WARNING: This presentation is intended to educate and describe the inner workings of common lock mechanisms, methods useful to manipulate locks owned by or under full control of the person taking part of this con, and means to protect themselves from intruders possessing bypass techniques contained herein. The presenter/author makes no claims as to the accuracy of the following information, nor endorses or encourages activities of malevolent intent.

LOCKPICKING : FINGERING LOCKS FOR FUN

A presentation for PinoyGreyhat.org

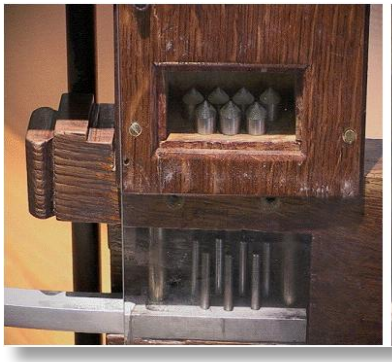
JollyMongrel (arf arf)

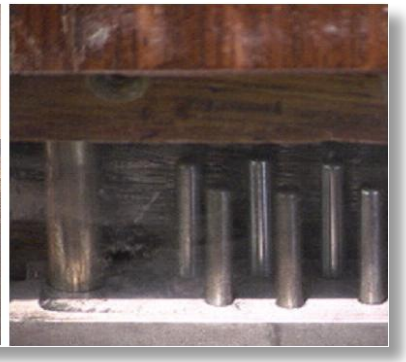
"And the key of the House of David will I lay upon His Shoulder."
-Isaiah, CH. XXII, V. 22

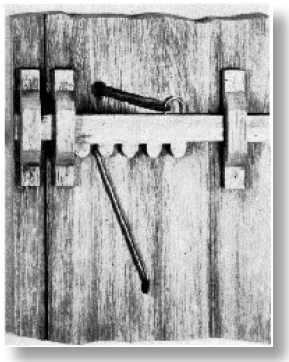
BACKGROUND (7 MINUTES PLEASE)

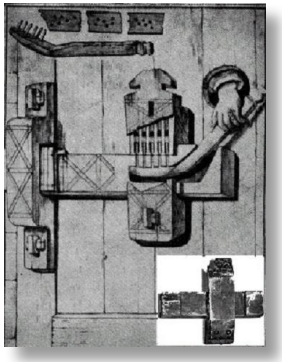
Lock | Brief History

- Egyptians
  - The oldest known lock was found by archeologists in the Khorsabad palace ruins near Nineveh. The lock was estimated to be 4,000 years old. It was a forerunner to a pin tumbler type of lock, and a common Egyptian lock for the time. This lock worked using a large wooden bolt to secure a door, which had a slot with several holes in its upper surface. The holes were filled with wooden pegs that prevented the bolt from being opened.
  - *"the gate was fastened by a large wooden lock, the wooden key with iron pegs at one end to lift the iron pins in the lock, being so much as a man can carry."* – *Joseph Bonomi in Ninevah and its Palaces*









Lock | Brief History

- Greek
  - Greeks are credited with making simple bolt-locking mechanisms

"Whenever the parts of a lock which come in contact with the key are affected by any pressure applied to the bolt, or to that portion of the lock by which the bolt is withdrawn and shot, in such a manner as to indicate the points of resistance to the withdrawal or shooting of the bolt, such a lock can be picked. Where a key can enter, a false key, whether in key form or in the form of bent wire, can also enter."

