

**Very IMPORTANT DISCLAIMER:** 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. Again, the aim of this presentation is to initiate intellectual intercourse and awareness on the subject matter at hand.


# LOCKPICKING : FOR EDUCATIONAL AND AWARENESS PURPOSES ONLY

A presentation for rOOTcON 5 (September 9-11, 2011)

By: JollyMongrel (arf arf )

# OUTLINE OF THIS PRESENTATION

- Background
  - Brief (not the underpants) History of Locks
- Lock Anatomy
- Lock Operation
- Lock Exploitation
  - Destructive
  - Non-destructive
- Basic lock challenge
- Case study (Antwerp Diamond Heist)
- Possible Scenarios
- Demo
- Summary and moral of the presentation
- References



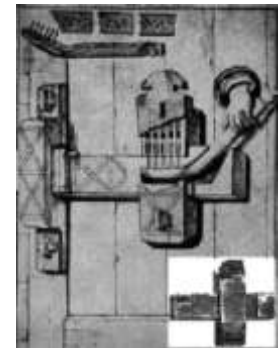
*"And the key of the House of David  
will I lay upon His Shoulder."  
-Isaiah, CH. XXII, V. 22*

**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*



*"The main purpose of your body, DAMMIT!!!, is to carry your heads around!!  
YOU DICKHEADS!!!"*

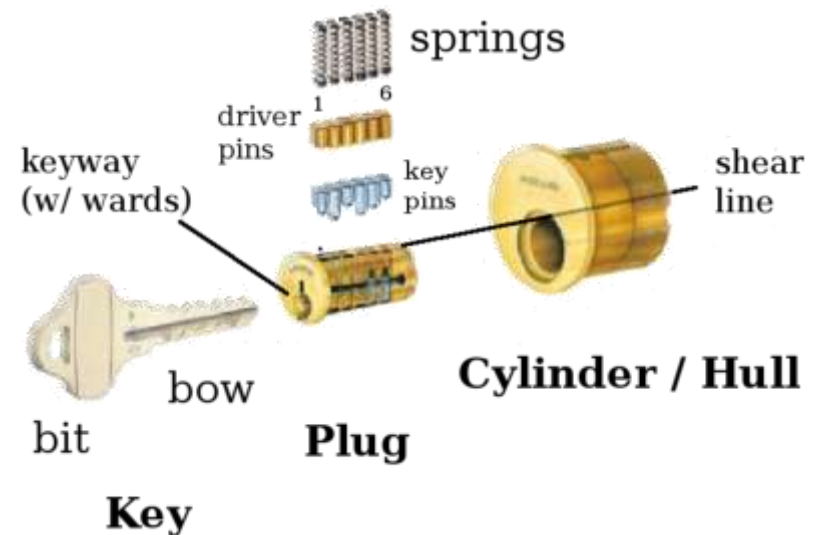
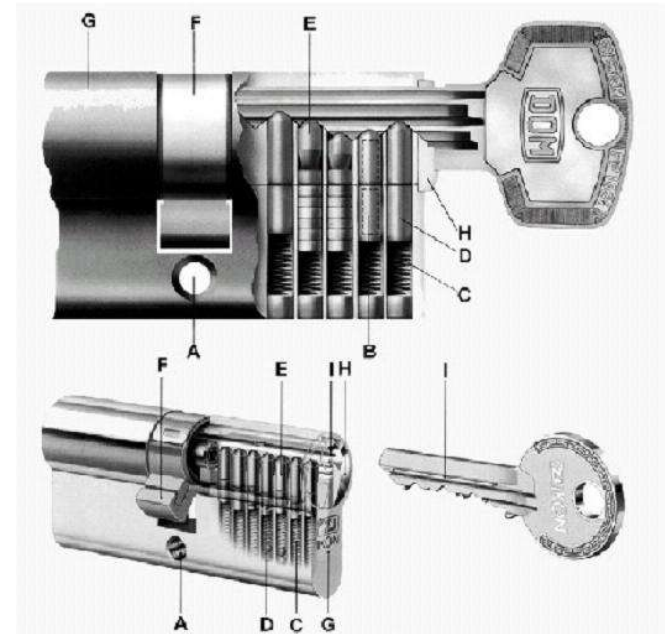
- anonymous ROTC commandant

