CS 497: Cybersecurity

Galin Zhelezov
Department of Engineering and Computer Science
York College of Pennsylvania

YORK COLLEGE OF PENNSYLVANIA

Section 2.2 – Locks and Keys

Legal Notice

- **Laws regarding lock picking vary significantly state-by-state**
- **In most states purchase and possession of dedicated lock picking tools is legal**
    - Penalties are raised significantly if you get caught using them in the commission of a crime

Public domain image from http://commons.wikimedia.org/wiki/File:Madame_Restell_in_jail.jpg

What Is Physical Security?

- **Any physical object that creates a barrier to unauthorized access**
- **This includes: locks, latches, safes, alarms, guards, guard dogs, doors, windows, walls, ceilings, floors, fences, door strikes, door frames and door closers**

Is Physical Security An IT Concern?

- **You have been working hard to secure your network from cyber attacks**
  - Redundant layers of antivirus programs, firewalls and intrusion detection systems should protect against every possible electronic method of entry
- **But what if an attacker gains access to the server room or network wiring closet ...**
- **Is you network still safe?**

Destructive vs. Nondestructive Entry

- **Destructive entry**
  - Involves using force to defeat physical security
  - Methods involve crowbars, bolt cutters and sledge hammers
  - Negative impact on IT resources is apparent
  - Remediation steps also obvious
- **Nondestructive entry**
  - Compromises security without leaving signs of a breach
  - Defeats intrusion detection
  - Greater and long-term threat

Compromising Locks

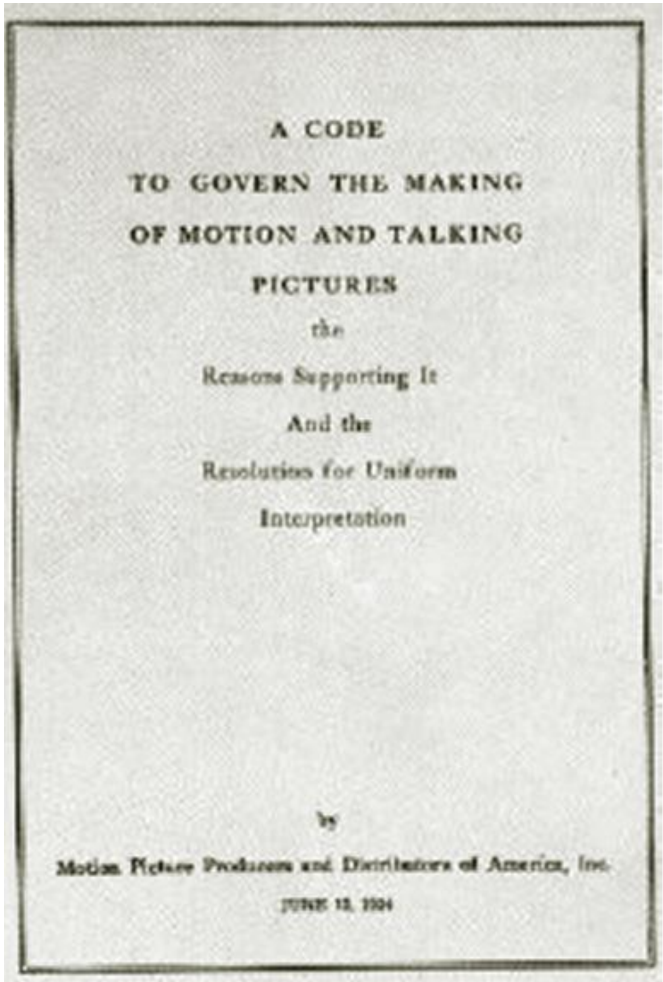
- **For centuries, the lock has been one of the cornerstones of physical security**
  - We rely on dozens of them every day to protect people and assets
- **The trust most people place in locks is unwarranted**
  - Most locks can be easily compromised with nondestructive methods
  - Sometimes within seconds and with readily available tools
- **“Locks keep honest people honest”**

Lock Picking

- **Lock picking had been the exclusive art of locksmiths, professional thieves, spies and magicians for hundreds of years**
- **However, with the advent of the Internet, information about lock picking methods and tools has become readily available**
  - E.g., YouTube has many lock picking videos

Lock Picking in Movies

- **Genuine lock picking in movies used to be prohibited**
- **Before 1967, the Hays code (Motion Picture Production Code) required censorship of Hollywood movies**
  - “All detailed (that is, imitable) depiction of crime must be removed, such as lock picking or mixing of chemicals to make explosives”



A CODE

TO GOVERN THE MAKING

OF MOTION AND TALKING

PICTURES

the

Reasons Supporting It

And the

Resolution for Uniform

Interpretation

by

Motion Picture Producers and Distributors of America, Inc.

