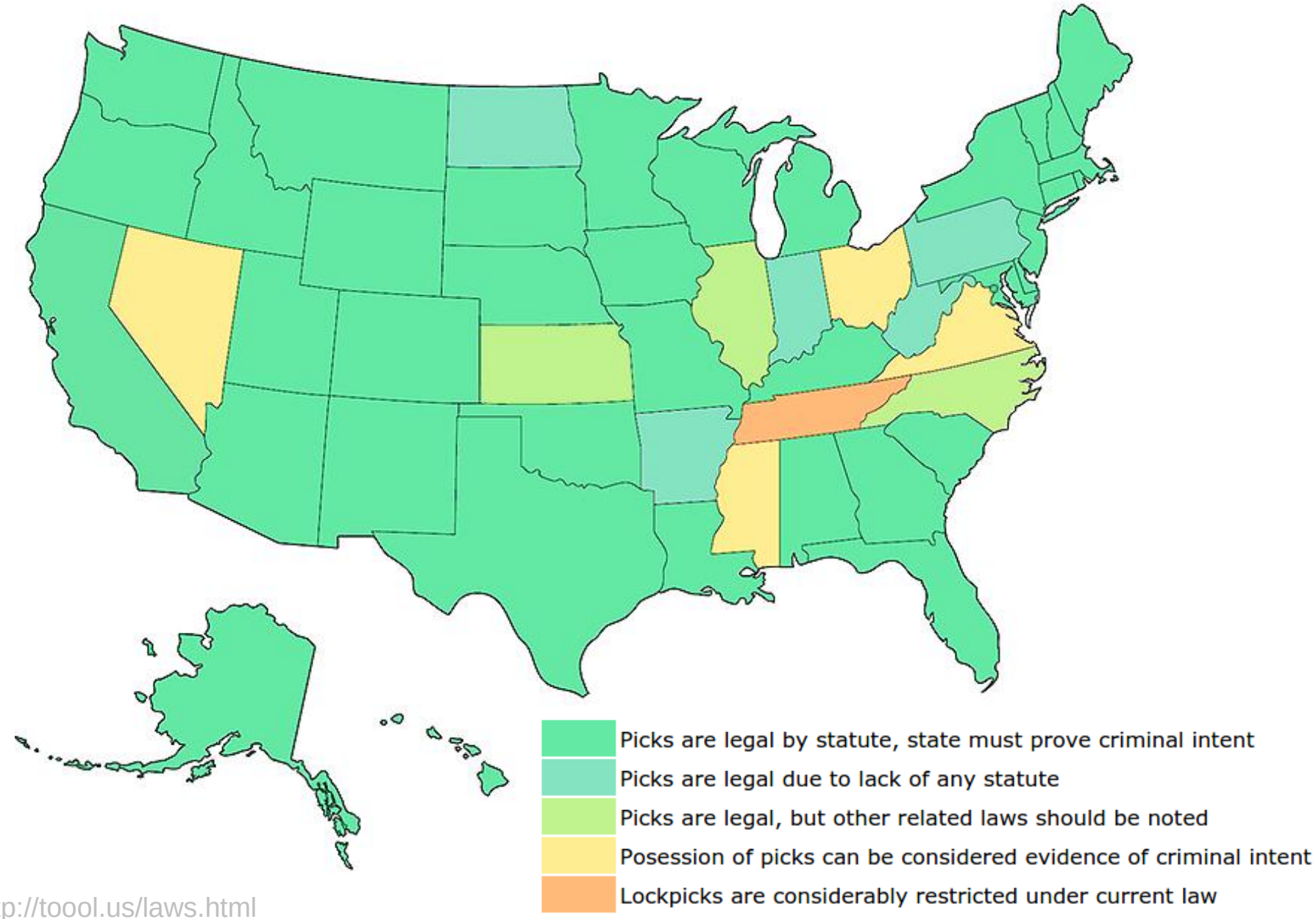
Physical Security: Locks and Keys

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



http://toool.us/laws.html

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 authentication, firewalls, and intrusion detection systems should protect against electronic methods 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

