

Trojan Security

The Study of Lock Picking

by Chi So

University of Southern California
Sept. 2007

Disclaimer

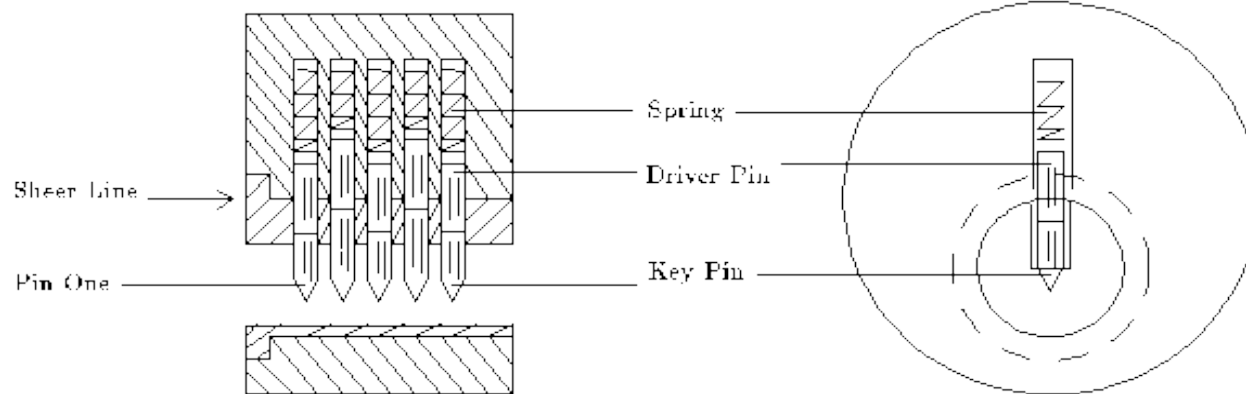
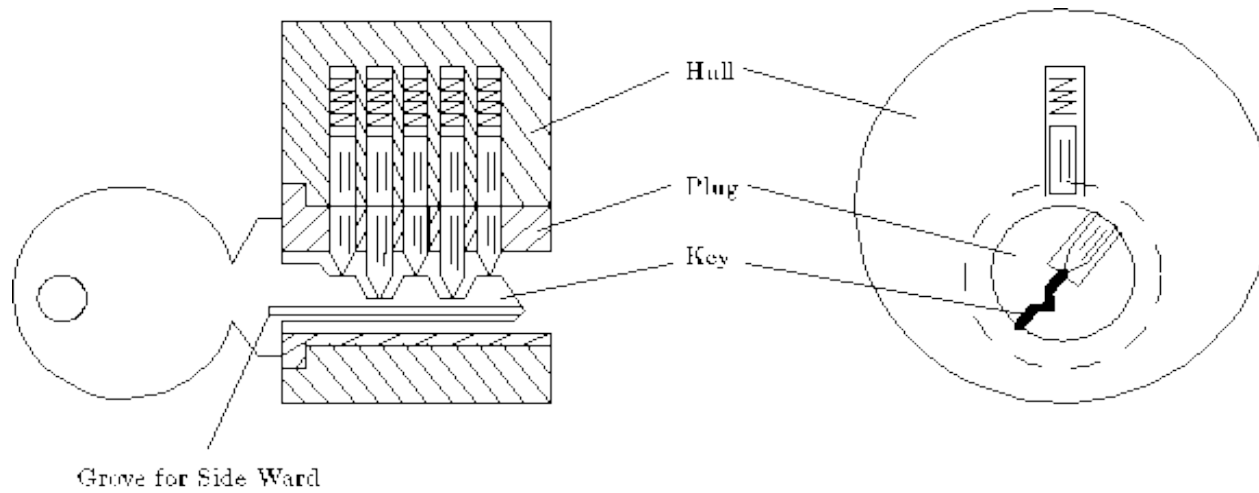
- All ideas discussed shall be used only for academic and lawful purposes. Under no circumstance shall it be used for illegal actions.

In other words, no evil stuff...