JUNE 13, 1934

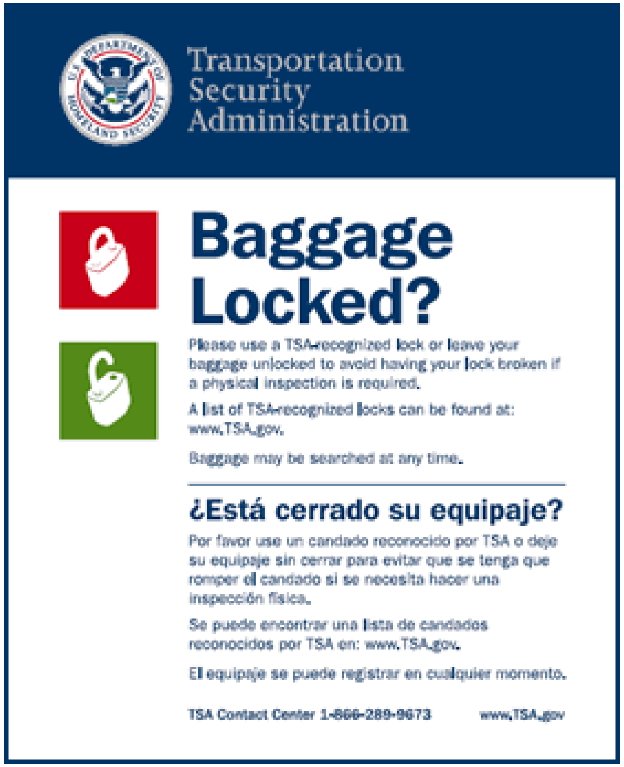
Public domain image from http://commons.wikimedia.org/wiki/File:Motion_Picture_Production_Code.gif

LOCK TYPES

Image from http://commons.wikimedia.org/wiki/File:Ancient_warded_lock_open.jpg used with permission under Gnu Free Documentation License 1.2

TSA Lock

- **The U.S. government has established a set of rules for the inspection of baggage without the presence of passengers**
- **Special TSA-approved locks allow both inspection and protection against theft**
- **An important element is that the inspection must be easily verifiable by the user**



Transportation Security Administration

Baggage Locked?

Please use a TSA-recognized lock or leave your baggage unlocked to avoid having your lock broken if a physical inspection is required.

A list of TSA-recognized locks can be found at: www.TSA.gov.

Baggage may be searched at any time.

¿Está cerrado su equipaje?

Por favor use un candado reconocido por TSA o deje su equipaje sin cerrar para evitar que se tenga que romper el candado si se necesita hacer una inspección física.

Se puede encontrar una lista de candados reconocidos por TSA en: www.TSA.gov.

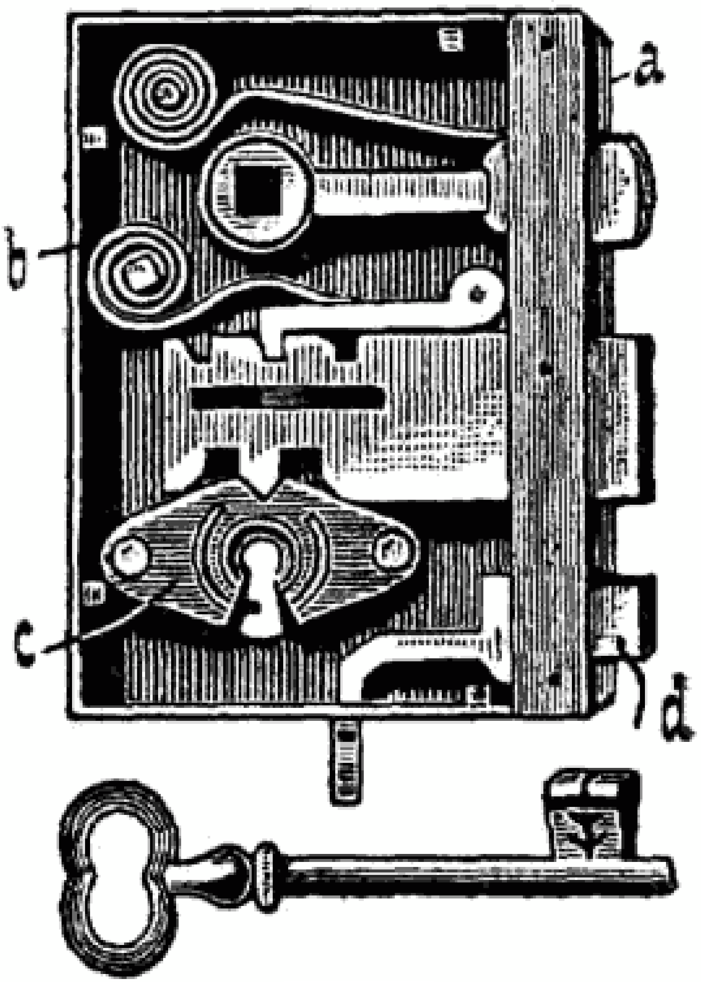
El equipaje se puede registrar en cualquier momento.