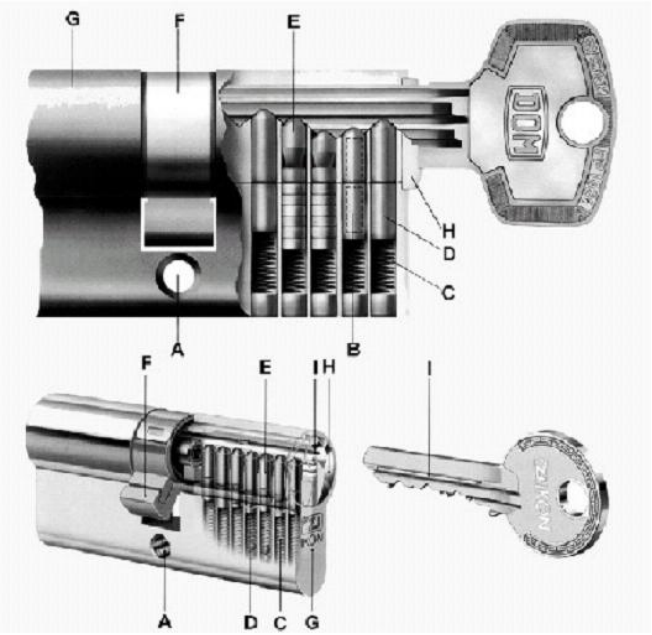
A.C.HOBBS

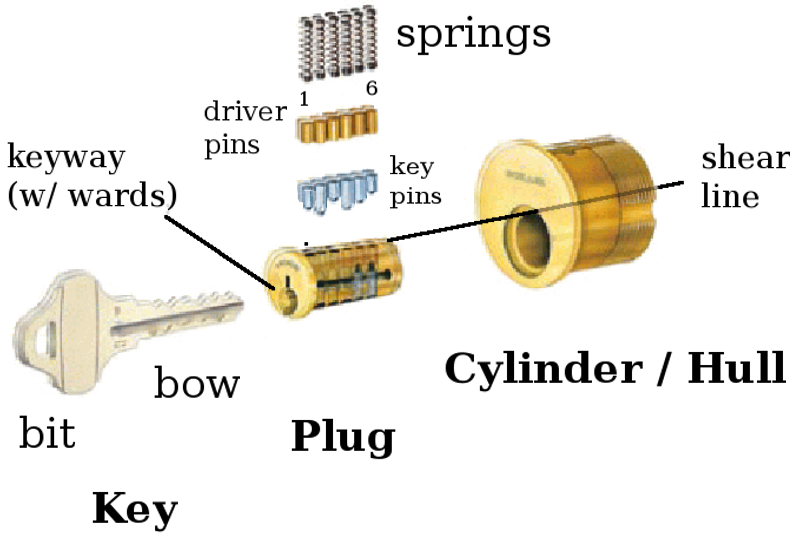
LOCK ANATOMY (7 MINUTES PLEASE)

Pin Tumbler | Anatomy

PARTS OF A PIN-TUMBLER LOCK

- **Shell** - The shell contains all of the internal components: the upper and lower sets of pins, the springs, and the plug.
- **Plug** - This is the active, rotating component of the pin tumbler lock.
- **Keyway** - The keyway limits the number of keys that can enter the lock and thereby increases security.
- **Key** – A device used to unlock the lock.
- **Pin Chamber** – a bored chamber in the shell containing the pin tumblers and spring
- **Pins** – also called tumblers. Provides the security locking mechanism.
- **Spring** – Springs provide the bias to force each tumbler-set into the plug and to maintain the integrity of the pin-stack while the key is inserted and removed.
- **Shear line** – The level to which all pins must be raised in order for the plug to rotate