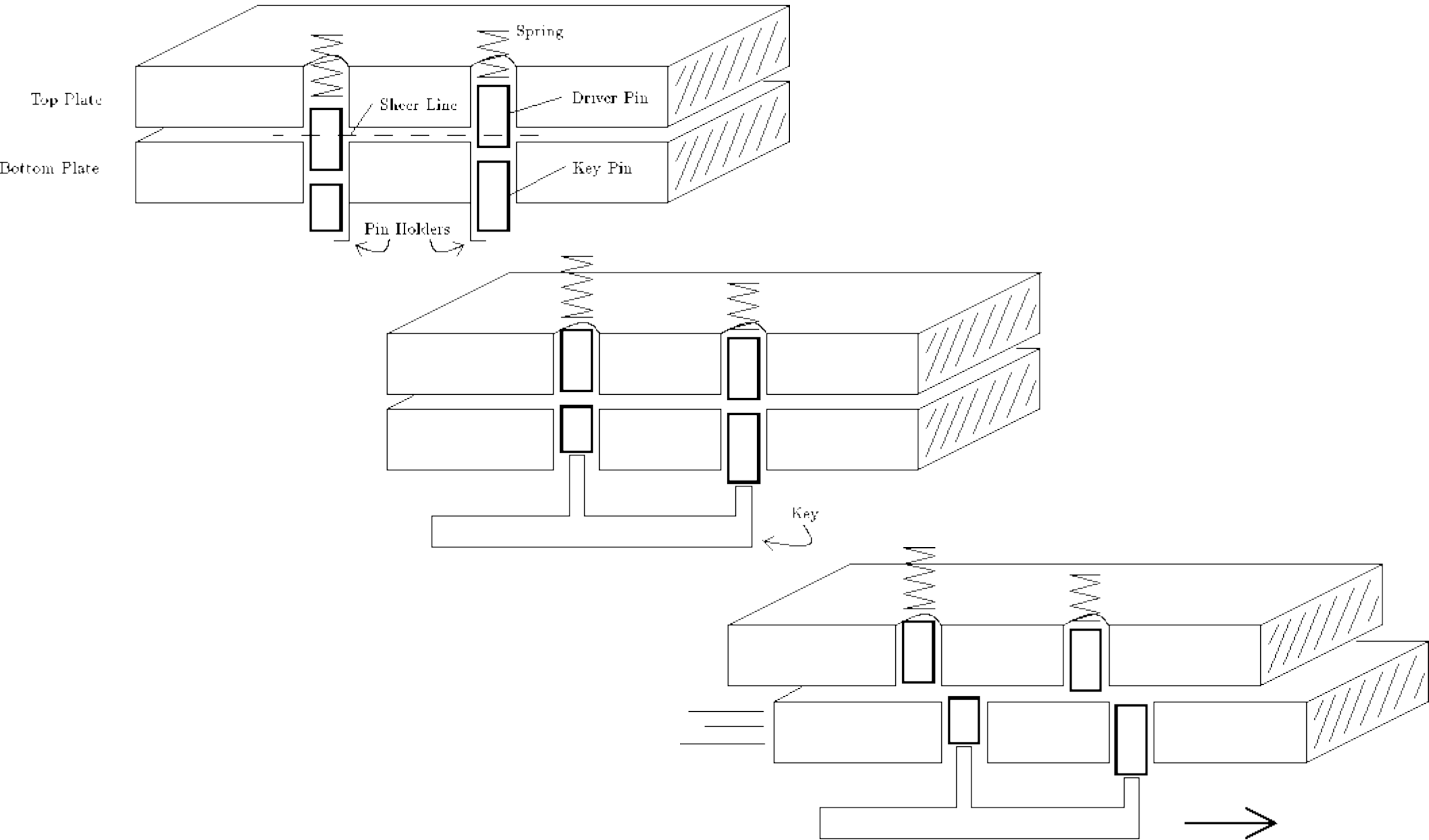
What is Lock Picking?

- “The theory of lock picking is the theory of exploiting mechanical defects”
 - MIT Guide to Lock Picking
- “is the art of unlocking a lock by analysing and manipulating the components of the lock device, without the original key.”
 - Wikipedia – Lock picking
- “To impress women!”
 - Chi

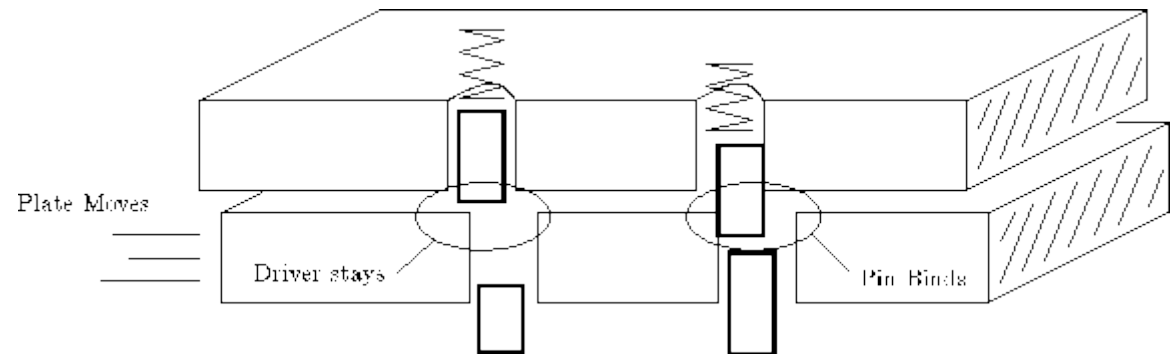
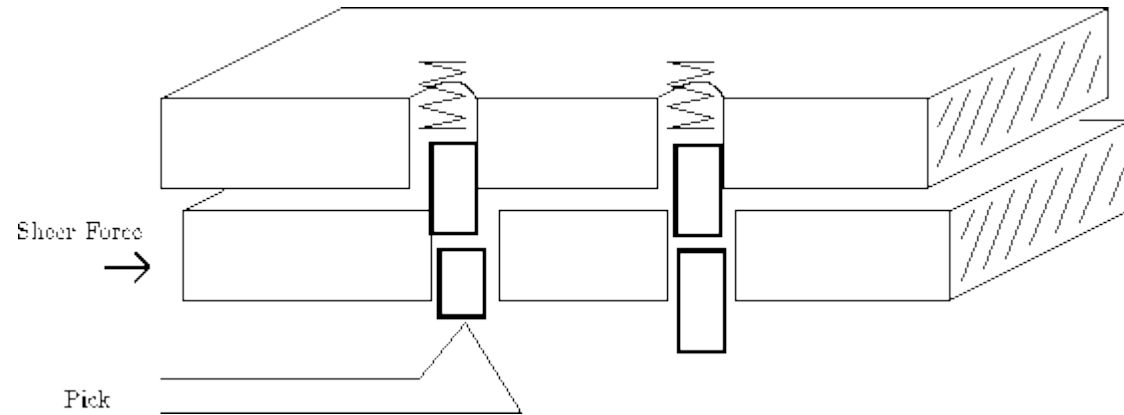
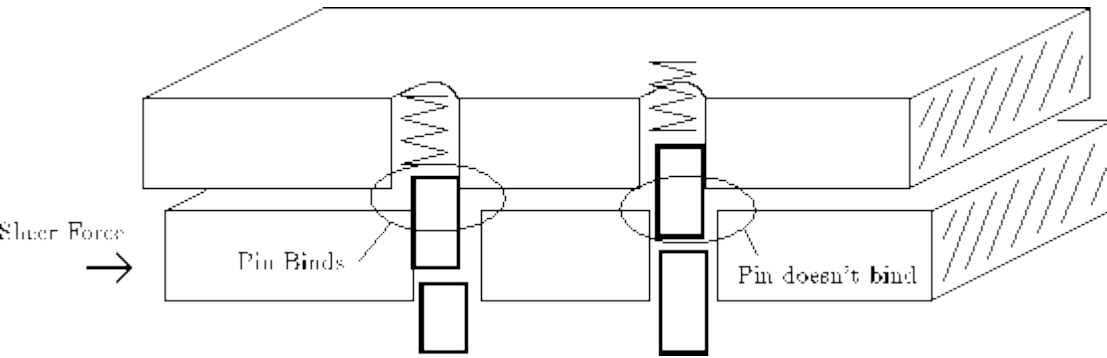
How Keys & Locks Work?