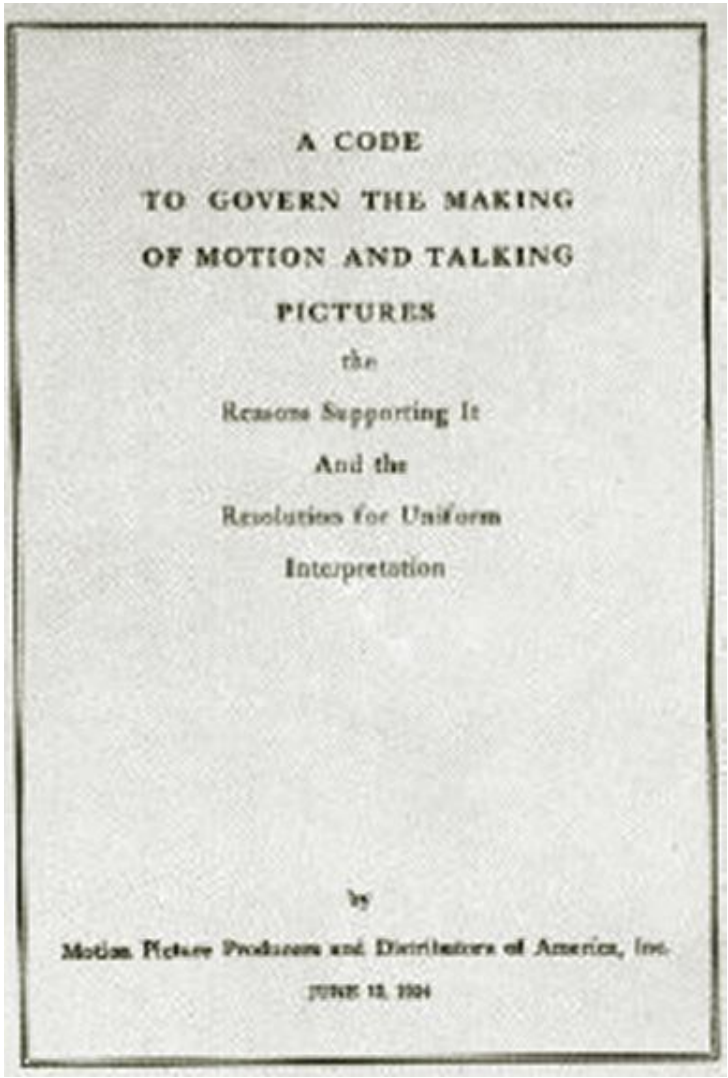
Pick vs. Bypass

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

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"