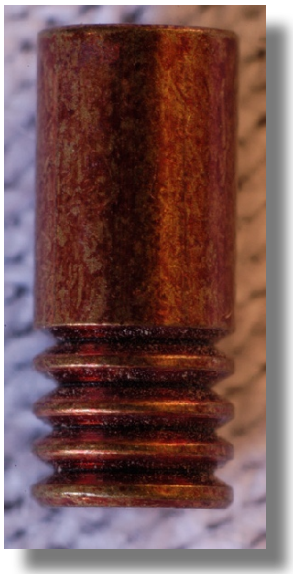




Security Pins | Anatomy

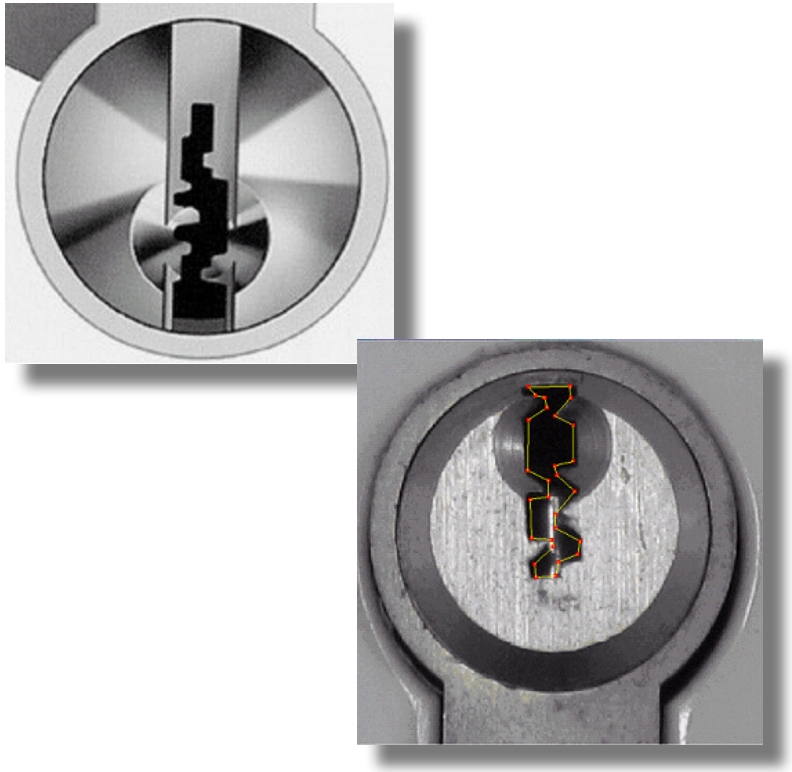
SECURITY TUMBLERS

- Spool
- Serrated
- Mushroom



Keyways | Anatomy

Paracentric Keyway



"Whenever the parts of a lock which come in contact with the key are affected by any pressure applied to the bolt, or to that portion of the lock by which the bolt is withdrawn and shot, in such a manner as to indicate the points of resistance to the withdrawal or shooting of the bolt, such a lock can be picked. Where a key can enter, a false key, whether in key form or in the form of bent wire, can also enter."

A.C.HOBBS

LOCK OPERATION (7 MINUTES PLEASE)

"Whenever the parts of a lock which come in contact with the key are affected by any pressure applied to the bolt, or to that portion of the lock by which the bolt is withdrawn and shot, in such a manner as to indicate the points of resistance to the withdrawal or shooting of the bolt, such a lock can be picked. Where a key can enter, a false key, whether in key form or in the form of bent wire, can also enter."

A.C.HOBBS

LOCK EXPLOITATION (20-30 MINUTES PLEASE)

