



# HISTORY OF LOCKS, DESIGNS, AND BYPASS

Locks, Safes, and Security  
LSS+ Multimedia Supplement

[www.securitylaboratories.org](http://www.securitylaboratories.org)



# BYPASS AND PRODUCT DESIGN: CONSEQUENCES

- ◆ LISHI PICK FOR VAG CARS
- ◆ SPUTNIK
- ◆ LEVER LOCK IMPRESSIONING TOOL
- ◆ BUZZ PICK TOOL
- ◆ BELLOCK GUN LOCK
- ◆ KENS TV GUN LOCK REPORT



# C. Tomlinson, 1853

- ◆ A commercial, and in some respects a social doubt has been started within the last year or two, whether or not it is right to discuss so openly the security or insecurity of locks. Many well-meaning persons suppose that the discussion respecting the means for baffling the supposed safety of locks offers a premium for dishonesty, by showing others how to be dishonest. This is a fallacy. Rogues are very keen in their profession, and know already much more than we can teach them respecting their several kinds of roguery.



## C. Tomlinson....

- ◆ Rogues knew a good deal about lock-picking long before locksmiths discussed it among themselves, as they have lately done. If a lock, let it have been made in whatever country, or by whatever maker, is not so inviolable as it has hitherto been deemed to be, surely it is to the interest of honest persons to know this fact, because the dishonest are tolerably certain to apply the knowledge practically; and the spread of the knowledge is necessary to give fair play to those who might suffer by ignorance.





## C. Tomlinson....

- ◆ It cannot be too earnestly urged that an acquaintance with real facts will, in the end, be better for all parties. Some time ago, when the reading public was alarmed at being told how London milk is adulterated, timid persons deprecated the exposure, on the plea that it would give instructions in the art of adulterating milk; a vain fear, milkmen knew all about it before, whether they practiced it or not; and the exposure only taught purchasers the necessity of a little scrutiny and caution, leaving them to obey this necessity or not, as they pleased.



# BYPASS: WHY IMPORTANT

- ◆ Protection of life
- ◆ Protection of property
- ◆ Protection of information
- ◆ Sabotage
- ◆ Espionage
- ◆ National security
- ◆ Terrorism



# BYPASS: REQUIRED KNOWLEDGE

- ◆ Locks
- ◆ Safes
- ◆ Security: physical and electronic
- ◆ Bypass technologies
- ◆ Bypass tools and techniques
- ◆ Specific bypass issues
- ◆ Specific vulnerabilities
- ◆ Master keying systems



# REQUIRED SUBJECTS

- ◆ · Anti-picking features
- ◆ · Bypass capability and methods of entry
- ◆ · Bypass techniques
- ◆ · Code cutting of keys
- ◆ · Cross-keying
- ◆ · Databases and reference materials for locks
- ◆ · Decoding of locks·



# REQUIRED SUBJECTS

- ◆ · Differs and depth coding: theory and reality
- ◆ · Disassembly of locks
- ◆ · Evidence of bypass
- ◆ · Forensic analysis of locks
- ◆ · Forensic disassembly of locks
- ◆ · Identification of locks, keys, and components
- ◆ · Impressioning



# REQUIRED SUBJECTS

- ◆ · Key duplication procedures
- ◆ · Keying of locks
- ◆ · Keying systems, including master keying
- ◆ · Keyways and restrictions
- ◆ · Locking hardware
- ◆ · Locks, and theory of operation of each type of mechanism
- ◆ · Manufacturing specifications for locks and keys
- ◆ · Metals and Metallurgy



# REQUIRED SUBJECTS

- ◆ · Methods of forced-entry
- ◆ · Picking
- ◆ · Safes: construction, locks, and methods of entry
- ◆ · Security systems and access control
- ◆ · Specifications for key machines
- ◆ · Tolerance specifications
- ◆ · Tools utilized in bypass





# WHO IS AFFECTED?

- ◆ Anyone who has property to protect
- ◆ Valuable items
- ◆ Valuable information
- ◆ Any premises
- ◆ EVERYONE IS AFFECTED BY LACK OF SECURITY



# BYPASS: THE PROBLEM

- ◆ Lack of knowledge by law enforcement investigators
- ◆ Lack of training of forensic specialists
- ◆ Lack of knowledge by tradecraft
- ◆ Lack of expertise by manufacturer
- ◆ Lack of data by public about bypass
- ◆ Potential for bypass: often unknown



