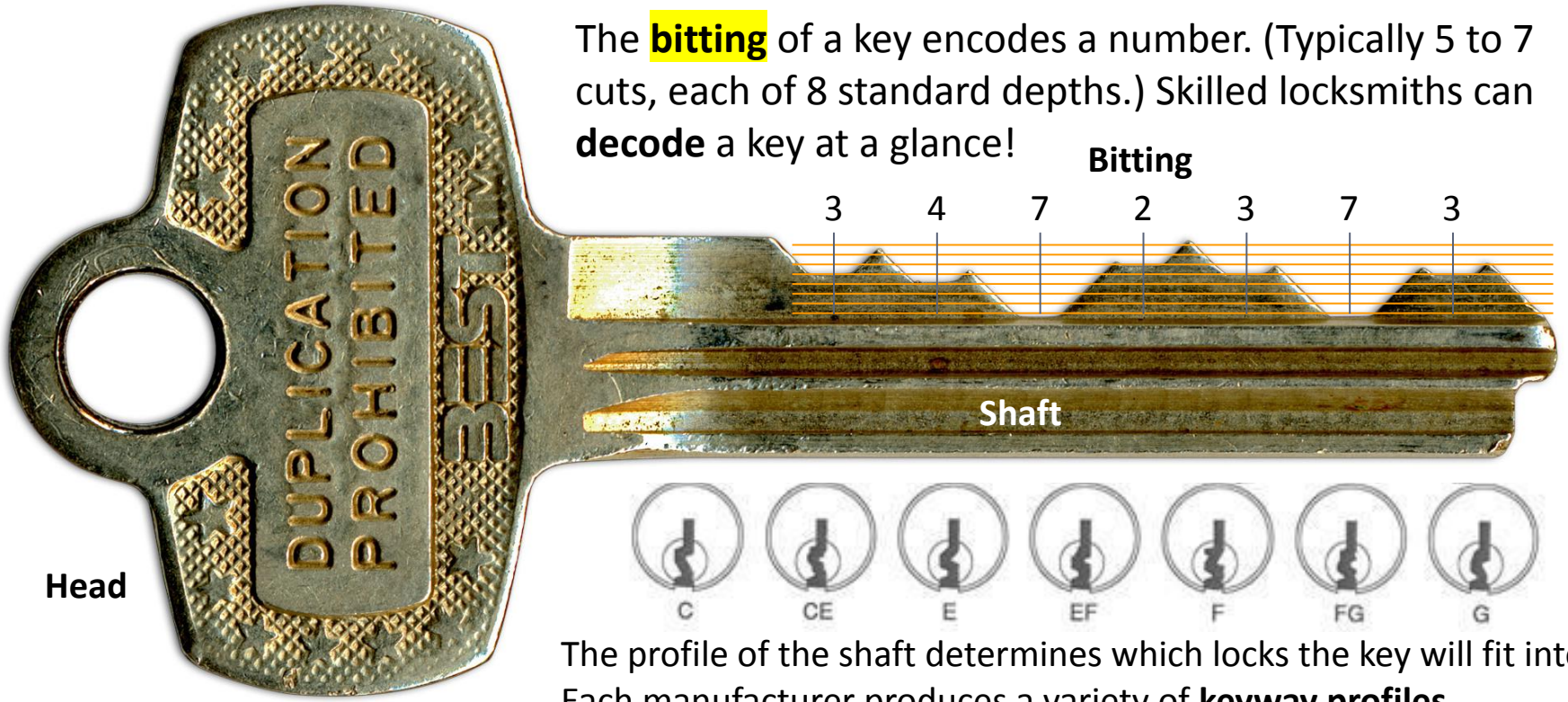
2. When the correct key is inserted (*left*), the ridges of the key push up the pin stacks so that the cuts of the pin stacks align with the shear line. With the wrong key (*right*), at least one pin blocks the shear line, so the plug can't turn





3. The alignment of the cuts with the shear line allows the plug to be rotated. A lever attached to the plug retracts the bolt, allowing the door to be opened

Decoding a Key



The **bitting** of a key encodes a number. (Typically 5 to 7 cuts, each of 8 standard depths.) Skilled locksmiths can **decode** a key at a glance!