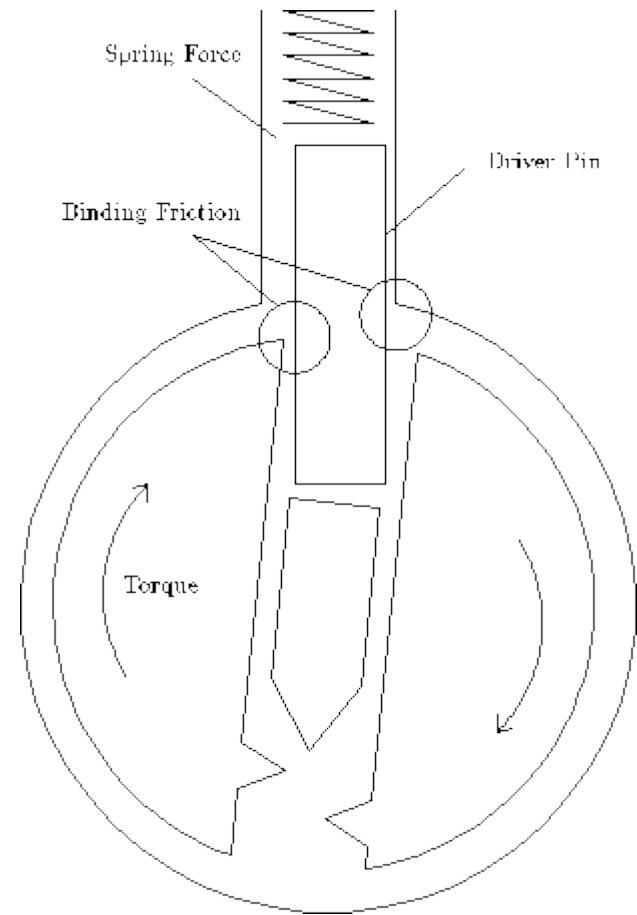
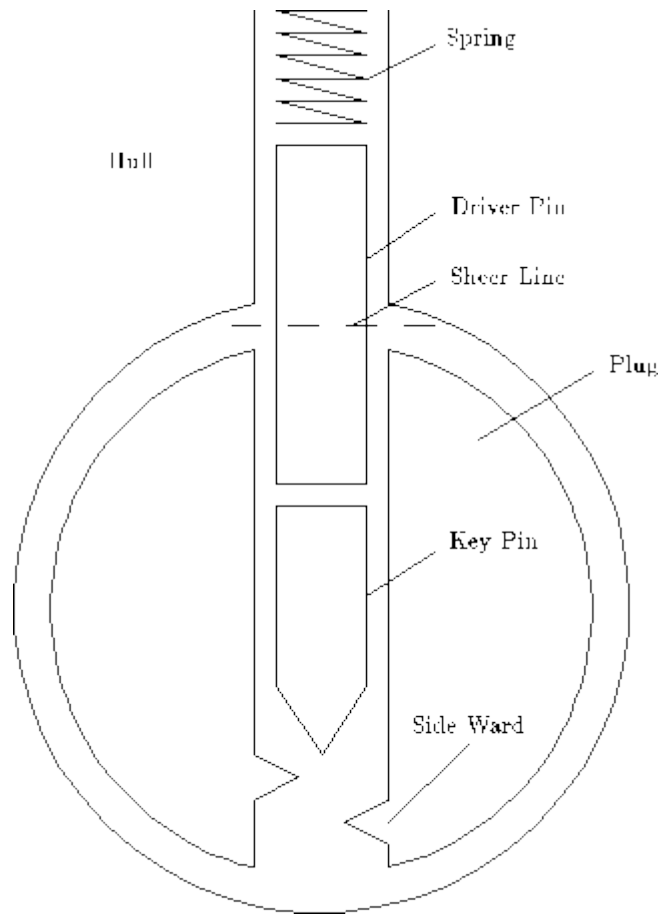
The Flatland Model