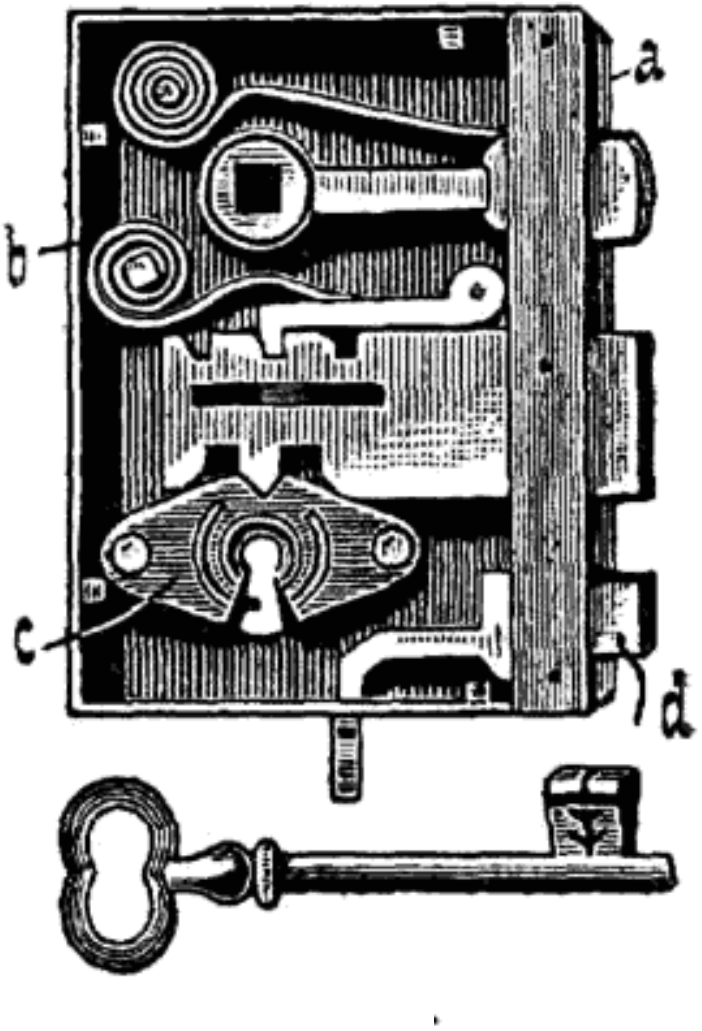

A CODE
TO GOVERN THE MAKING
OF MOTION AND TALKING
PICTURES
the
Reasons Supporting It
And the
Resolutions for Uniform
Interpretation
by
Motion Picture Producers and Distributors of America, Inc.
JUNE 13, 1934