**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



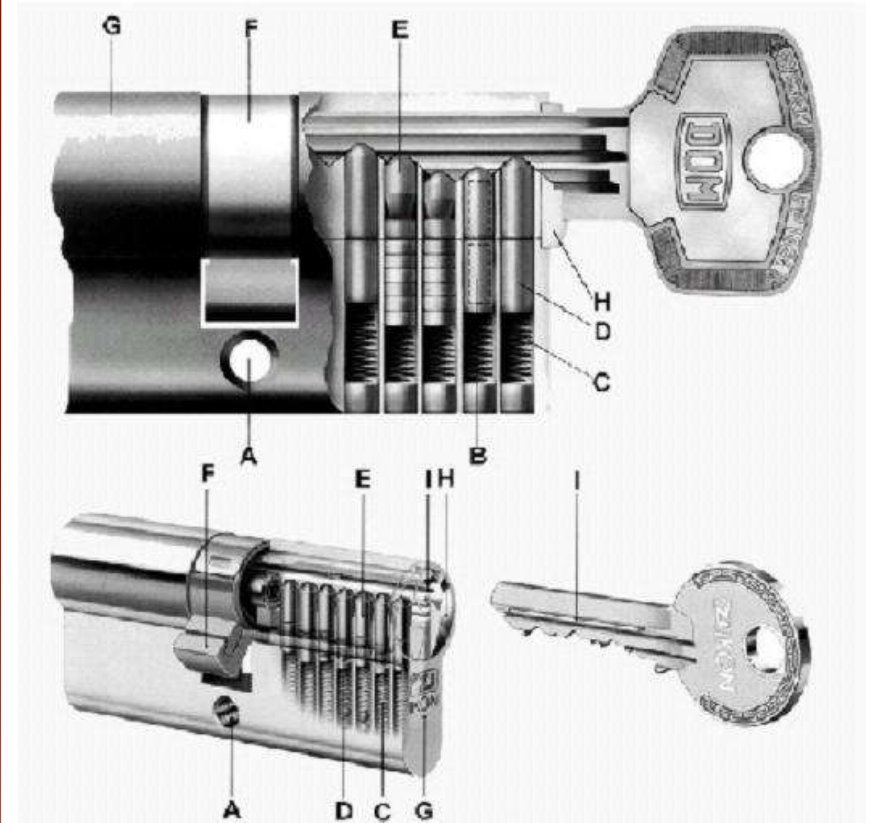
*"Fresh body organs for sale: liver, 200,000; kidney promo, buy 1, take 1, 75,000; eyes, brownish/black color, 25,000 ...."*

- anonymous forum poster

**LOCK OPERATION (7 MINUTES  
PLEASE)**

# Mechanism | Lock Operation

Regardless of the mechanisms, design and brand, the theory of all mechanical locks are very similar. The default state is maintained in a locked position until some mechanical action/s is/are actuated to remove obstruction and allow freedom of moveable parts. The obstructions are formed by the pins, levers, wafers, or discs. Removing this blockage involves the insertion of a key that rearranges and moves each of the obstructions to a common point, called a "shear line".