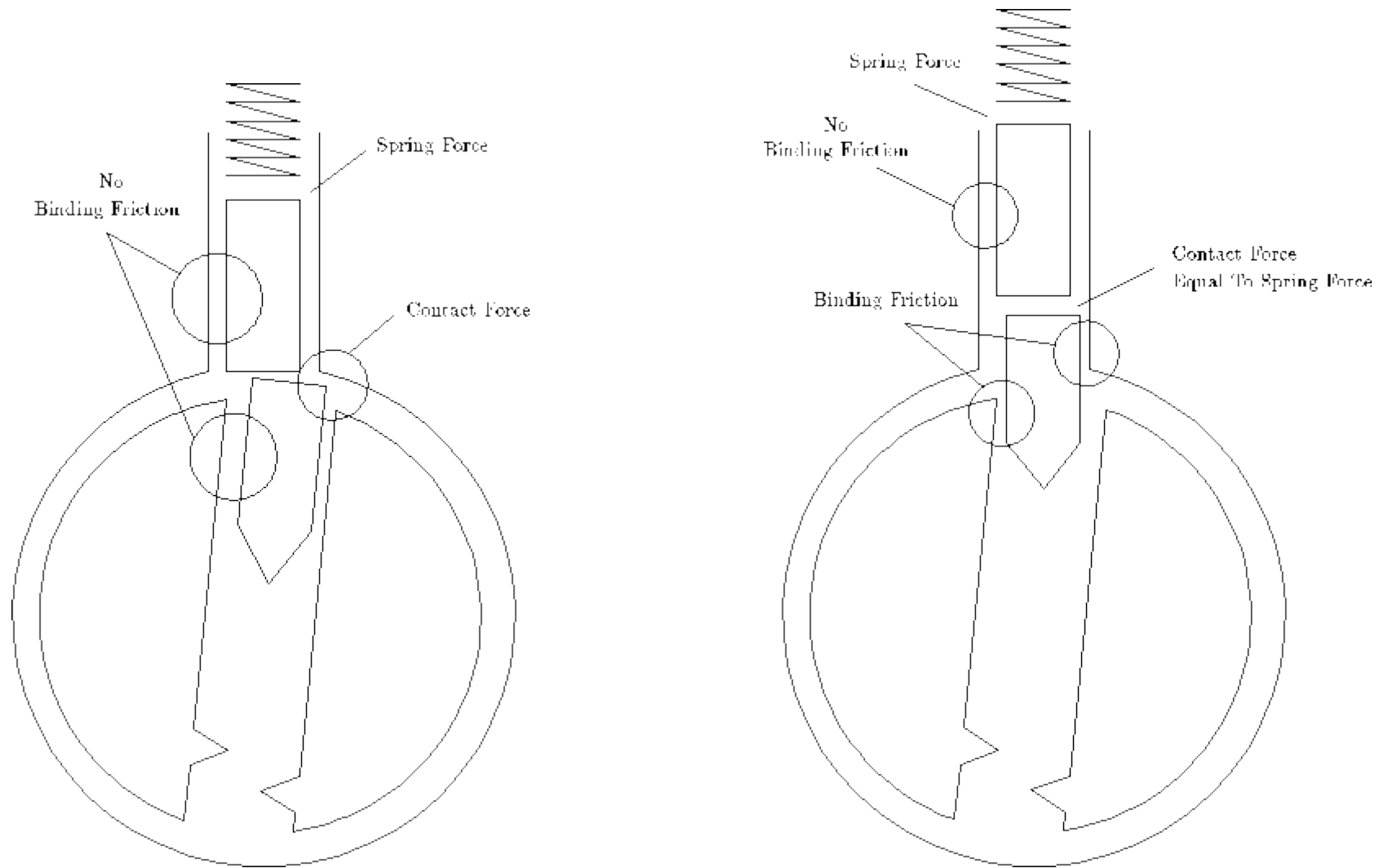
Basic Lock Picking



Pin Column Model



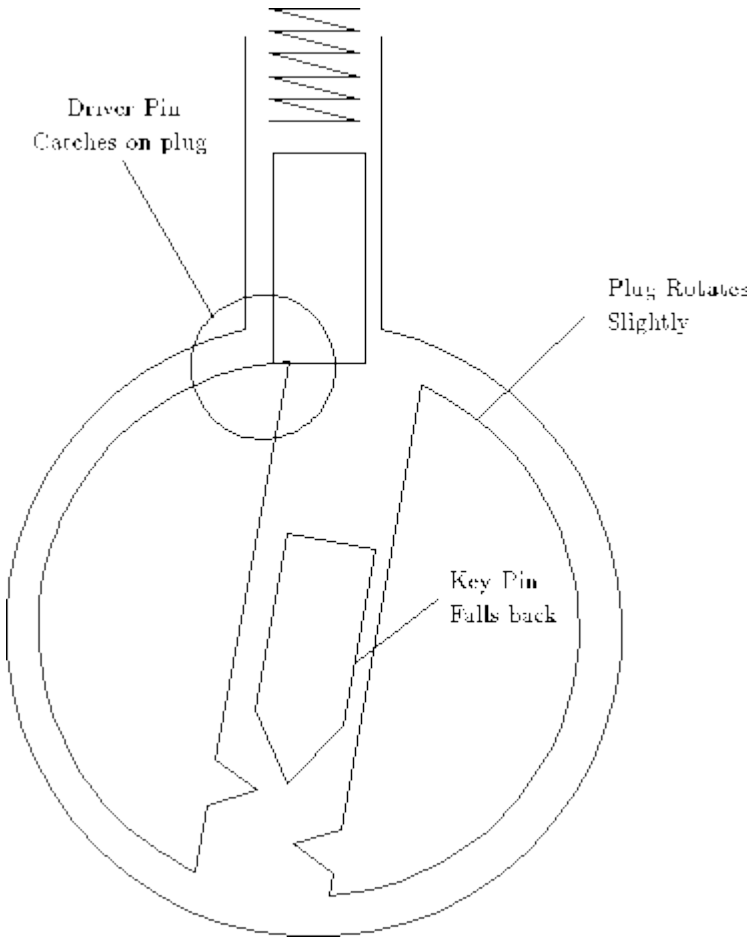
Pin Column Model



Scrubbing

- Quicker than single pin lock picking
 - Run your pick over all the pins (i.e. like scrubbing the floor) to set some of the pins in place.
 - Have to apply the right pressure and torque
- Scrubbing is quick since you don't need to focus on individual pins