# PHYSICAL SECURITY

Mechanical locks are used to protect the physical world from attackers

- Ubiquitous: residential, commercial, industrial, schools, government, etc.
- ◆ To control access to locking mechanism:
  - Combination locks aim to require demonstration of a secret procedure
  - Keyed locks aim to require possession of a secret physical token, a “key”



# LOCKS: THEIR HISTORY AND DESIGNS



# PRIMER ON LOCKS

- ◆ Basic locking mechanisms
- ◆ Must understand theory of operation
- ◆ Bypass theories
- ◆ Security assessment and limitations



# BASIC TYPES OF LOCKS

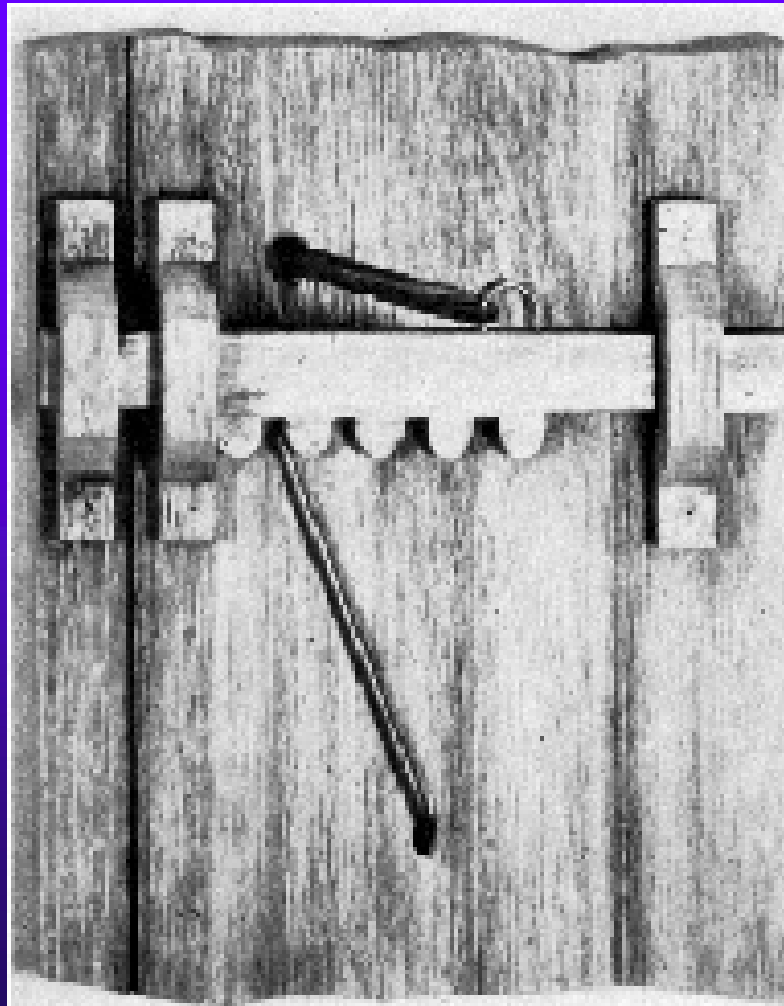
- ◆ Warded
- ◆ Lever
- ◆ Wafer
- ◆ Pin Tumbler
- ◆ Hybrid
  - Magnetic
  - Sidebar: many configurations
  - Rotating Disk
  - Laser track
  - Dimple
  - Axial pin tumbler
- ◆ Combination