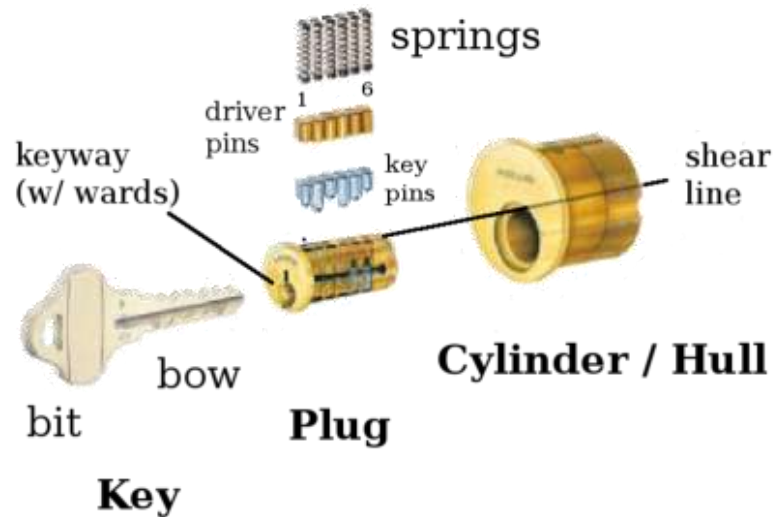




# Vulnerability | Lock Operation

Locks can be exploited because of “Tolerance Errors” or a certain level of gap between moving parts (pins-plug-shell). Poor tolerance allows easier exploitation.

*More moveable parts increase the avenue of exploitation and you can always go for the weakest link.*





*"... Huwag, KUYA, huwaaaag! ."*

- from a sensual RADIO DRAMA

**LOCK EXPLOITATION (20-30  
MINUTES PLEASE)**

# || Destructive | Lock Exploitation

## Mechanical Brute Force Attack

- The most direct way to bypass physical access control mechanisms
- Uses drilling, impact, explosive, physical strength, etc.
- Commonly used by burglars
- Used for one-time entry
- Barbaric
- Popular method in the Philippines



# 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

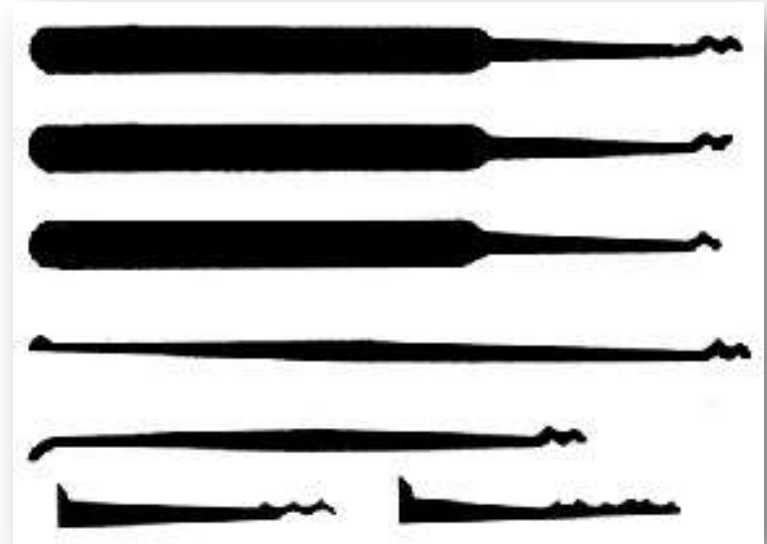
Lock bumping is a lock picking technique for opening a pin tumbler lock using a specially-crafted bump key. One bump key will work for all locks of the same type.



# Covert | Lock Exploitation

## Raking

Involves vigorously scrubbing the pins to set in alignment to the shearline



# Covert | Lock Exploitation

## Impact Guns (Pick/snap guns)

*A "kiddie" version of picking but effective and fast (anyway, there is a saying that THE END JUSTIFIES THE MEANS)*

There is a class of lock-picking tools that rely upon the generation of a mechanical shock or impact applied to the base of all tumblers simultaneously in order to bounce drivers into the shell for a brief window of time. These tools can be loosely categorized as impact guns or tools and are primarily designed for pin tumbler locks.



# Covert | Lock Exploitation

## Single Pin Picking (SPP)

Picking simulates the action of a key. The actual sequence of physical steps involved in picking and opening any lock, and more particularly a pin tumbler lock, require three distinct operations: **1.** the application of torque; **2.** the manipulation of each tumbler; **3.** and the actuation of the locking mechanism. If the lock fails to open, then the operative must assess obstacles that prevented a successful bypass, select different tools or techniques, and make another attempt.