Destructive | Lock Exploitation

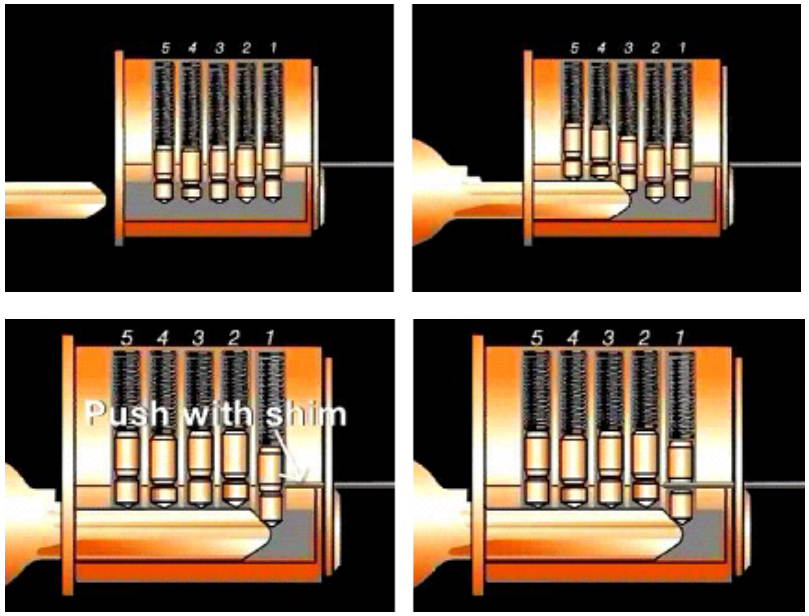
Mechanical Brute Force Attack

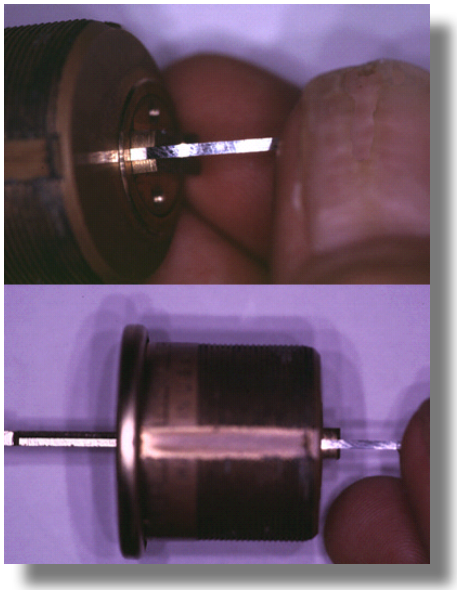
- The most direct way to bypass locks
- Commonly used by burglars
- Used for one-time entry

Covert | Lock Exploitation

Shimming

Shimming is a technique whereby pressure is applied against the edge of each tumbler, in succession, by a very thin strip of metal called a shim. It is inserted from the back of the lock in the clearance area between the plug and shell. As each tumbler is forced upward, the shim will slip between the tumblers as they cross shear line.





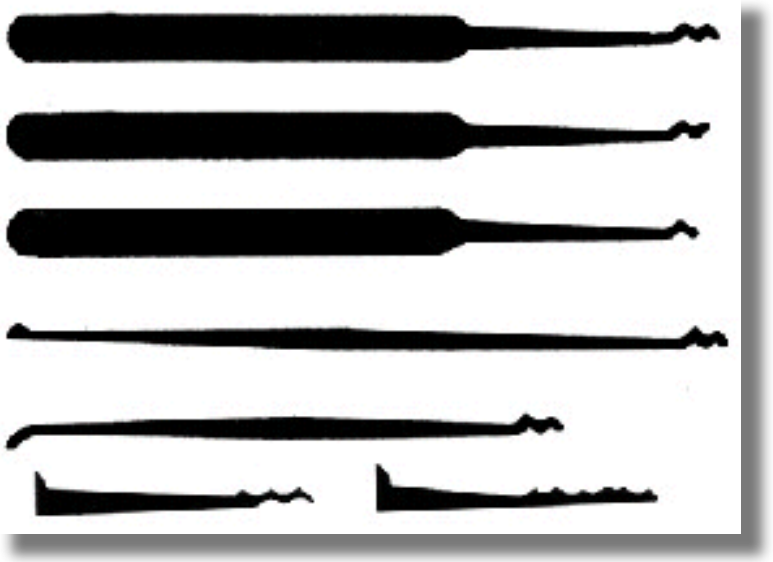
Covert | Lock Exploitation

Bumping or 999 rapping

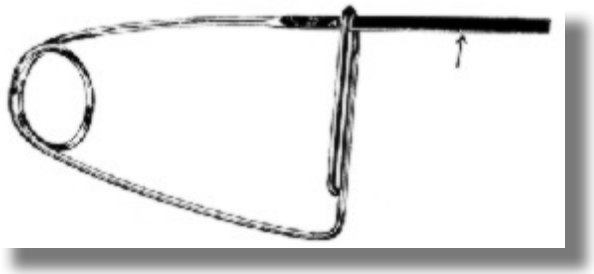
Lock bumping is a lock picking technique for opening a pin tumbler lock using a specially-crafted bump key. One bump key will work for all locks of the same type.

Covert | Lock Exploitation

Raking



Impact Guns (Pick/snap guns)



Covert | Lock Exploitation

Single Pin Picking (SPP)

"Whenever the parts of a lock which come in contact with the key are affected by any pressure applied to the bolt, or to that portion of the lock by which the bolt is withdrawn and shot, in such a manner as to indicate the points of resistance to the withdrawal or shooting of the bolt, such a lock can be picked. Where a key can enter, a false key, whether in key form or in the form of bent wire, can also enter."