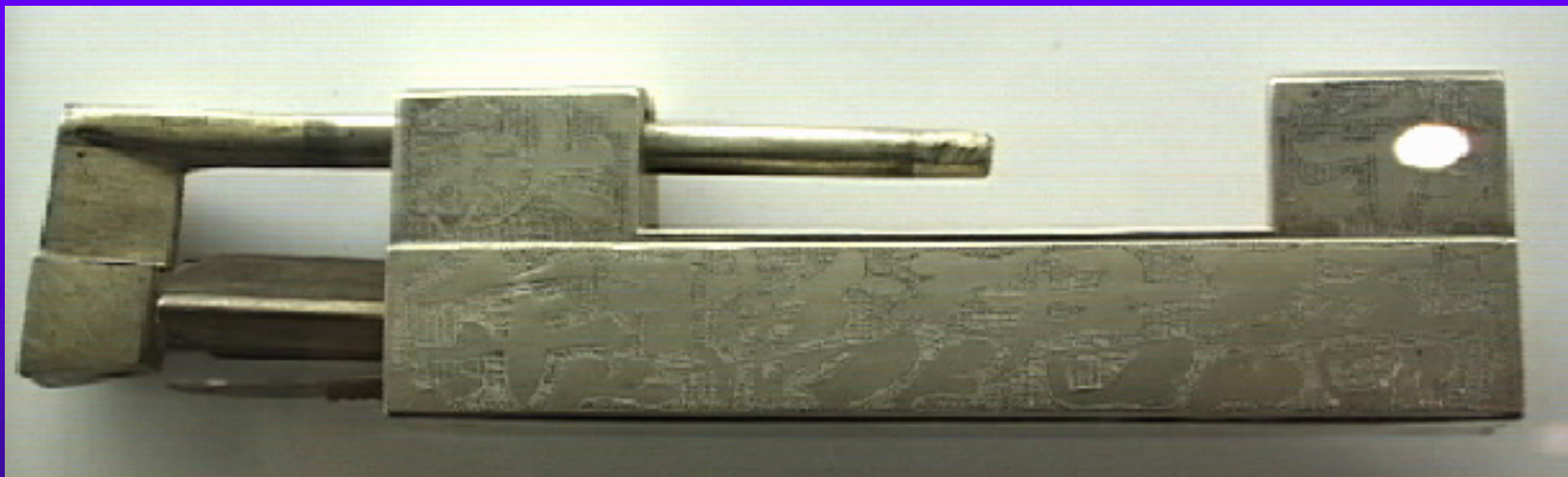
# BEGINNING OF PHYSICAL SECURITY



# GREEK LOCK



# ROMAN PADLOCK





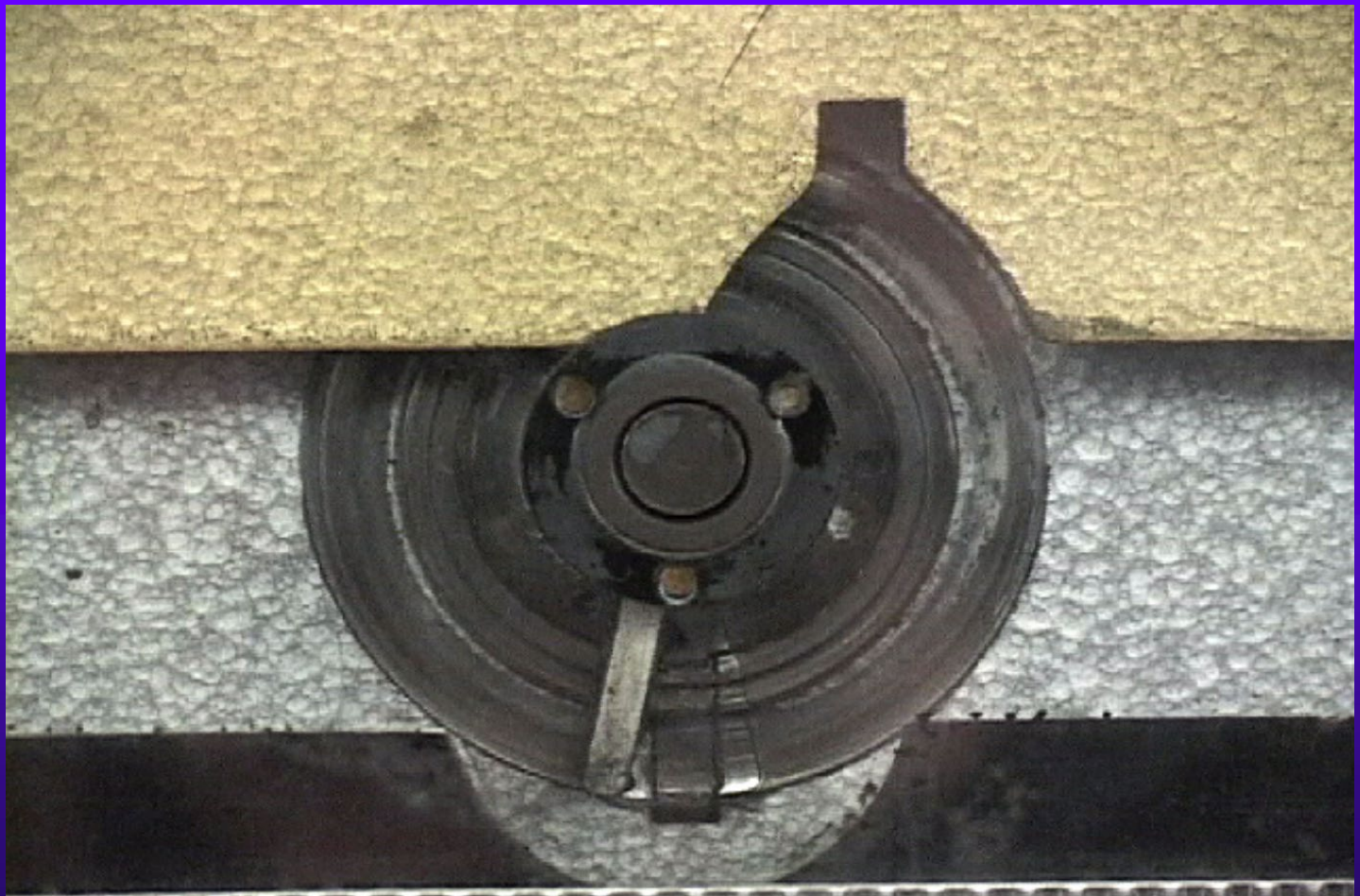