# Covert | Lock Exploitation

**Impressioning** (*an advanced technique to be discussed and demoed in the next con*)

Involves duplication of keys using various methods.

Impressioning is perhaps the most valuable skill of the covert entry specialist and the locksmith. Once the technique is acquired, it will provide a working key. While many locks cannot be picked for a variety of reasons, impressioning is a method to bypass almost every locking mechanism, even if certain security enhancements are present.





*"You are just secure as your weakest link"*  
- a line from a novel



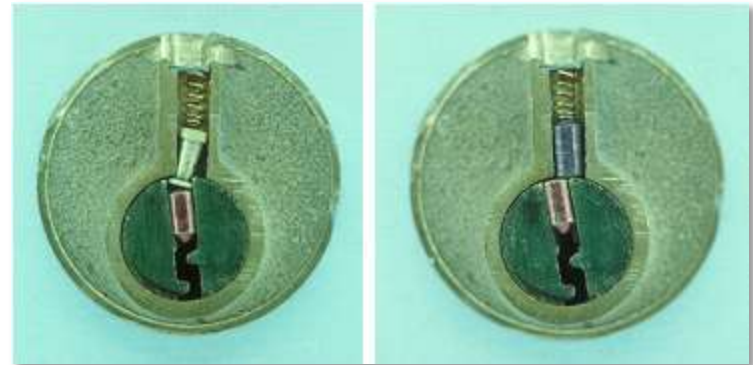
# BASIC LOCK CHALLENGES (3 MINUTES)

# Keyways | Basic Challenge

## SECURITY TUMBLERS

- Spool
- Serrated
- Mushroom

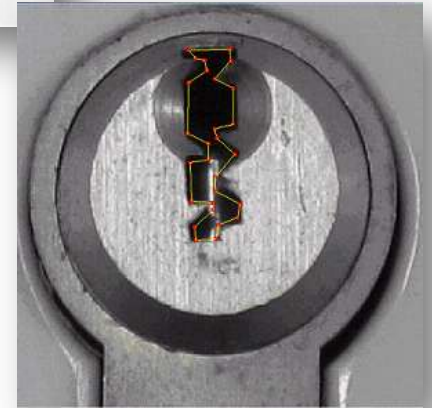
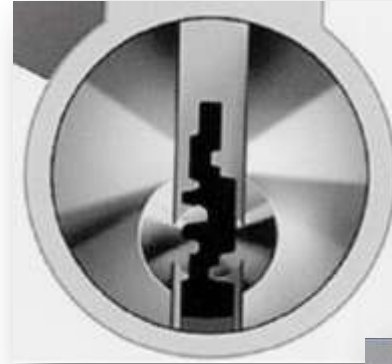
This components provide false-setting that can confuse and frustrate lockpickers.



# Keyways | Basic Challenge

## Paracentric Keyway

Provides difficulty in maneuvering picks because of the jagged design of the keyhole



*"Mala prohibita... mala ense... ignorance of the law excuses no one!!!"*  
- overheard from a crowd of debaters