TSA Contact Center 1-866-289-9673 www.TSA.gov

Public domain government image

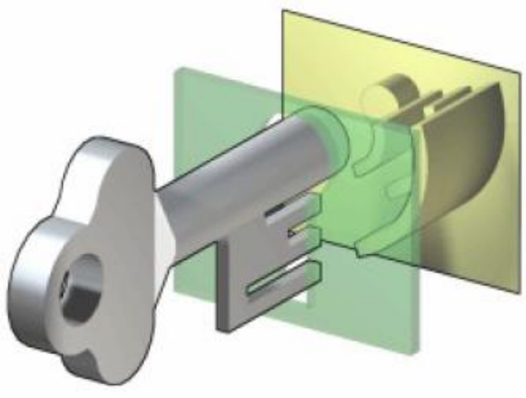
Warded Locks

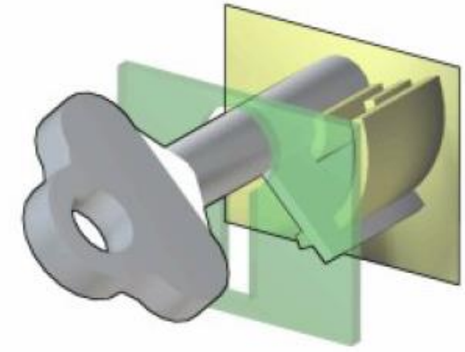
- **Locks of this type were used in ancient times**
- **The key moves the bolt assisted by a support spring**
- **Security relies on the fact that not all keys pass through the key hole**



Skeleton Key

- **Usually in old style doors or desks**
- **Different concentric obstructions**
- **Easy to lock pick with Skeleton keys**
- **They come from ancient Rome**





Images from http://en.wikipedia.org/wiki/File:Warded_locked.png used by permission under Gnu free documentation license 1.2

Pick vs. Bypass

Break open a lock in a nondestructive manner can be achieved either through:

•Pick: acting on the lock mechanism simulating the operation of the key

•Bypass: manipulation of the bolt without using the lock

1860: Yale Pin Tumbler Lock

Public domain image of Linus Yale, Jr.

- Modern version of the Egyptian single-pin design
- Utilizes two pins for locking

- **Double-detainer theory of locking**

- **Created shear line**

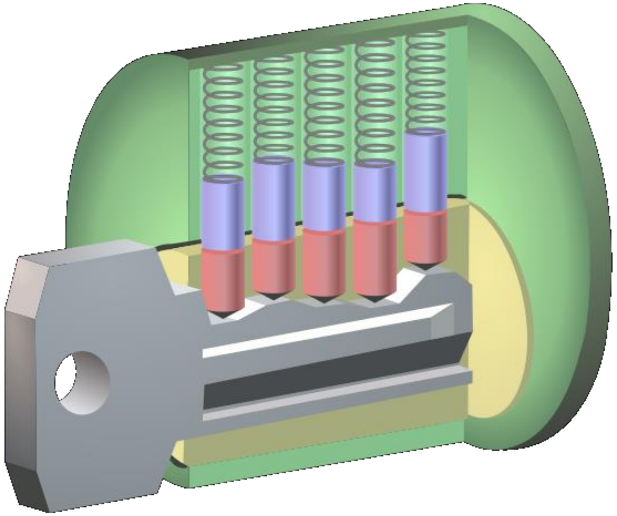
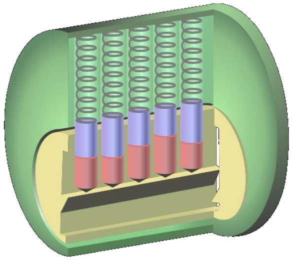


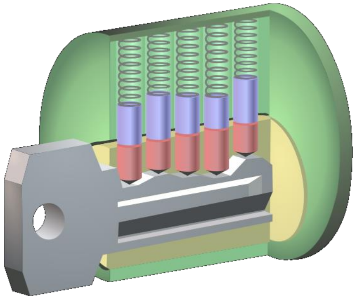
Image from http://en.wikipedia.org/wiki/File:Pin_tumbler_with_key.svg used with permission under Gnu Free Documentation License 1.2

How Does a Pin Tumbler Lock Work?

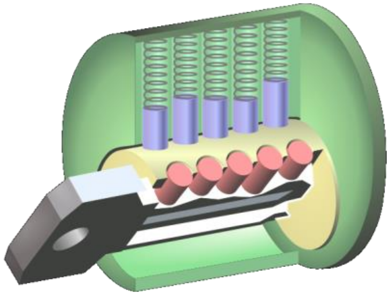
1. **When a key is not present, the pin stacks are pushed down by the springs so that the driver (top) pins span the plug and the outer casing, preventing the plug from rotating.**



2. **When the correct key is inserted, the ridges of the key push up the pin stacks so that the cuts of the pin stacks are aligned with the shear line.**



3. **The alignment of the cuts with the shear line allows the plug to be rotated.**



Images from http://en.wikipedia.org/wiki/File:Pin_tumbler_with_key.svg used with permission under Gnu Free Documentation License 1.2

How Does a Pin Tumbler Lock Work?