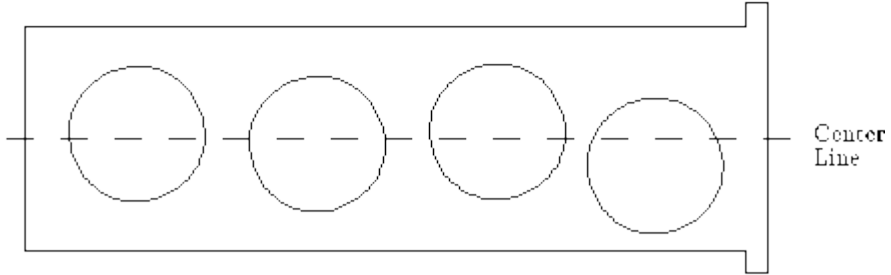
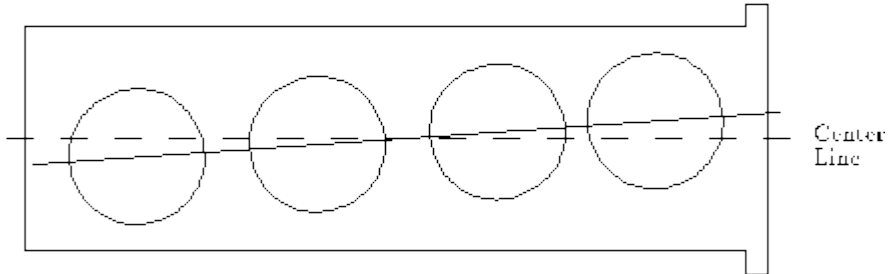
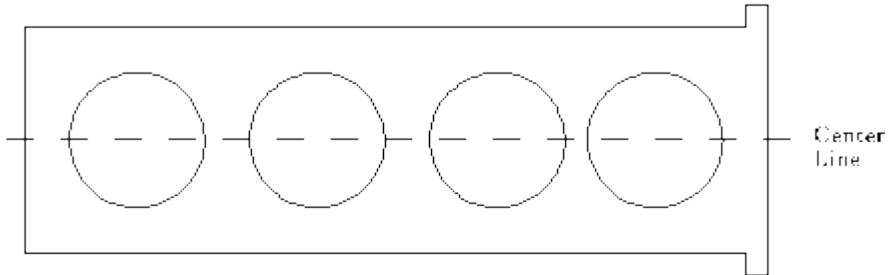
Scrubbing



Back

Top view of plug

Front



Random Hole Alignment

Scrubbing Step by Step

1. Insert the pick and torque wrench. Get an idea on the stiffness of the springs.
2. Apply small torque. Insert pick without touching the pins, quickly pull out to overcome the springs.
3. Keeping the torque, repeat to set all pins. If you think you failed start over.
4. If you feel most of the pins are set, continue with a slightly larger torque.

Some Food For Thought

- You don't need to look into the lock!
 - Unless you have X-Ray vision.. Seriously you don't need to look.
- Grace over power, you're not trying to destroy the lock.
- Picture the mechanics of the lock while you're picking
- Start with small torque and increase as you get more set.
- Experience!

Exercises For Lock Picking

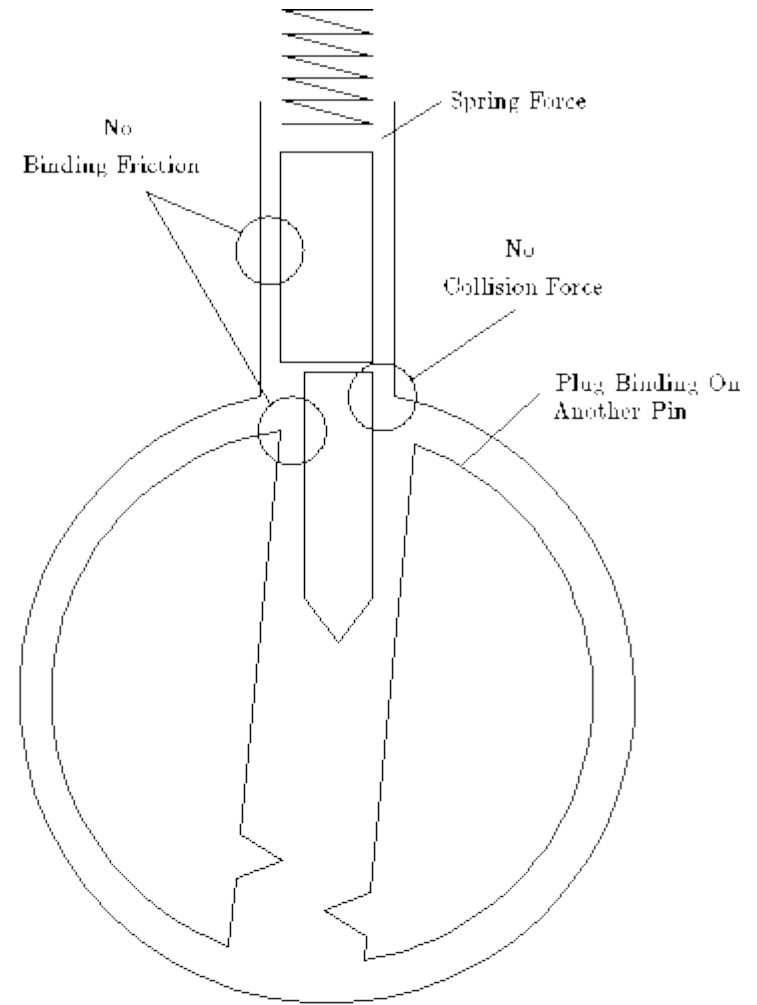
- Bouncing the Pick
 - Getting a feel on how to move the pins
- Picking Pressure
 - Moving the pick to get the idea on how much force to apply
- Picking Torque
- Identifying Set Pins
 - Listen/Feel the pins that that been set

Lock Picking Issues

- Which way to Turn?!?!?
- How Far to Turn?
 - Usually 90 for desk/filing cabinets/padlocks
 - Deadbolt might require 360
 - Doors might require 180
- Pins Not Setting
 - Slow down, take a deep breath
 - Start Over