A.C.HOBBS

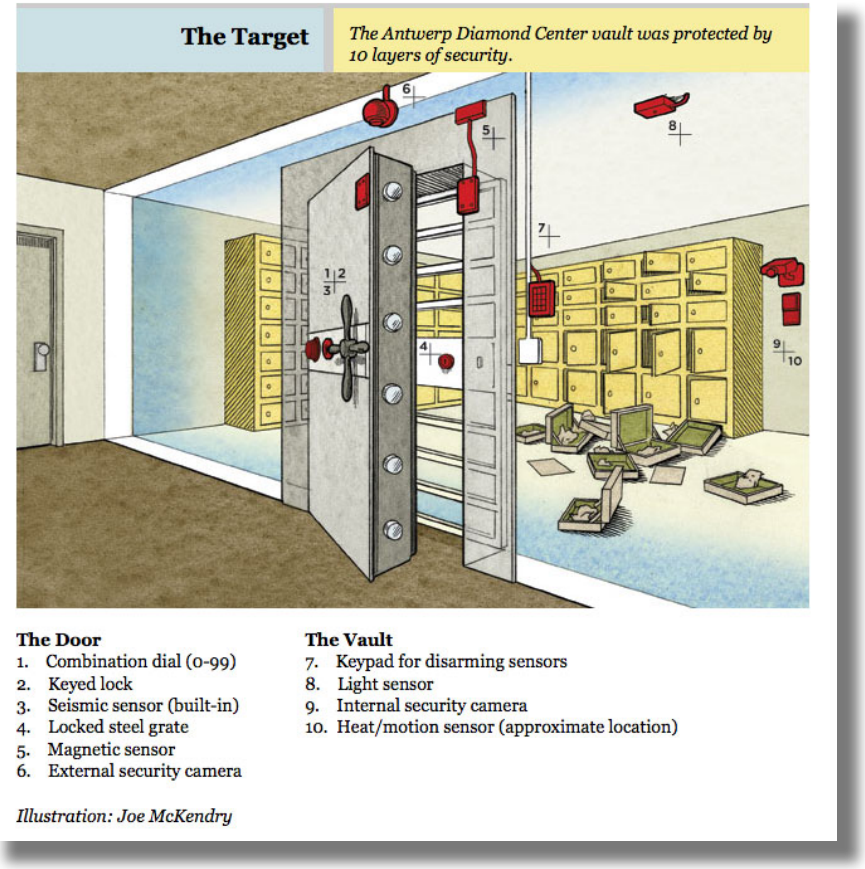
CASE STUDY (10 MINUTES)

Antwerp Diamond Heist | Case Study

In February 2003, Notarbartolo was arrested for heading a ring of Italian thieves *(Leonardo Notarbartolo, Elio D'Onorio, aka the Genius; Ferdinando Finotto, alias the Monster;Pietro Tavano, alias Speedy and the oldest in the team coined as "King of Keys" (Antonio Falleti)).* They were accused of breaking into a vault two floors beneath the Antwerp Diamond Center and making off with at least $100 million worth of loose diamonds, gold, jewelry, and other spoils.

Antwerp Diamond Heist | Case Study

The vault was thought to be impenetrable. It was protected by 10 layers of security, including infrared heat detectors, Doppler radar, a magnetic field, a seismic sensor, and a lock with 100 million possible combinations. The robbery was called the heist of the century, and even now the police can't explain exactly how it was done.



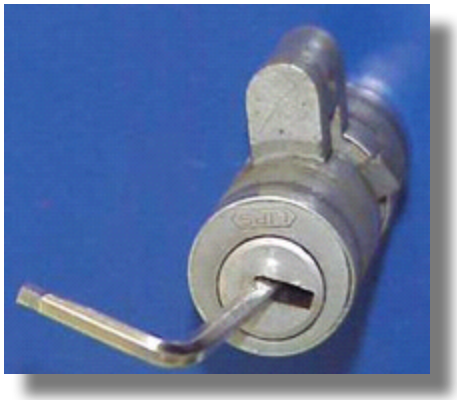
Antwerp Diamond Heist | Case Study

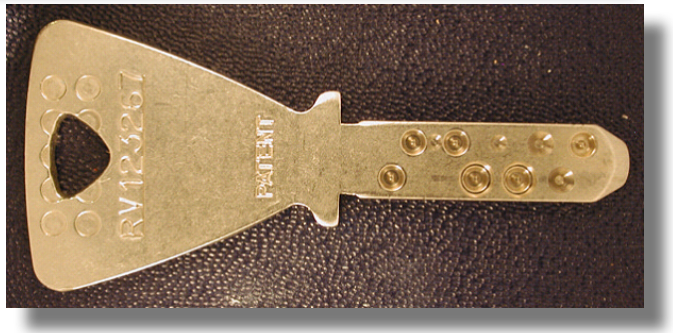
The loot was never found, but based on circumstantial evidence, Notarbartolo was sentenced to 10 years. He has always denied having anything to do with the crime and has refused to discuss his case with journalists, preferring to remain silent for the past six years.