- **If an inappropriate key is insered, then the pins do not align along the shear line and the lock does not turn.**

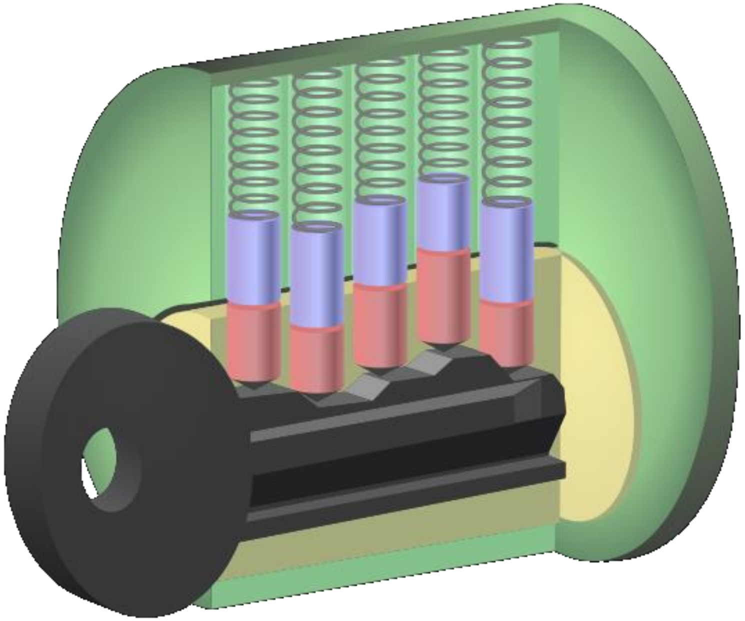


Image from http://en.wikipedia.org/wiki/File:Pin_tumbler_with_key.svg used with permission under Gnu Free Documentation License 1.2

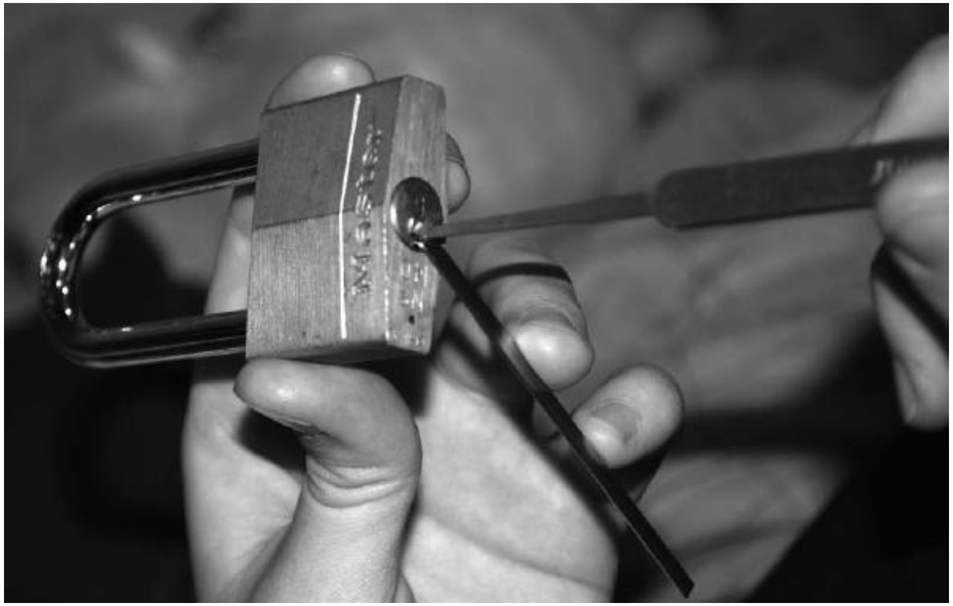
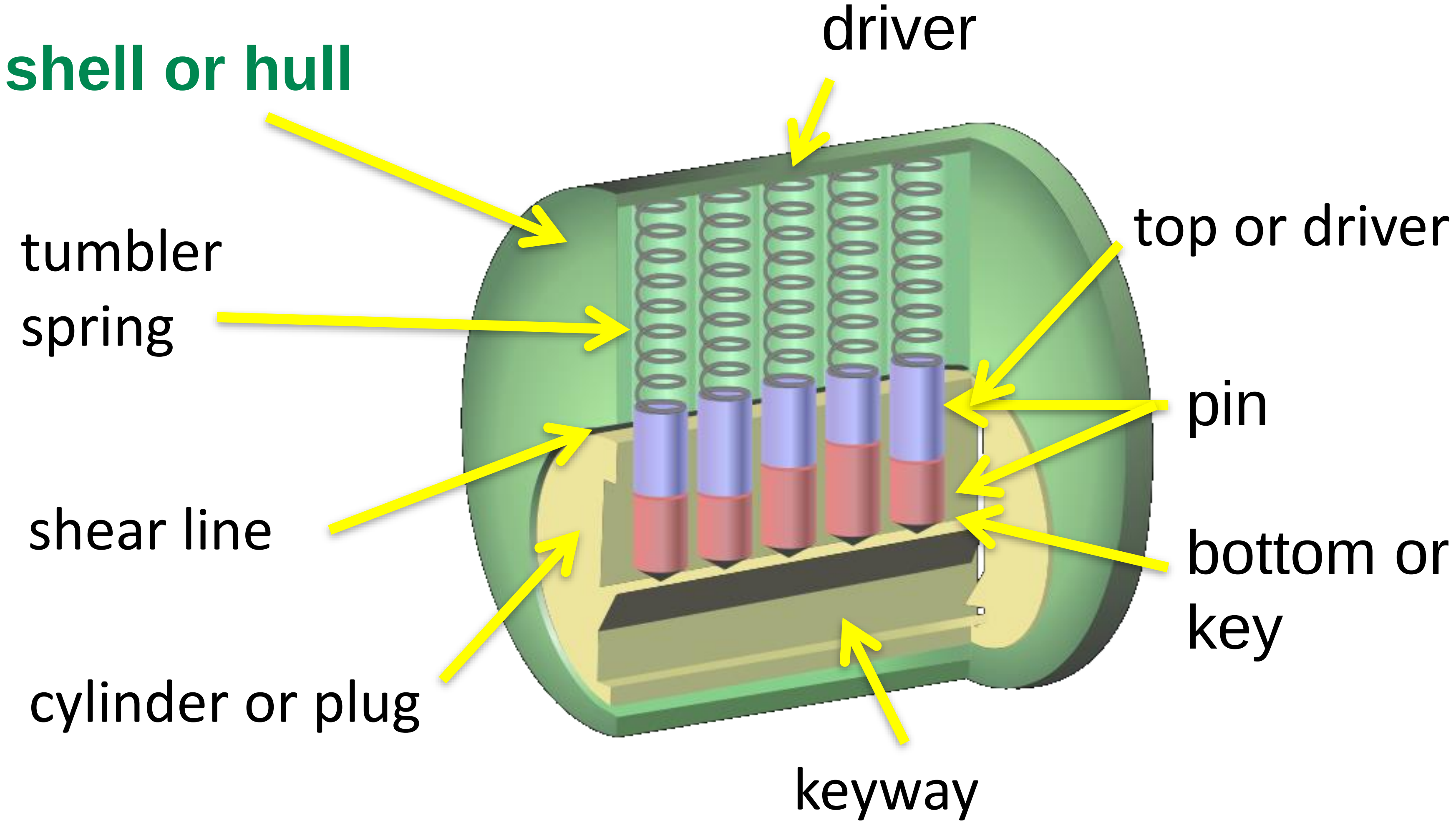