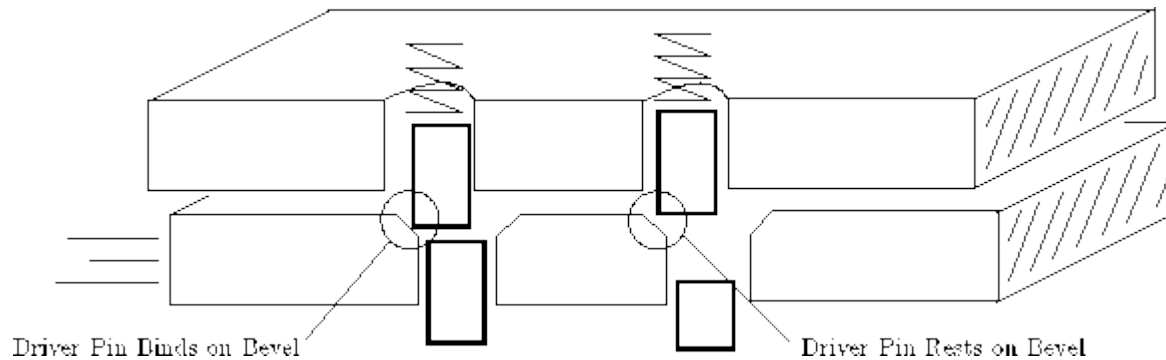
Lock Picking Defenses

- Pin Diameter
 - Feels funny
 - Have to be careful
 - Defense against picking



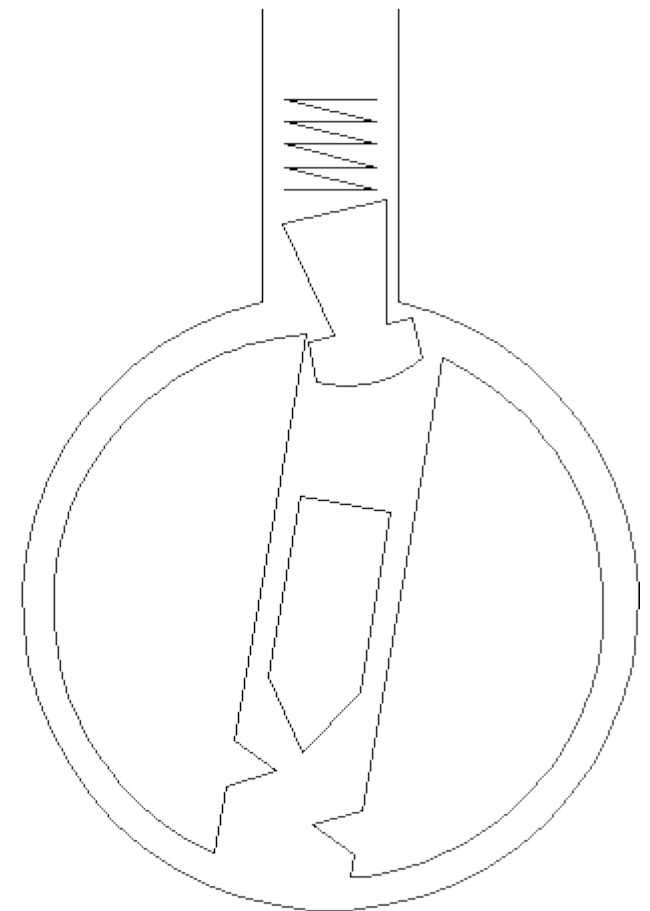
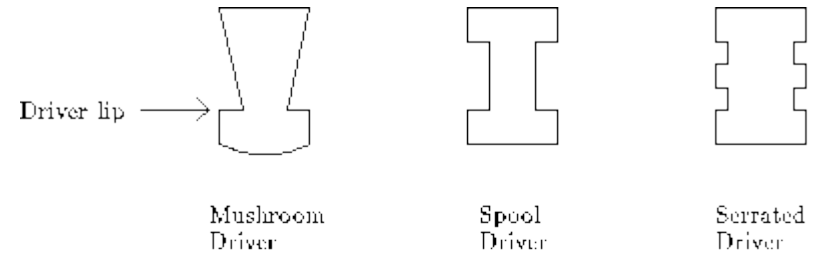
Beveled Holes, Rounded Pins

- Defense against scrubbing
- Makes you think you got the pins gets
- If the pin is on the Bevel, it might not move
- Restart if you can't make it move.