Until now.

Antwerp Diamond Heist | Case Study

- Lips dimple lock was the subject of attack at the Antwerp diamond exchange in Belgium during a $100,000,000 burglary in 2003.
- The locks were employed on safety deposit boxes inside the vault.
- The tool is a modified Allen wrench that is used to rake the tumblers.





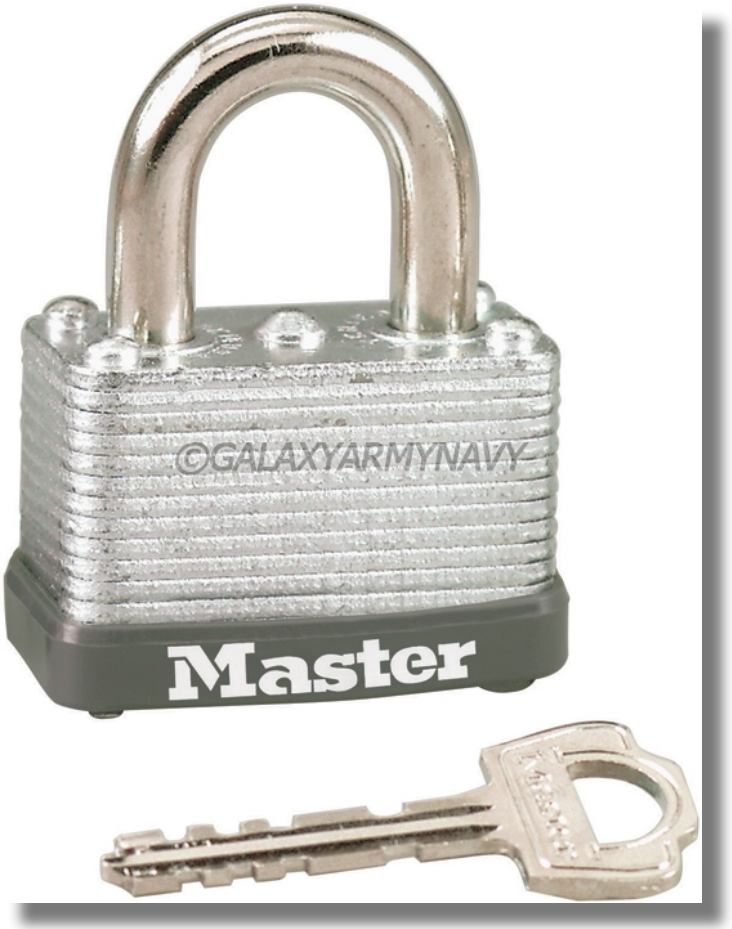
"Whenever the parts of a lock which come in contact with the key are affected by any pressure applied to the bolt, or to that portion of the lock by which the bolt is withdrawn and shot, in such a manner as to indicate the points of resistance to the withdrawal or shooting of the bolt, such a lock can be picked. Where a key can enter, a false key, whether in key form or in the form of bent wire, can also enter."

A.C.HOBBS

DEMO (10 MINUTES)

Master Padlock

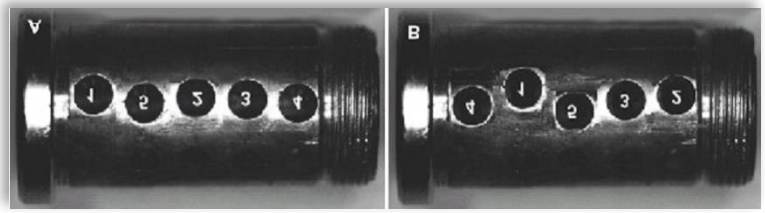
- High respect for the company
- Relatively easy lock to pick
- Semi-paracentric keyway