The profile of the shaft determines which locks the key will fit into. Each manufacturer produces a variety of **keyway profiles**

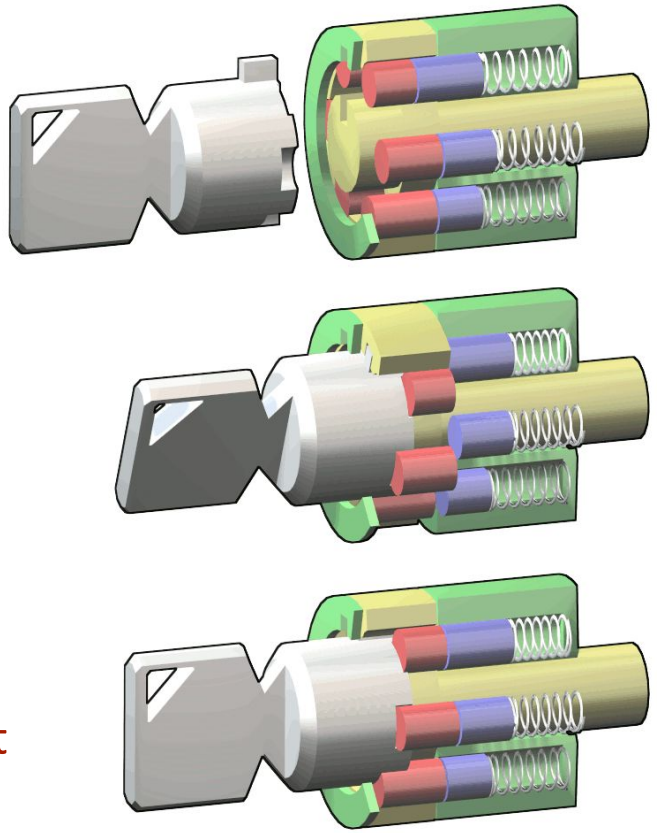
The bitting and profile code are sufficient to reproduce the key

Kinds of Locks: Tubular Locks

Tubular locks are a form of pin tumbler lock commonly used when there's not enough space for a standard length key

Design <u>doesn't</u> imply higher security

Examples: bike locks, vending machines, etc.



Inexpensive tubular locks can be opened in seconds simply by jamming in a soft plastic pen and twisting

Lock Picking

Lock picking is the practice of opening a lock by manipulating the internal mechanism without the original key

Techniques long known to criminals and guarded as a secret by professional locksmiths

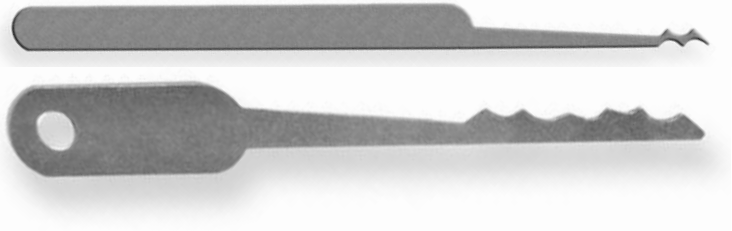
Since rise of the Internet, tools and information have become widely available, and lock picking has become a popular hobby and competitive activity

Lock picking tools are widely available.

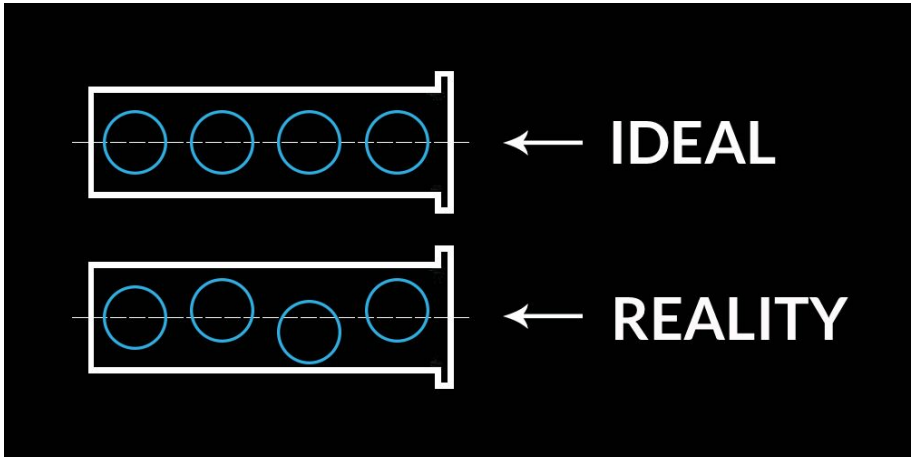
Wrenches are used to provide torque to the plug while you manipulate the pins:

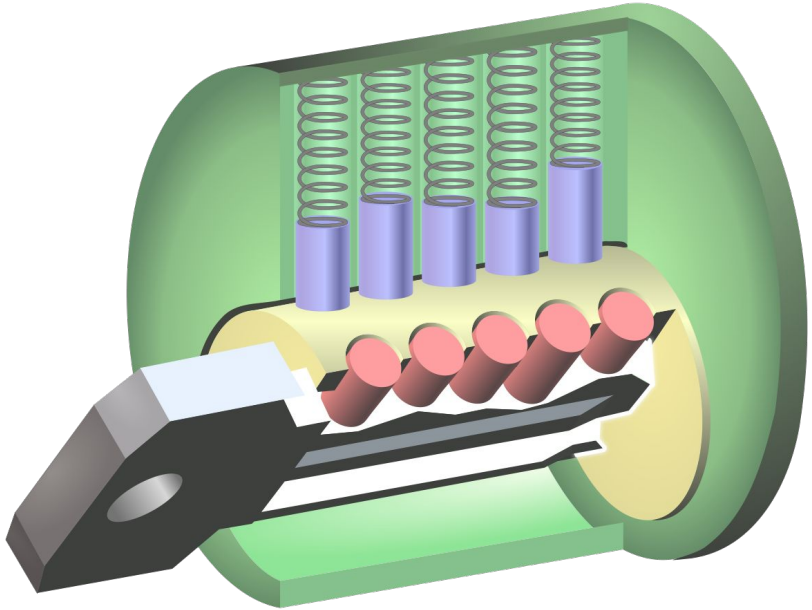
Feelers are used to move individual pins:

Scrubbers are used to move groups of pins:



Lock Picking



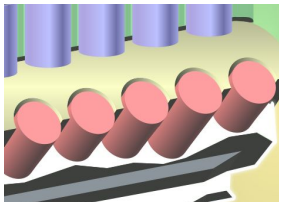


Your lock is only as good as its manufacturing tolerances

Don't buy cheap locks,
or else you'll get what you paid for!

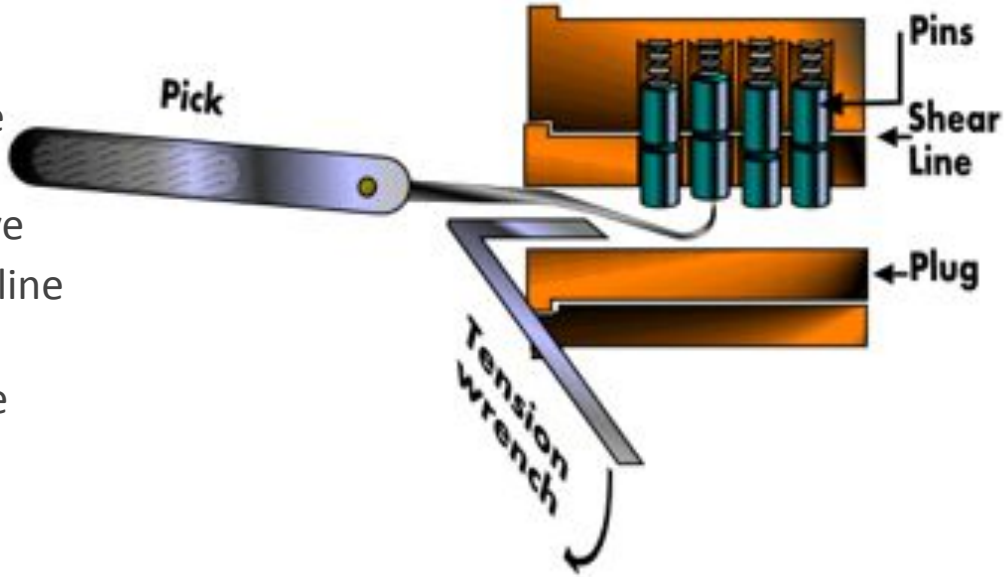
Lock Picking: Feeler Picking

Feeler picking exploits manufacturing imperfections to open a pin tumbler lock one pin at a time