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

LOCK TYPES

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



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

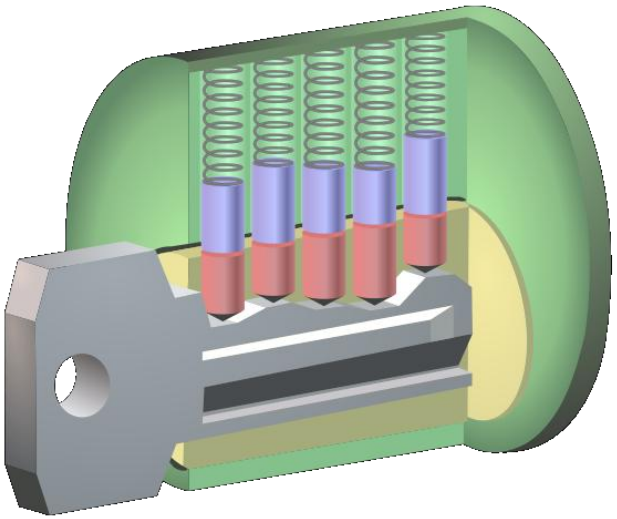
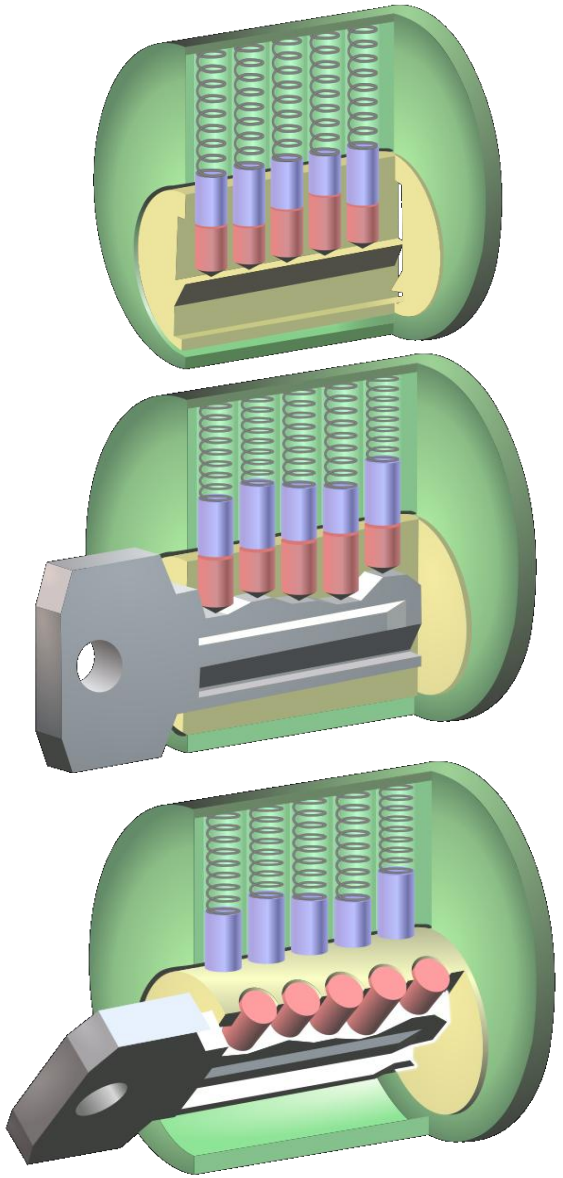