Photo by Dan Rosenberg included with permission.

LOCK PICKING

Terminology



shell or hull

driver

tumbler spring

top or driver

pin

shear line

bottom or key

cylinder or plug

keyway

Image from http://en.wikipedia.org/wiki/File:Pin_tumbler_with_key.svg used with permission under Gnu Free Documentation License 1.2

Lockpicking Tools

- **Feelers**
- **Scrubbers**
- **Tension tools**

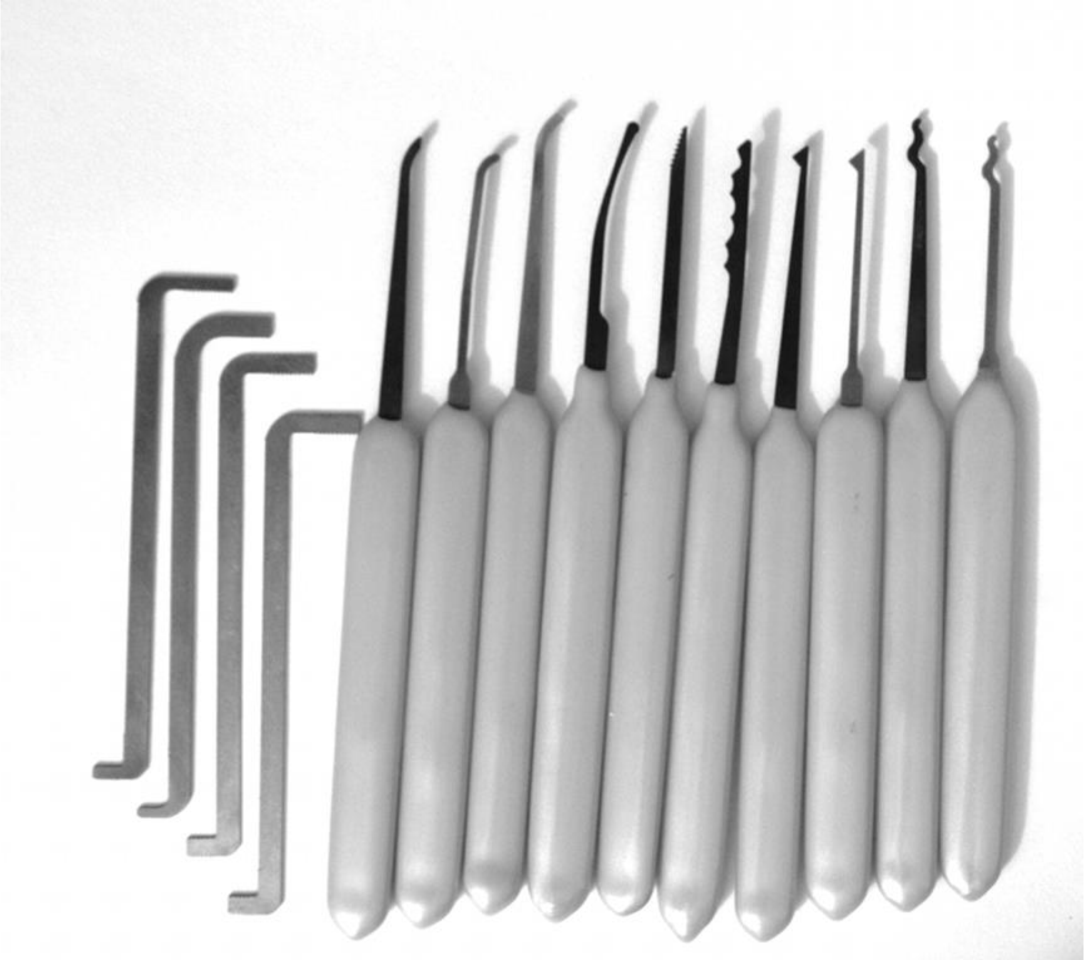


Photo by Jennie Rogers included with permission.