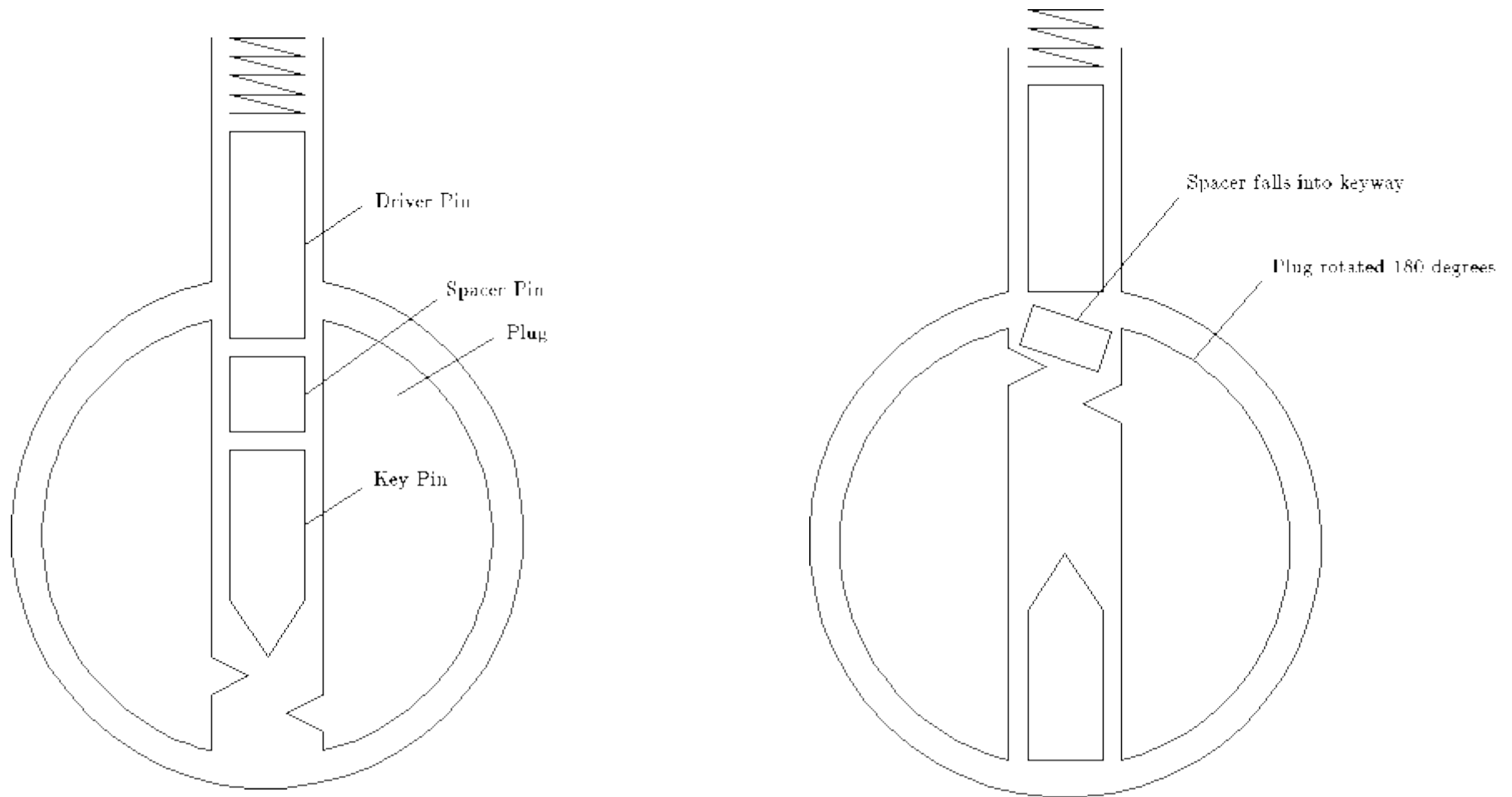


Driver Pin Shape

- Makes individual picking slightly more difficult
- Does it stop key bumping?
- Use light torque, heavy pressure.



How Do Master Keys Work?



Vibration Picking / Key Bumping

- The idea is similar to Newton's Cradle

Defcon 3 Idea Video

- <http://www.youtube.com/watch?v=XQDR-DBQRfI>



Key Bumping Checklist

- Need a bumpkey

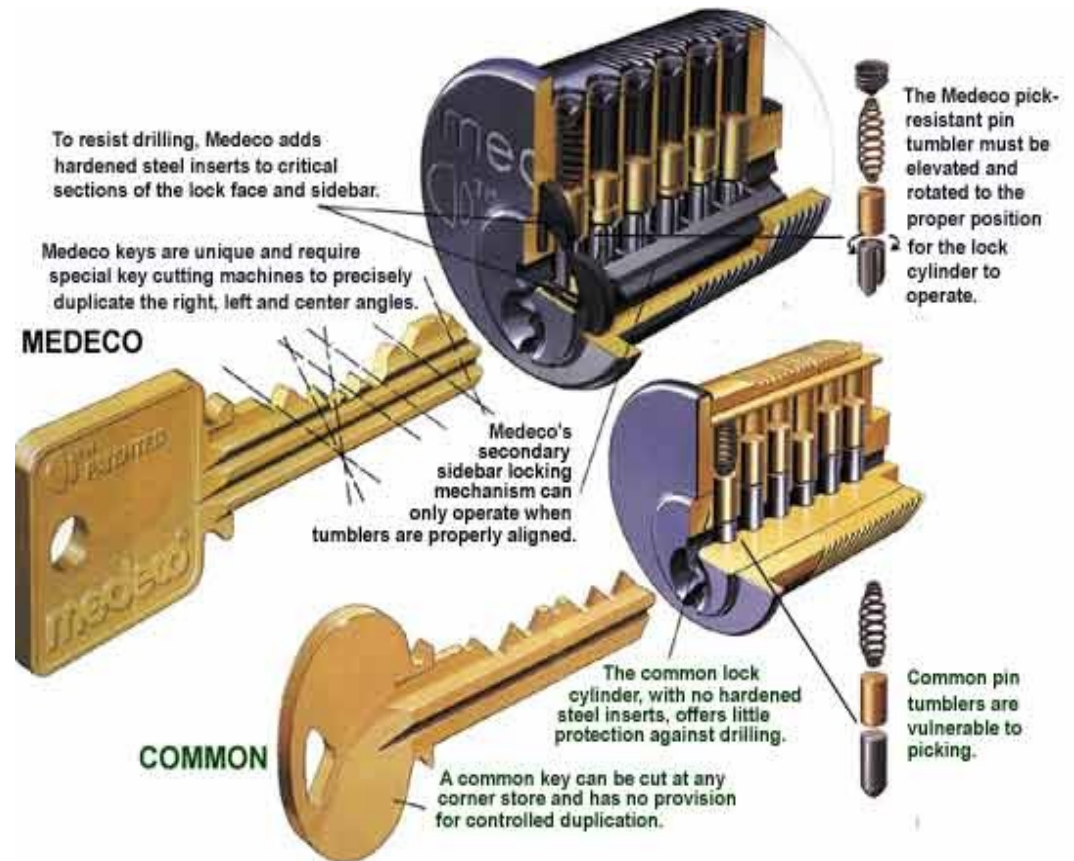


Key Bumping Defenses

- Modified shape of driver pin,
- Gel - <http://www.pickbuster.co.uk/>
- High Security Locks
- A mean dog with a taste for human blood
- <http://www.youtube.com/watch?v=kUJWc7rj8I>