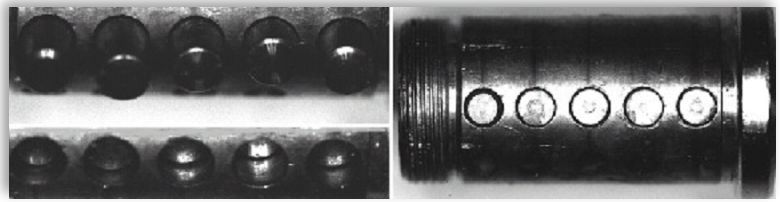


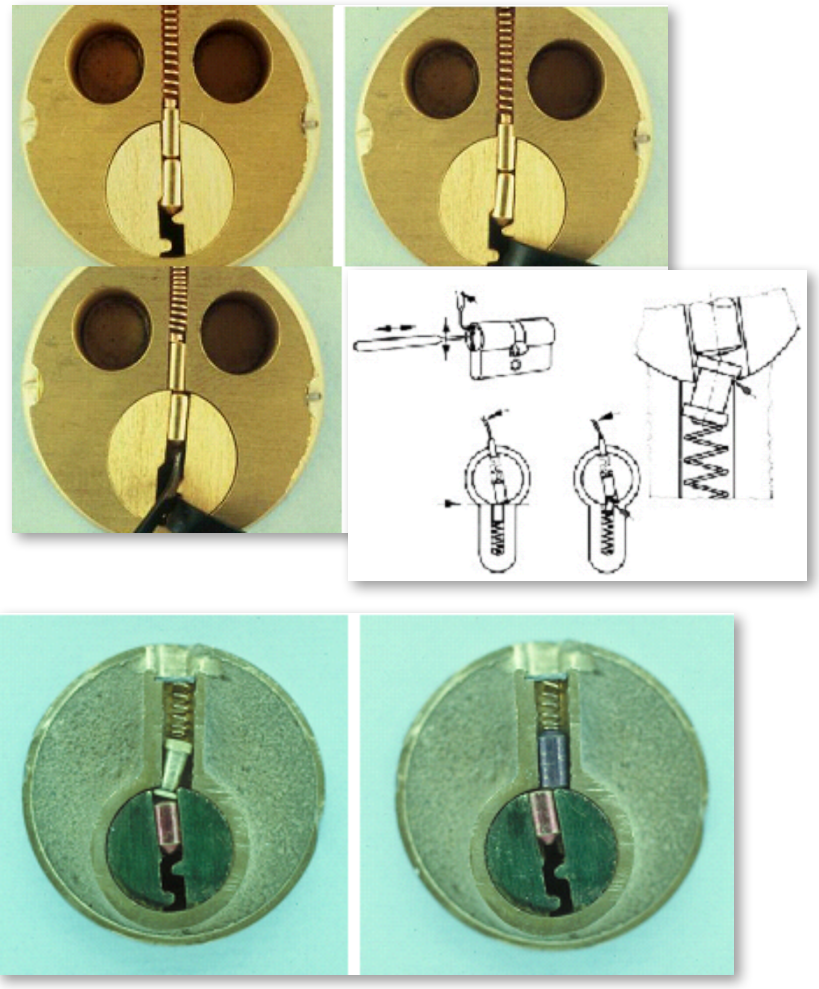
"Whenever the parts of a lock which come in contact with the key are affected by any pressure applied to the bolt, or to that portion of the lock by which the bolt is withdrawn and shot, in such a manner as to indicate the points of resistance to the withdrawal or shooting of the bolt, such a lock can be picked. Where a key can enter, a false key, whether in key form or in the form of bent wire, can also enter."

A.C.HOBBS

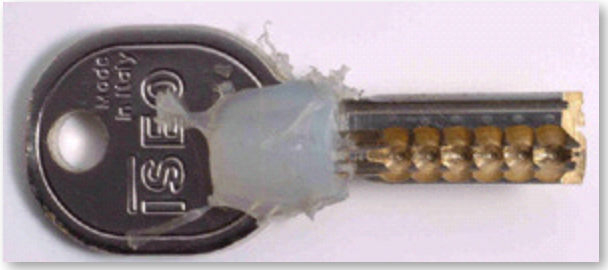
SUMMARY & MORAL OF THE STORY (7 MINUTES PLEASE)