# WARDED LOCK

# WARDDED LOCK

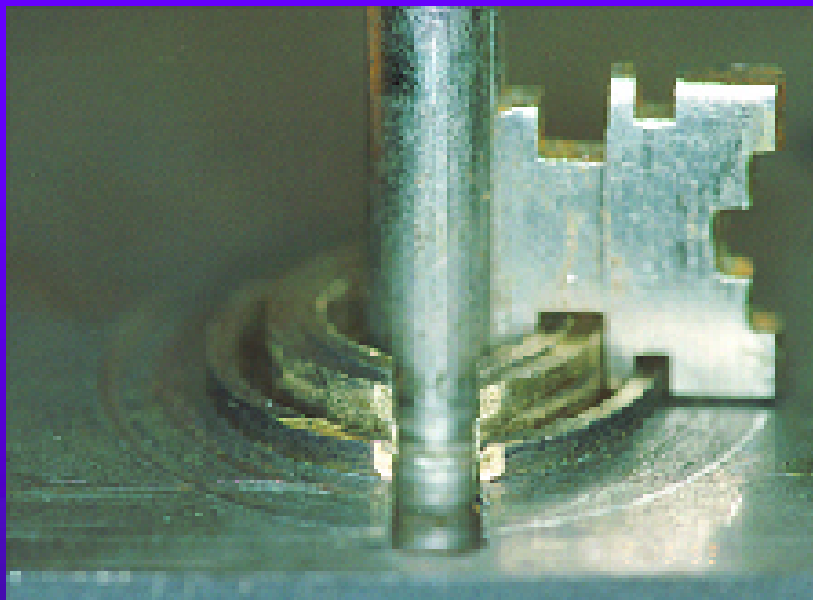




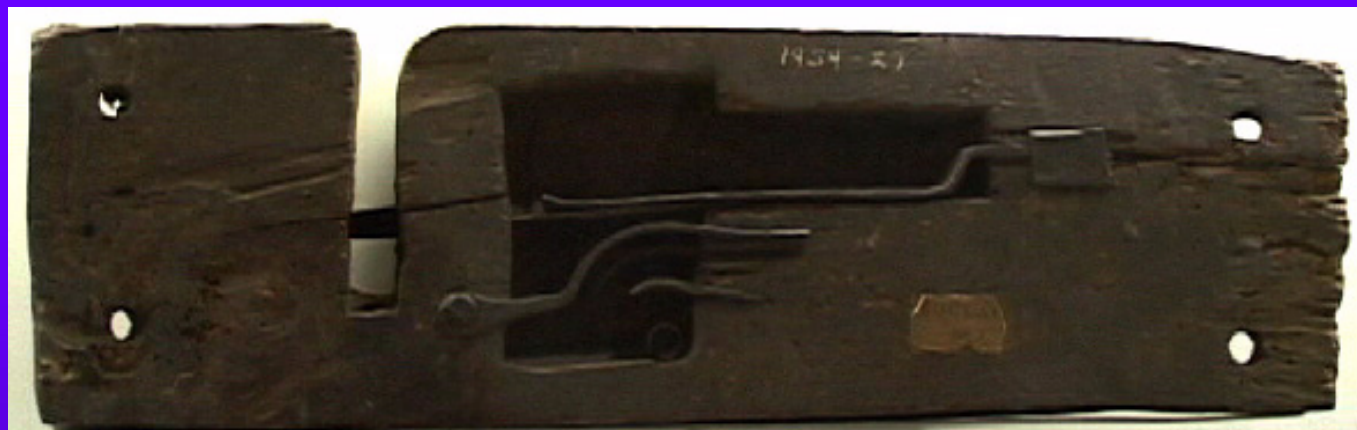