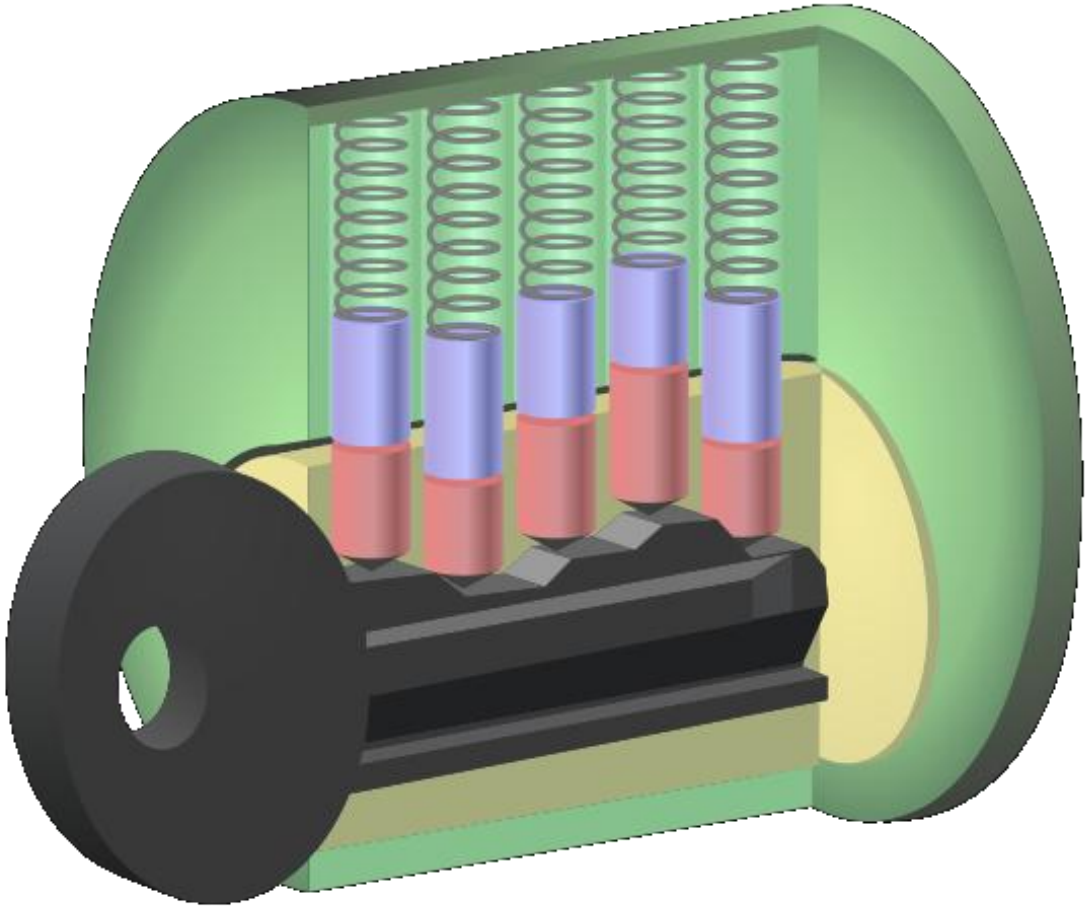
Image from http://en.wikipedia.org/wiki/File:Pin_tumbler_with_key.svg used with permission under Gnu Free Documentation License 1.2

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.