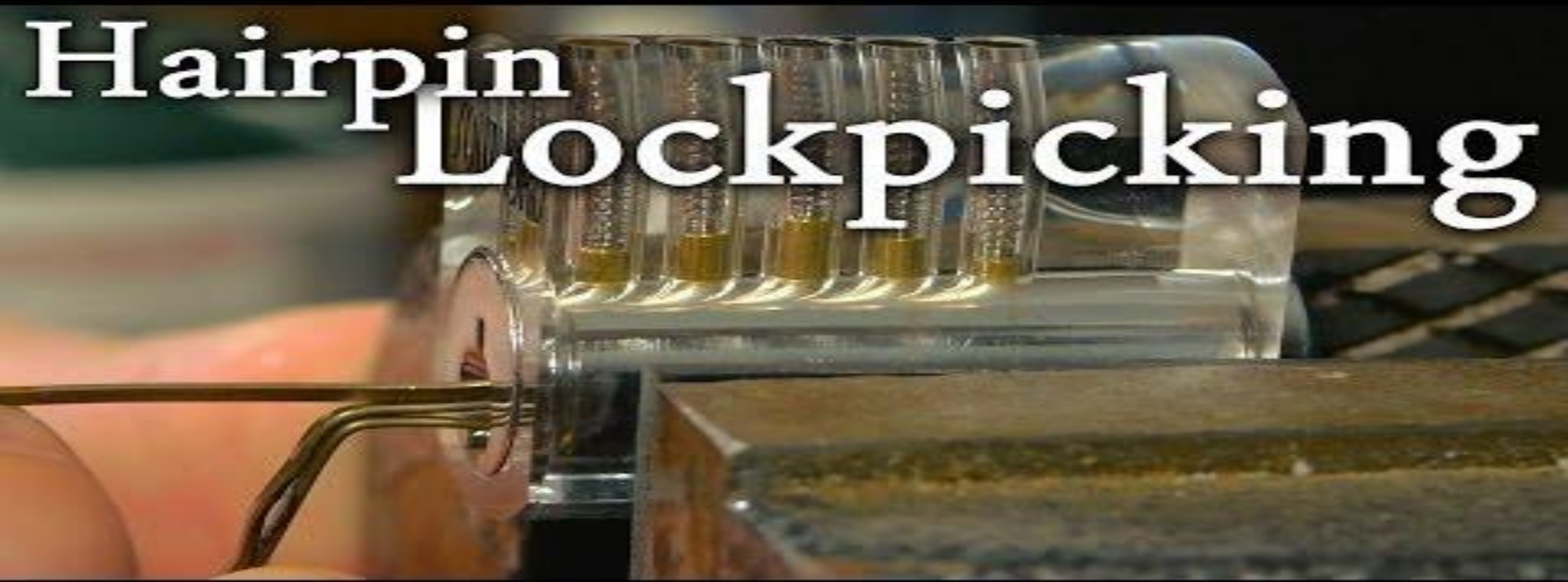


Pin chambers are minutely misaligned, so when a pin stack is aligned with the shear line, the plug can turn very slightly and hold the top pin in place

1. Apply light torque to the plug using a tension wrench
2. Use a feeler to lift one pin at a time and identify a **binding pin**—a stack where the top pin is making contact with the shell. A binding pin will take more force to move
3. Lift binding pin until it reaches the shear line
4. The plug will rotate very slightly, with an audible click, and the top pin will become set (stuck) above the shear line
5. Find next pin and repeat until lock opens