Feeler Picking

- **Apply light tension**
- **Lift one pin at a time**
  - Identify binding pin
- **Lift binding pin until it reaches the shear line**
- **Setting the binding pin will rotate the lock slightly**
- **Find next pin and repeat the process**

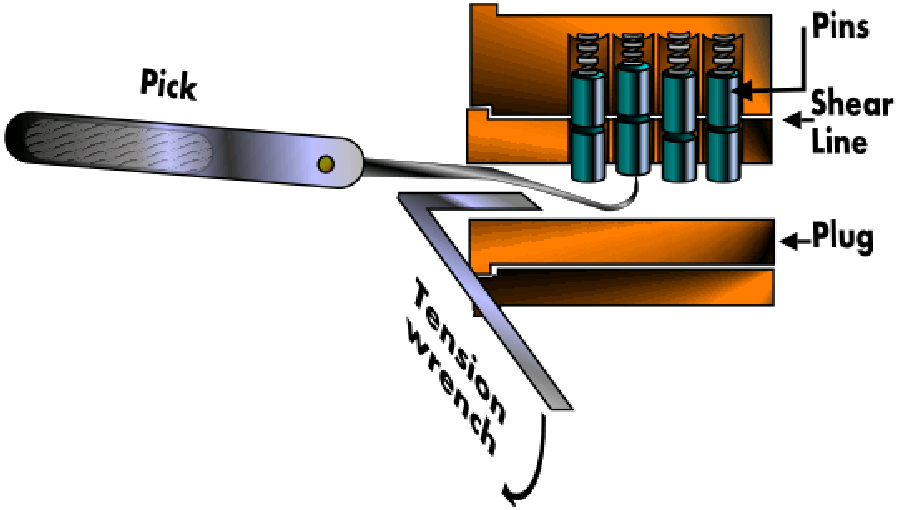


Image from http://commons.wikimedia.org/wiki/File:Pin_and_tumbler_lock_picking.PNG used with permission under Gnu Free Documentation License 1.2

Scrubbing / Raking

- **Apply light tension**
- **Work over pins back to front in a circular motion**
  - attempting to pop them into the shear line with the combination of tension
- **Good for beginners**
- **Usually employ snake pick or half diamond**

Photo by Jennie Rogers included with permission.

The Math of Lock Picking

- **Suppose we have**
  - 40 different kinds of key blanks
  - 7 pin positions
  - 8 different possible pin heights
- **Then the total number of possible locks is**
  - $40 \times 8^7 = 83{,}886{,}080$
- **Not all these are possible, however, as it is difficult to put long teeth next to small teeth.**

Rights Amplification in Master Keyed Systems

Reverse engineer master key from change key

Each lock has *P* pins, with *D* potential cut heights

Create *D-1* test keys for each pin position *p* from *1 to P*

At position *p,* cut each of the *D-1* keys with each possible bitting *excluding* the bitting of the change key at that position.

Rights Amplification (continued)

Query the lock until you find each pin position

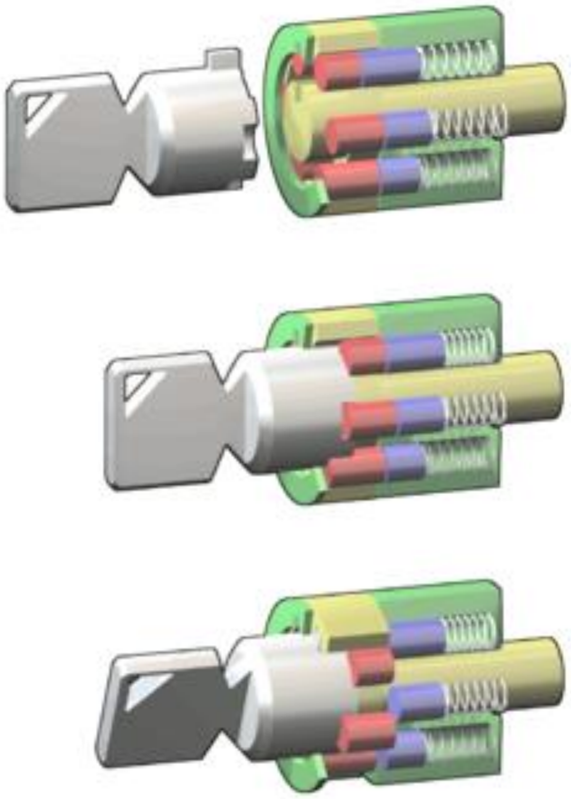
- i.e. To determine first key cut depth insert each of the D-1 test keys and determine which one does not bind to the pin
- Repeat for each pin