## CASE STUDY (10 MINUTES)

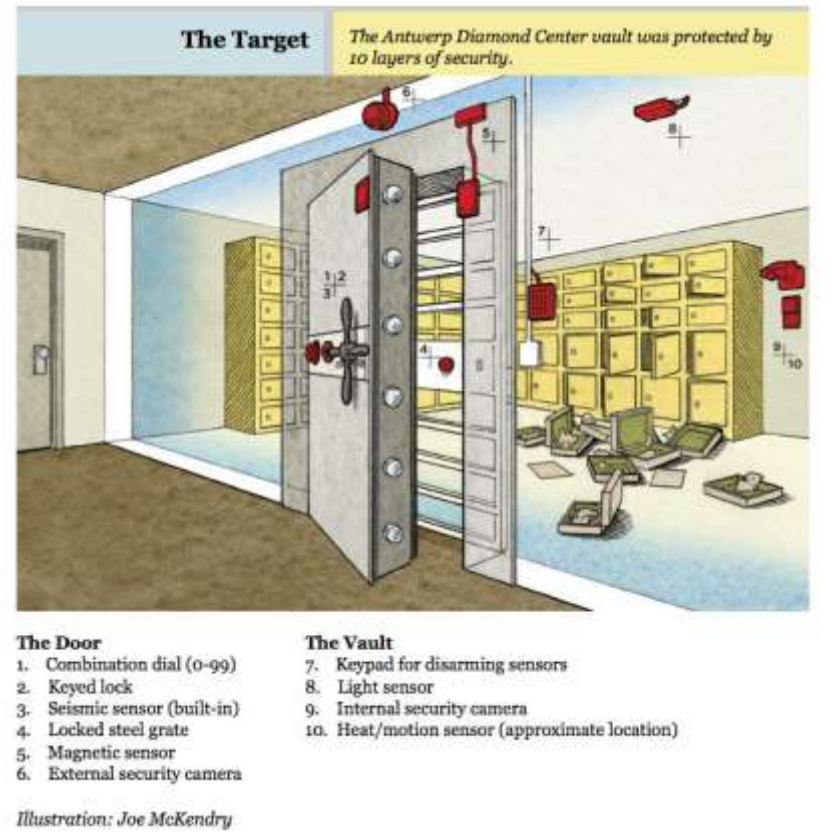
# Antwerp Diamond Heist | Case Study

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 Falletti)*). 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.



*"believe me, to see is to believe"*


- overheard from a circus magician

**POSSIBLE SCENARIOS (10 + OR - 10  
MINUTES)**

# || Dangers & | Possible Scenarios

- Spoof and social-engineer the post-office box (PO Box) subscribers. Physical version of spamming by making specially crafted mails and putting them on these boxes gaining a certain level of trust for a successful social engineering.
- Install bugs and Hayden Videos.
- Install beige-boxes in telephone junction boxes or any tapping device/s for snooping.
- Get hold of hardwares (i.e.: routers, laptops, hard disks) and sift credentials and other critical information assets.
- Install hardware keyloggers or any payload-rigged hardware (USB haksaw and the likes), etc...





*"believe me, to see is to believe"*

- overheard from a circus magician

**DEMO (10 + OR - 10 MINUTES)**

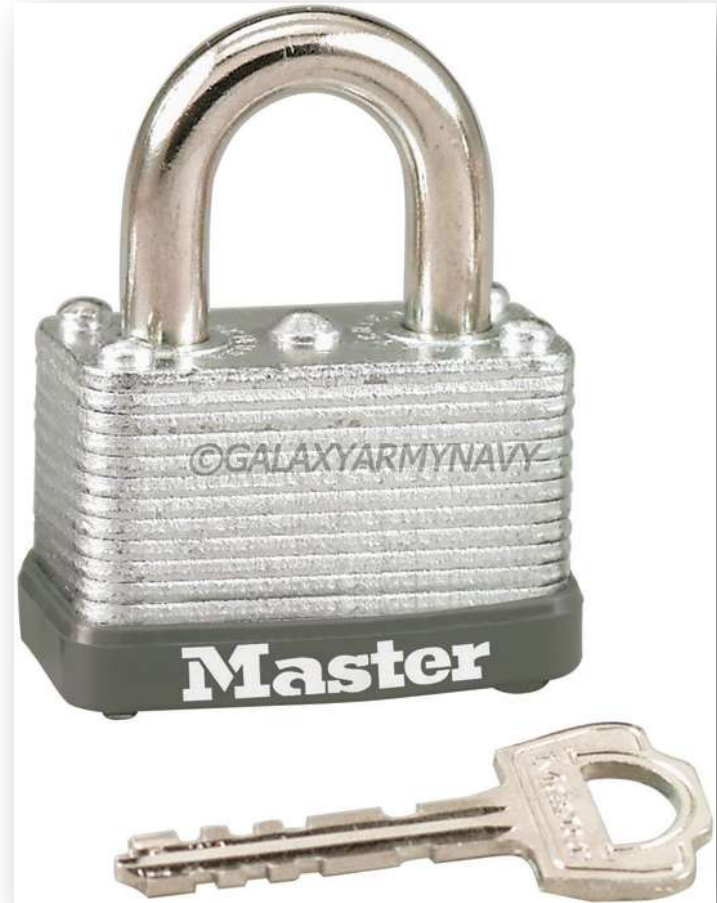
# Locks and Technique | Demo

Padlock

Handcuff (as provided by Dax)