A
B





PROBLEMS



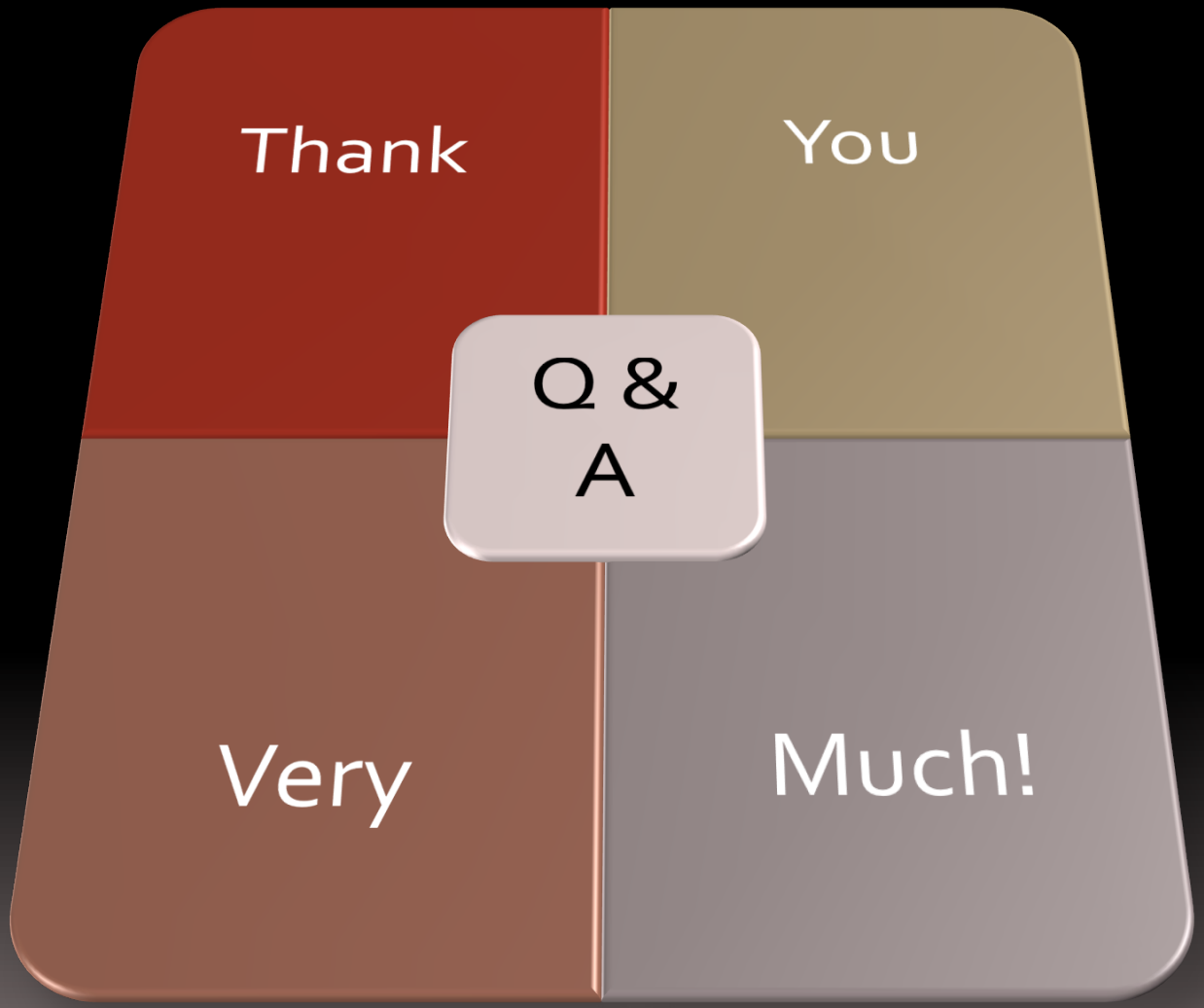
NON-DESTRUCTIVE MEANS

- Bypassing
  - Lockpicking
  - Shimming
  - Impressioning

REFERENCES

WWW.LOCKPICKING101.COM
WWW.BLACKBAG.NL
WWW.TOOOL.COM
WWW.WIRED.COM
WWW.CRYPTO.COM

LOCKS, SAFES & SECURITY BY MARC TOBIAS
MIT LOCKPICKING GUIDE


Thank
You
Q &
A
Very
Much!