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.

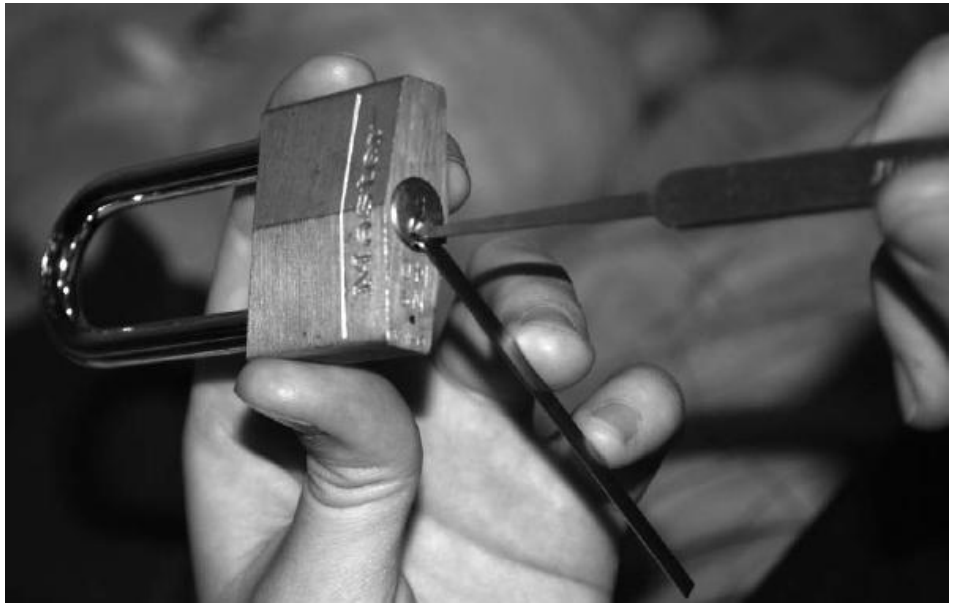
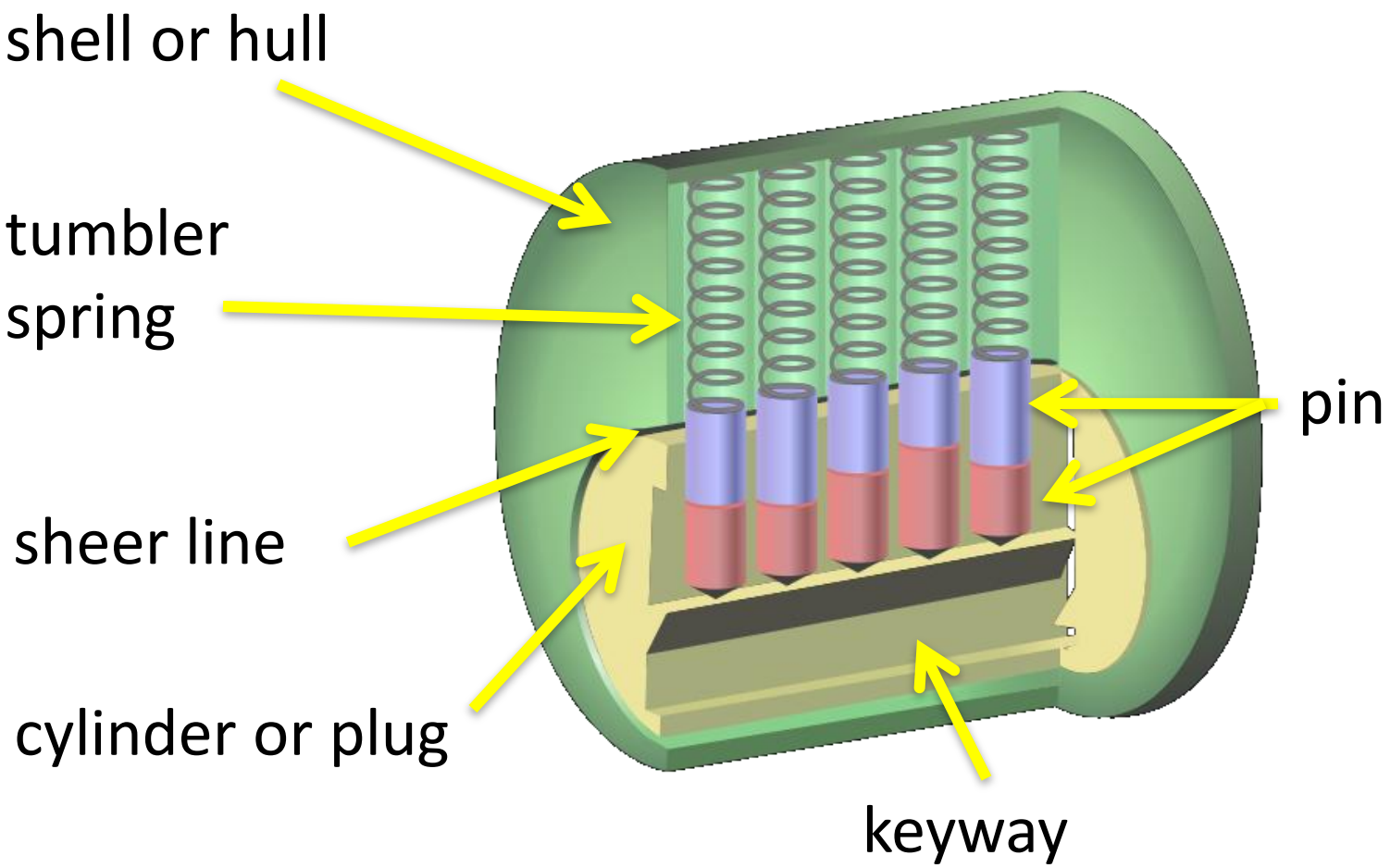