Lock Picking: Feeler Picking



https://youtu.be/cjuT_63Ioig?t=97

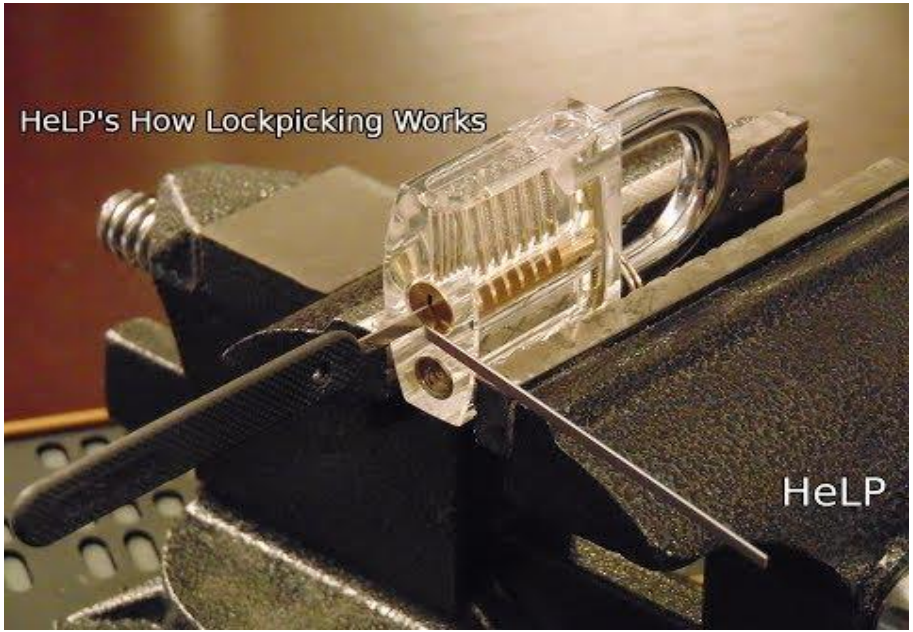
Lock Picking: Scrubbing/Raking

Scrubbing or **raking** moves many pins at random, in hopes of quickly setting them above the shear line

1. Apply light torque using tension wrench

2. Use a scrubber tool (*shown above*) to work pins from back to front, using a circular motion. Try to pop them over the shear line
3. With luck and a little practice, all will end up above the shear line and the lock will open

Basically a “brute force” attack. Works well on inexpensive locks and is good for beginners



https://youtu.be/uqgyDsDvq_Y?t=356

Try it yourself!

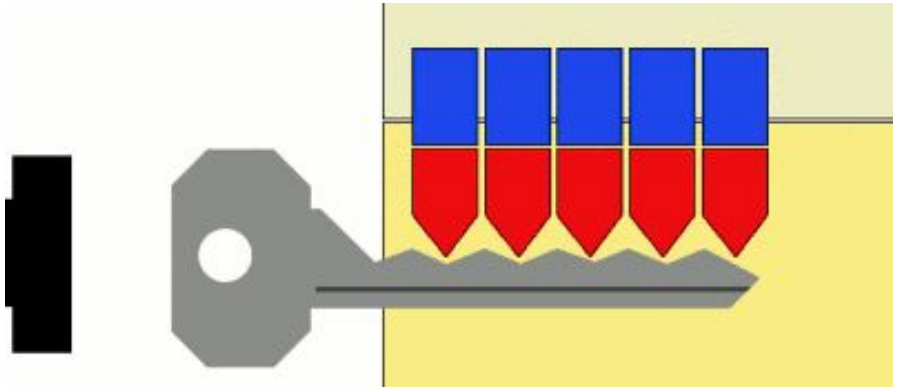
Lock Bumping

Bumping is a highly effective technique that uses inertia to get all the pins to jump above shear line simultaneously

Relies on a **bump key**, a key with all teeth cut to the lowest possible height

1. Insert bump key into lock
2. Twist key to apply light torque
3. Strike head of key sharply, transferring inertia to driver pins
4. Lock opens

Lock picking leaves evidence (scratches on pins), bump keys do not unless hit too hard