Rights Amplification Statistics

- Consumes *P(D-1)* blanks
- Can reduce to *P* blanks and file down on the fly
  - But this looks suspicious
- Search space is practically pruned by manufacturer specs
  - Maximum distance limit in legal adjacent cuts
  - Older installations sometimes require MKs to be higher on the pin stack

Tubular lock

- **Usually on car alarms or vending machines**
- **6-8 pins**
- **Easy to pick with special tool**
- **The tool could become a new key**



Images from http://en.wikipedia.org/wiki/File:Tubular_locked.png used with permission under Gnu Free Documentation License 1.2

Statistics

- **4-6 pins, 4-10 levels**

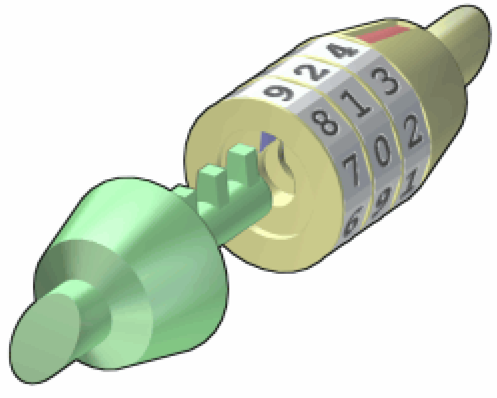
- **10^6 = 1,000,000 possible keys!**

- **The angular positions of the cylinders allow to obtain about 180 different positions $(180 \cdot 10)^6 = 3.4012224 \times 10^{19}$**

- **(Un) fortunately there is a need for some tolerance in locks**

Combination Locks

- **There are locks that do not require a physical key to be opened but a code**



- **Number of combinations is**

  - Number of digits

    times

  - Length of combination

Images from http://en.wikipedia.org/wiki/File:Combination_unlocked.png and http://commons.wikimedia.org/wiki/File:Electronic_lock_yl88.jpg used with permission under Gnu Free Documentation License 1.2

Combination Locks

- **Inexpensive combination padlocks allow attacks based on reducing the space of possible combinations to try**
  - The gears have a higher tolerance of the external disk combination
  - Nominal number of combinations is $40^3 = 64,000$
  - Possibilities can be reduced to about 80 by detecting critical gear points

Public domain image from http://commons.wikimedia.org/wiki/File:Lock.JPG

E.g., see http://www.wikihow.com/Crack-a-%22Master-Lock%22-Combination-Lock

Bumping

- A different way of picking locks
- Virtually all traditional Yale and similar locks can be opened by bumping
- What lock pickers say about bumping:
  - RELIABLE
  - REPEATABLE
  - SIMPLE TO LEARN

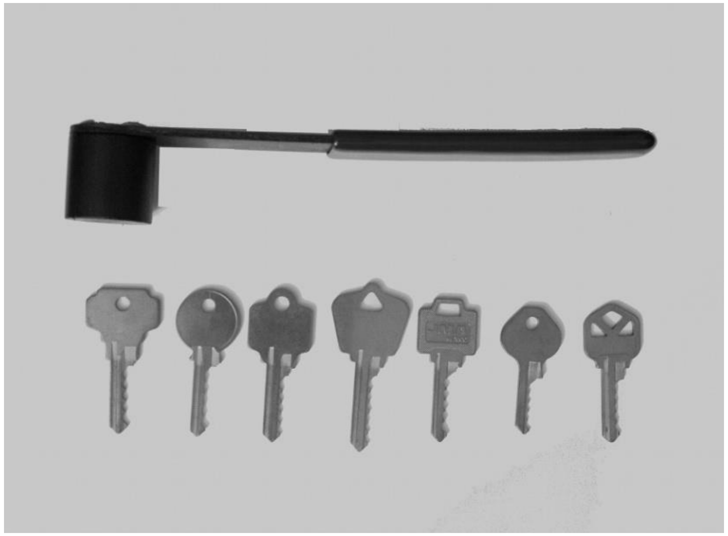


Photo by Jennie Rogers included with permission.

Bump Keys

- **Driver pins “jump” higher than the cylinder just for an instant**
- **If a light rotational force is applied, the cylinder will turn**
- **Lock bumping is a very fast method for opening the lock**
- **The lock is not damaged in any way**
- **Few key-pin locks cannot be bumped**

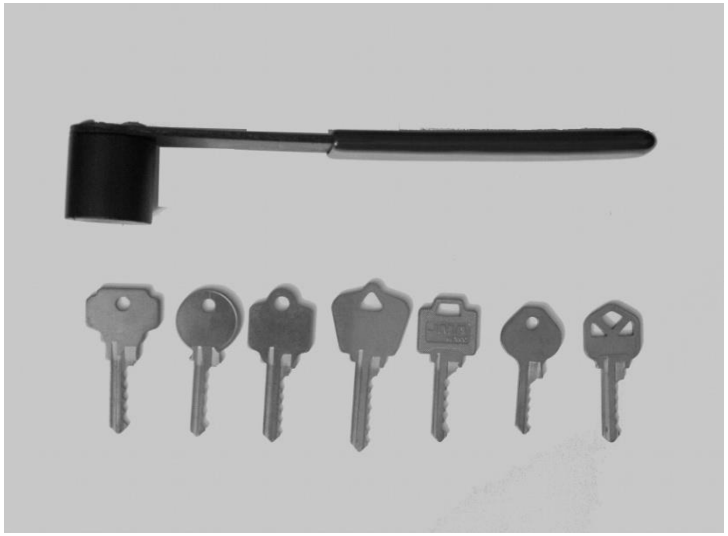


Photo by Jennie Rogers included with permission.