Photo by Dan Rosenberg included with permission.

LOCK PICKING

Terminology



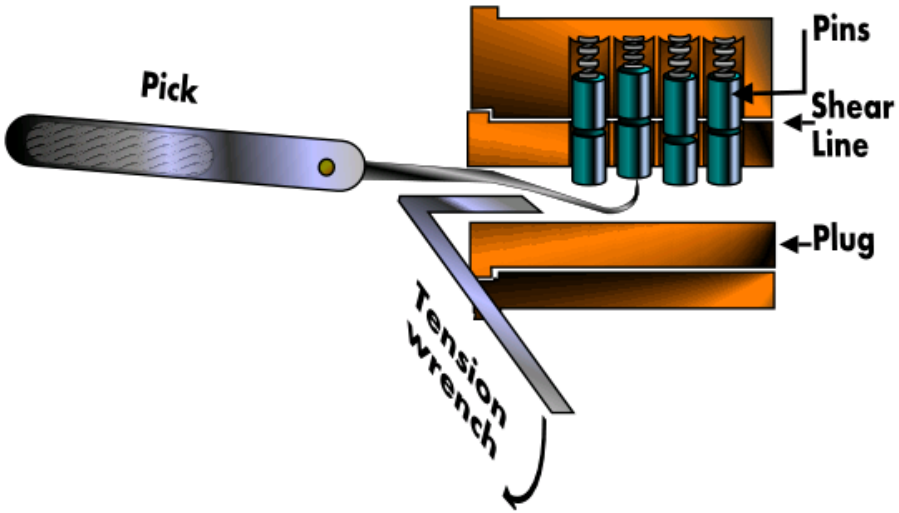
Lockpicking Tools

- 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



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

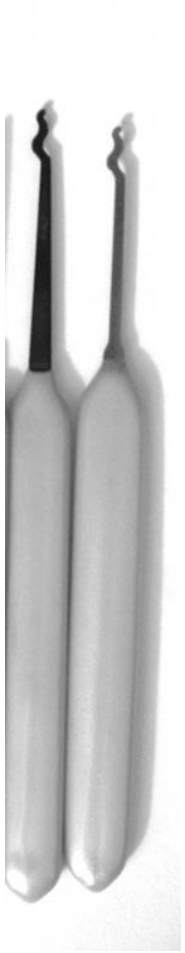


Photo by Jennie Rogers included with permission.

Lock picking defenses

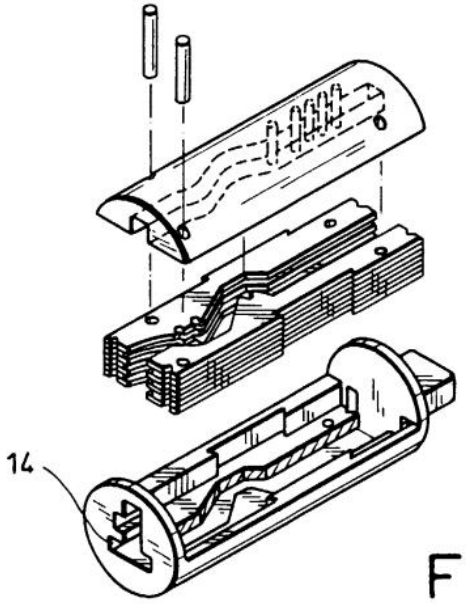
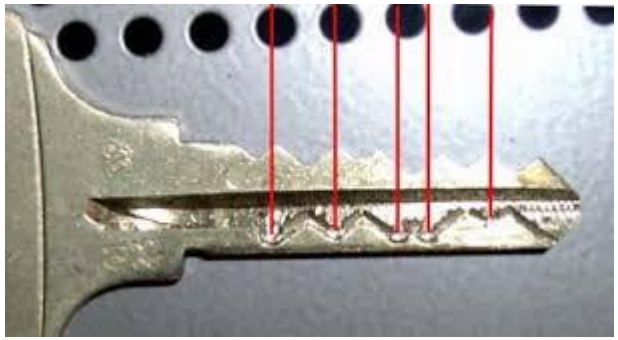
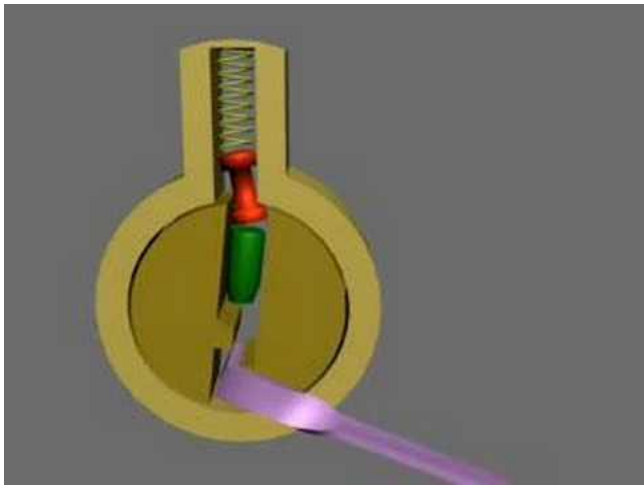


FIG.3 (PRIOR ART)





What about brute force?