Lock Bumping

https://youtu.be/cIfF4IWp0Xc?t=38

Lock Picking Tools and the Law

Laws regarding lock picks and covert entry tools vary from state to state

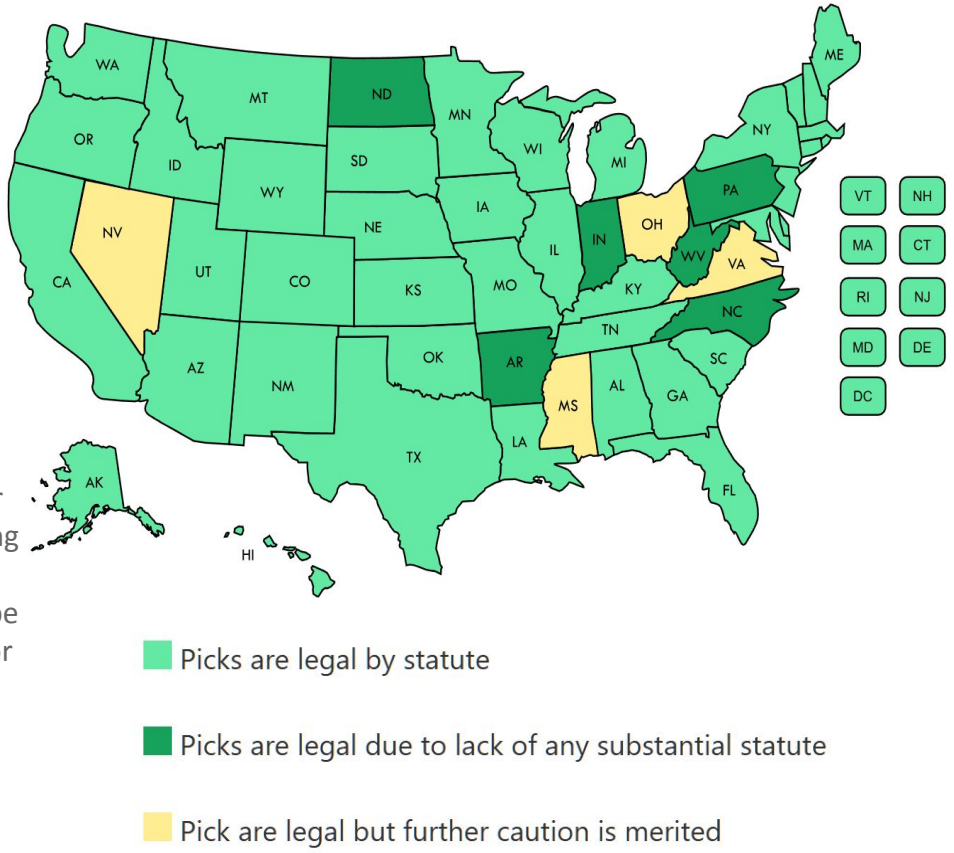
Purchase of lock picking tools is legal, but caution is merited in some states

Possession with intent to commit a crime is often a crime in itself

Michigan Compiled Laws - § 750.116 - Burglar's tools; possession
Any person who shall knowingly have in his possession any … tool or implement, device … adapted and designed for … forcing or breaking open any building, room, vault, safe or other depository, in order to steal therefrom any money or other property, knowing the same to be adapted and designed for the purpose aforesaid, with intent to use or employ the same for the purpose aforesaid, shall be guilty of a felony….

If in doubt, ask a lawyer.