Pick Gun

- **Manual and electronic pick guns are a popular method for quick and easy ways of opening up doors**

- **The pick gun is used in a similar way but usually has a trigger that creates an upward movement that must be repeated rapidly to open the lock**

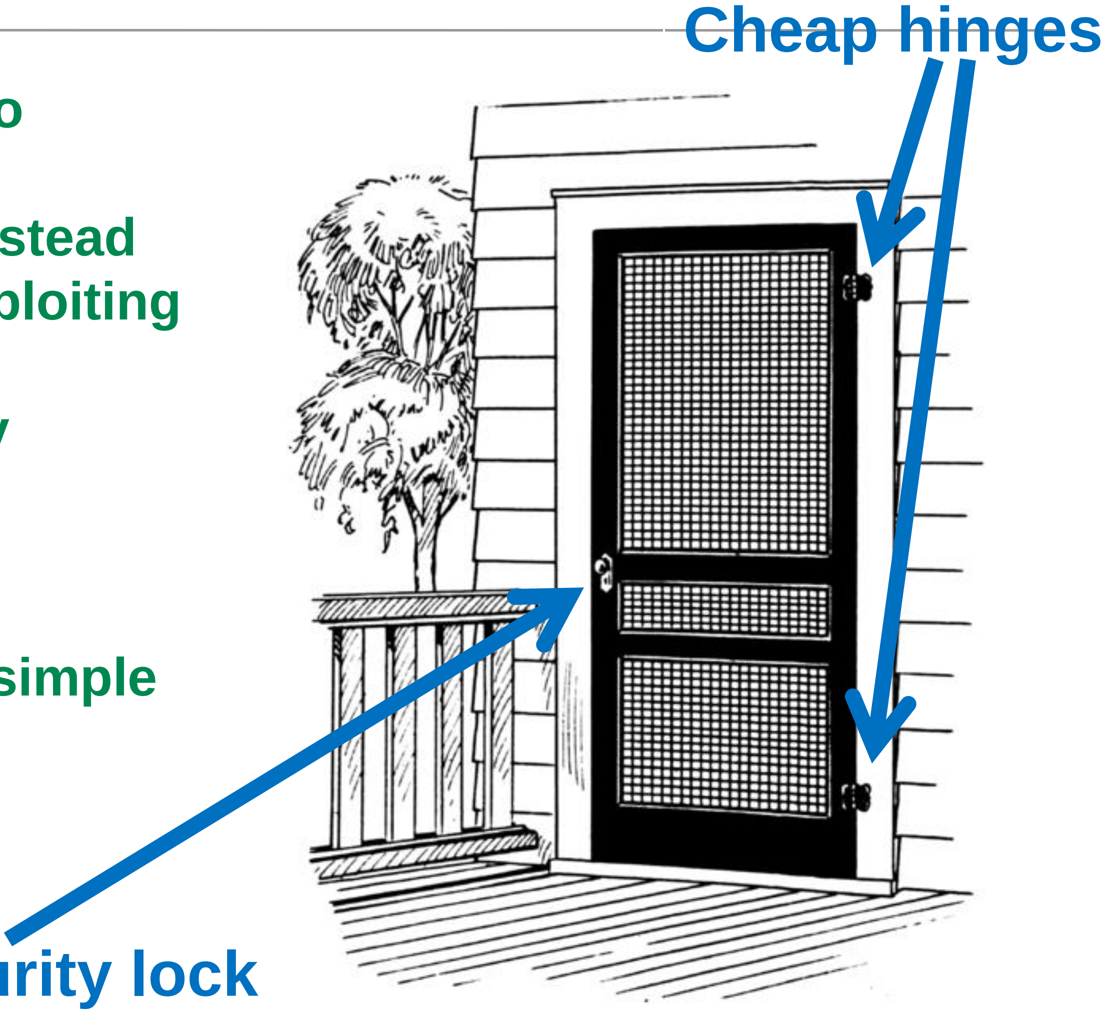
SPECIÁLNÍ ZAŘÍZENÍ
CYL 2
U-13459, sloužilo k vyhmatání zámkové vložky FAB
SPECIAL EQUIPMENT
used for lock picking of latch (making a door lock duplicate)

Public domain image from http://en.wikipedia.org/wiki/File:IDET2007_lock_picking_device.jpg

Side Channel Attacks

- **Rather than attempting to directly bypass security measures, an attacker instead goes around them by exploiting other vulnerabilities not protected by the security mechanisms.**

- **Side channel attacks are sometimes surprisingly simple to perform.**



Cheap hinges

High security lock

Public domain image by Pearson Scott Foresman from http://en.wikipedia.org/wiki/File:Screen2_%28PSF%29.png