- Suppose we have
  - 7 pin positions
  - 10 different possible pin heights
- Then the total number of possible locks is
  - $10^7 = 10{,}000{,}000$
- Not all these are possible, however, as it is difficult to put deep cuts next to shallow cuts.

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*

Cut all pin positions except *p* as known change key

Published by Matt Blaze at Penn

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

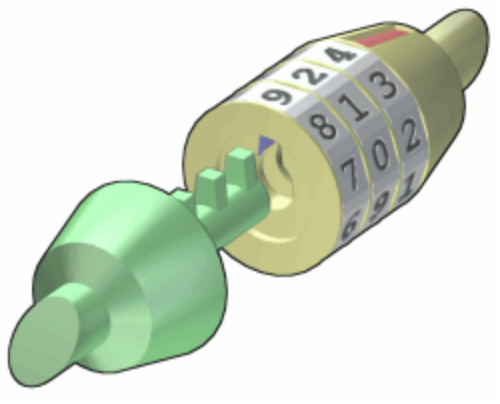
Search space is practically pruned by manufacturer specs

- maximum distance limit in legal adjacent cuts
- Older installations sometimes require MKs to be higher on the pin stack

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

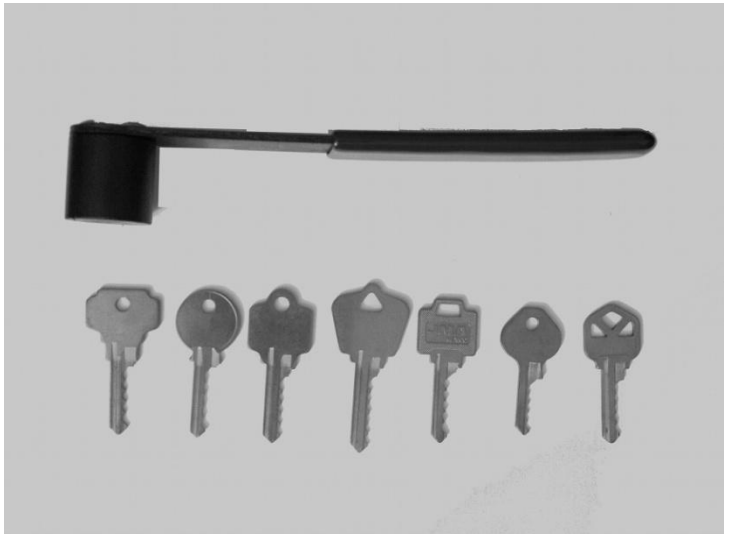


Photo by Jennie Rogers included with permission.

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
- Defense: different weighted pins

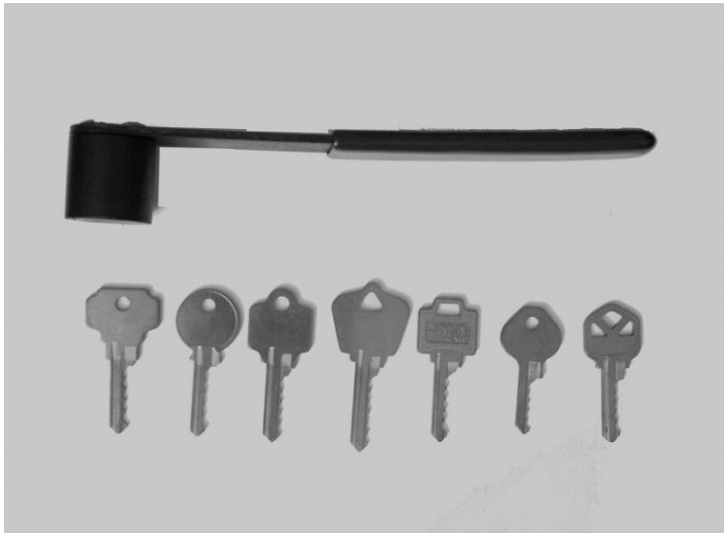


Photo by Jennie Rogers included with permission.