Source and details: https://toool.us/lockpicking-laws/

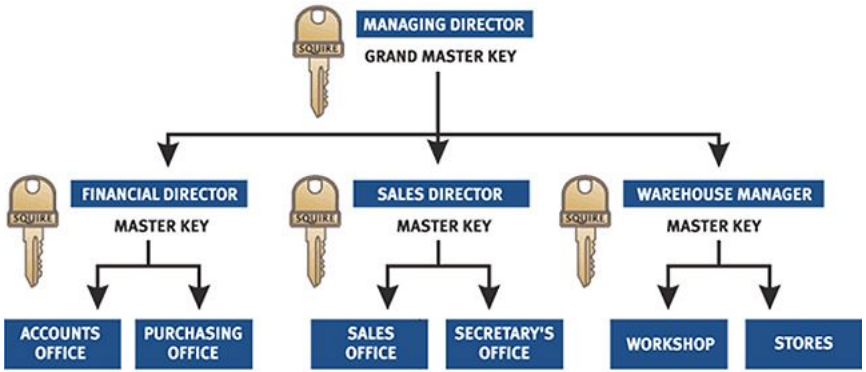


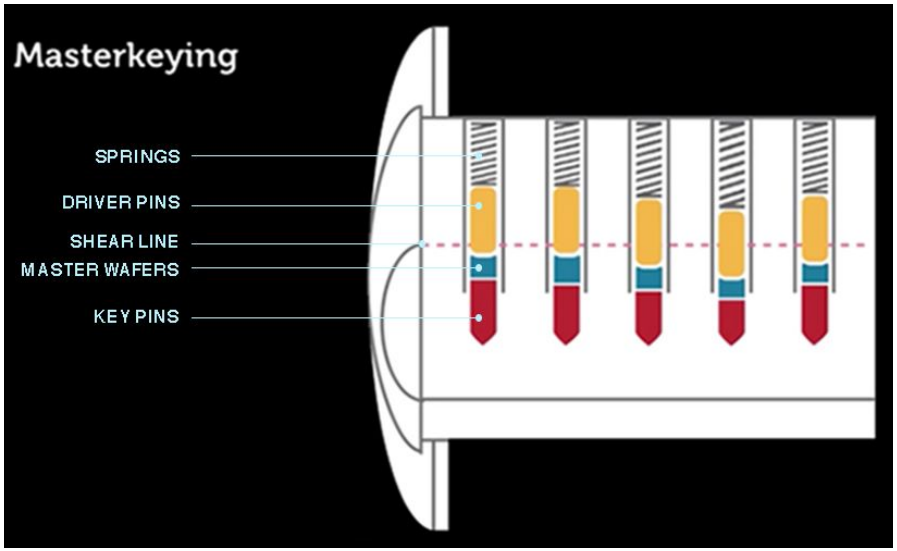
Master Key Systems

What if we want a special key that can open many different locks?

Master key systems add a layer of wafers to create a hierarchy of keys

Cut keys so either gap is at shear line. Multiple keys can now open same lock





Terminology:

master key, individual change keys

Add an additional layer of wafers for another layer in the hierarchy (grand master key)

Privilege Escalation Attack on Master Keys

Efficient algorithm to deduce master key, given any change key

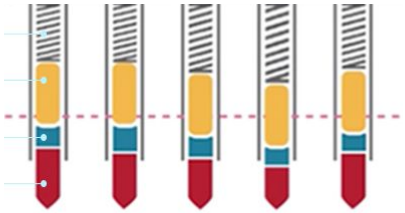
(First published by Matt Blaze in 2003)

Say lock has ***P*** pins, ***D*** possible depths.

For each pin position ***p***:

1. Create ***D***-1 variants of change key, each differing only in position ***p***. (One for each depth except the change key's)
2. Test these keys and figure out which one opens the lock. That will be the depth of the master key at ***p***

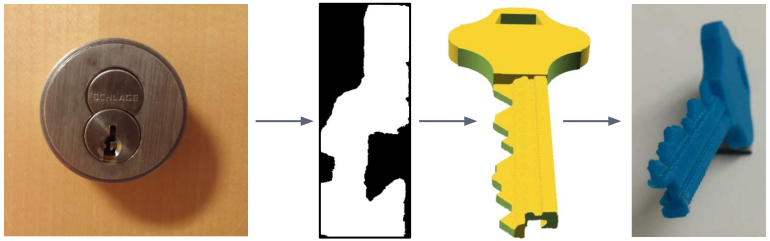
Consumes ***P***(***D***-1) blanks, but can optimize*



Insight: Each stack of pins operates independently, so any hybrid of master and change-key cut depths will open the lock

As a defense, some manufacturers produce **controlled blanks**, patented key profile shapes that they sell only to verified customers

However, 3D printing can be used to produce key blanks of any shape. Researchers showed can do automatically from photo of the lock



“Key” Takeaways

Physical security is an important aspect of many computer security problems:

- Powerful attacks possible with physical access to your devices or network

Understanding adversarial techniques can help you plan an effective defense:

- Need different defenses for covert entry versus destructive entry
- Almost all locks you encounter can be covertly bypassed with modest skill

For important assets, adopt a layered approach to physical security:

- **Locks:** slow down the attacker
- **Cameras/alarms:** deter or detect the attacker
- **Guards/police:** stop or arrest the attacker
- **Backups/encryption/disaster recovery plans:** help minimize damage

Coming Up

Thanks for a great semester everyone!

Please complete your course evaluations

Reminder:

Forensics Project due Thursday at 6 p.m.

Thursday Lecture

Exam Review Session

Final Exam

Tuesday, Dec. 17, 7–9 p.m.

IN PERSON (see Piazza for locations)