## Techniques

- Raking
- Single Pin Picking





*"arf! Arf! Arf!"*

- Jollymongrel



# SUMMARY & MORAL OF THE PRESENTATION (7 MINUTES PLEASE)

# Observations | & Moral of the story

- In the Philippines, pursuant to the articles (Chapter 10, art. 304) under the revised penal code, it is considered illegal to possess and practice Lockpicking without lawful cause.
- Presently, the presenter cannot identify local certifying body for local Locksmiths to be recognized as such.



# || Mitigating Measures | & Moral of the story

- Enhance physical security mechanisms (i.e.: physical tripwires, efficiently installed motion detectors, cctv, etc.)
- Invest in dependable and feisty dogs as security

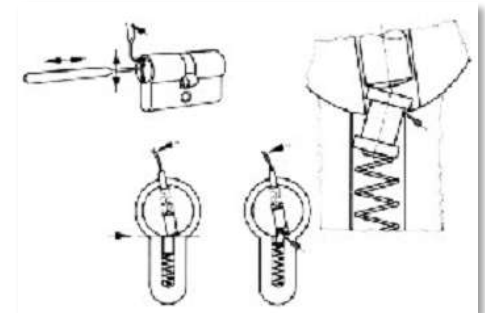
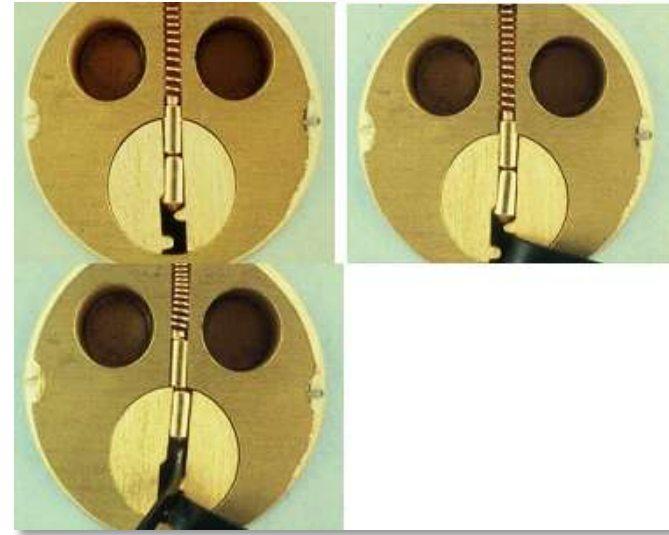
- Install dependable locks
- Regularly audit your physical security





# Summary | & Moral of the story

- Background
  - Brief (not the underpants) History of Locks
- Lock Anatomy
- Lock Operation
- Lock Exploitation
  - Destructive
  - Non-destructive
- Basic lock challenge
- Case study (Antwerp Diamond Heist)
- Demo
- Summary, mitigating measures, and plans for proceeding cons



# REFERENCES

[WWW.LOCKPICKING101.COM](http://WWW.LOCKPICKING101.COM)

[WWW.BLACKBAG.NL](http://WWW.BLACKBAG.NL)

[WWW.TOOOL.COM](http://WWW.TOOOL.COM)

[WWW.WIRED.COM](http://WWW.WIRED.COM)

[WWW.CRYPTO.COM](http://WWW.CRYPTO.COM)

LOCKS, SAFES & SECURITY BY MARCTOBIAS

MIT LOCKPICKING GUIDE



**That's all  
folks...**

**THANK YOU  
FOR YOUR  
TIME**

**And God bless us all!**