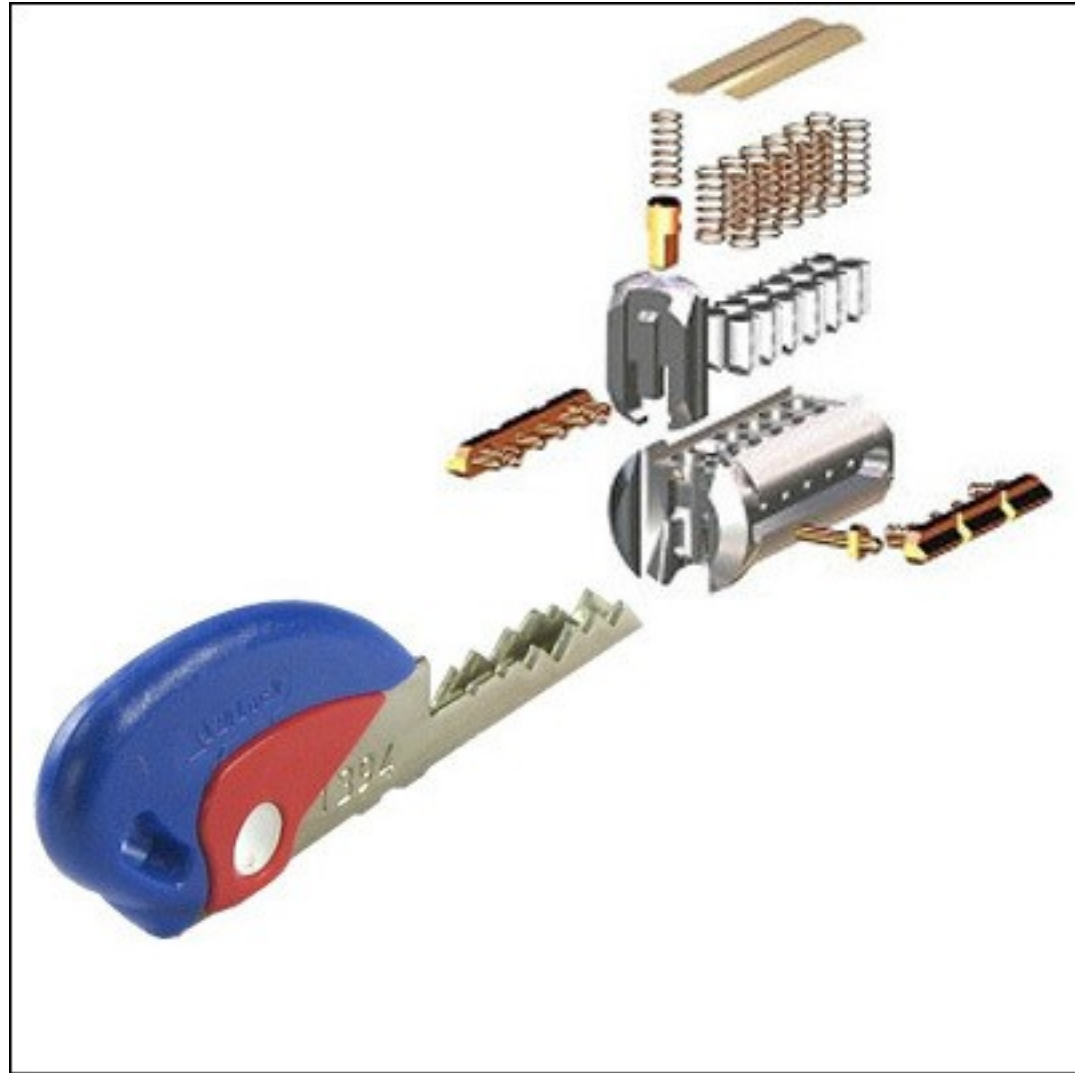
High Security Locks

- Medeco
- <http://www.youtube.com/watch?v=TRcB2c-tYE4>
- <http://www.youtube.com/watch?v=AoISzIkmVdc>



High Security Locks

- BiLock



Are We Secure?



“Oh Noes!!”

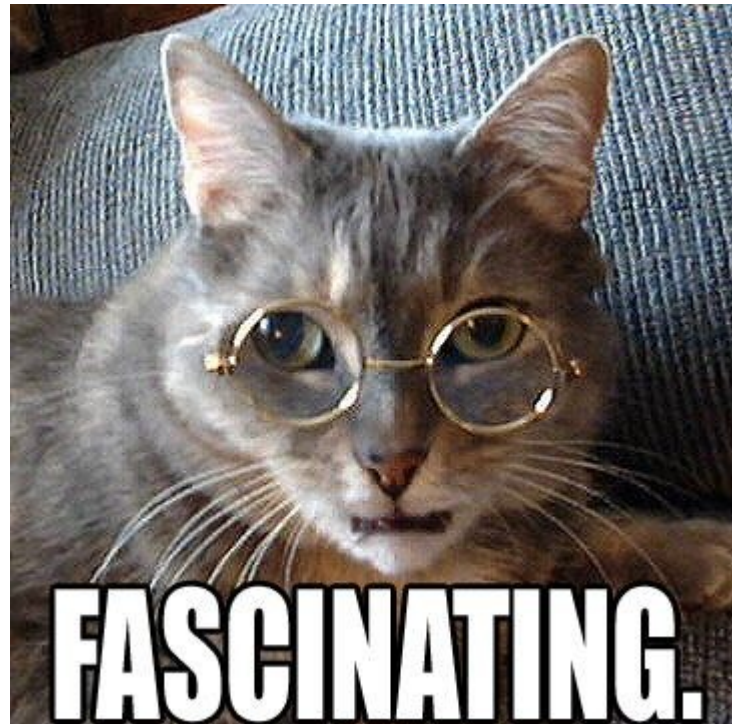
Other Defenses

- Guard Dog/Cat/Elephant
- Alarm System != Security System
- Better Locks



Are Lock Picks Legal?

- <http://www.leginfo.ca.gov/cgi-bin/displaycode?se>
- In California, YES as long as you're not doing something illegal. Also you must have someone's permission to pick their property.



References

- Images from “MIT Guide to Lock Picking”
 - Hosted on <http://www.lysator.liu.se/mit-guide/>
- “MIT Guide to Lock Picking” - Ted the Tool
 - MUST READ!
- Wikipedia – Lock Picking & Lock Bumping
 - en.wikipedia.org