# Warded lock detail



# WARDDED LOCK AND KEY



# EARLY WARDED LOCK





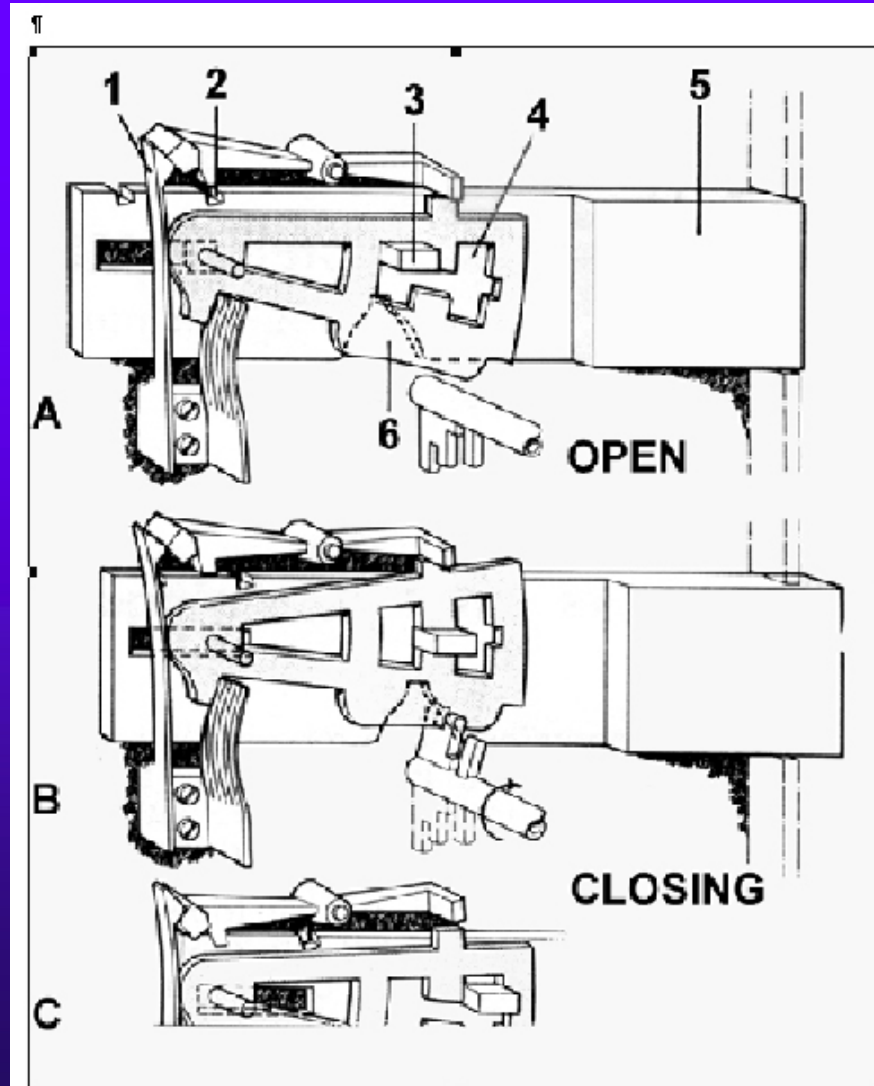
# Warded lock for chest



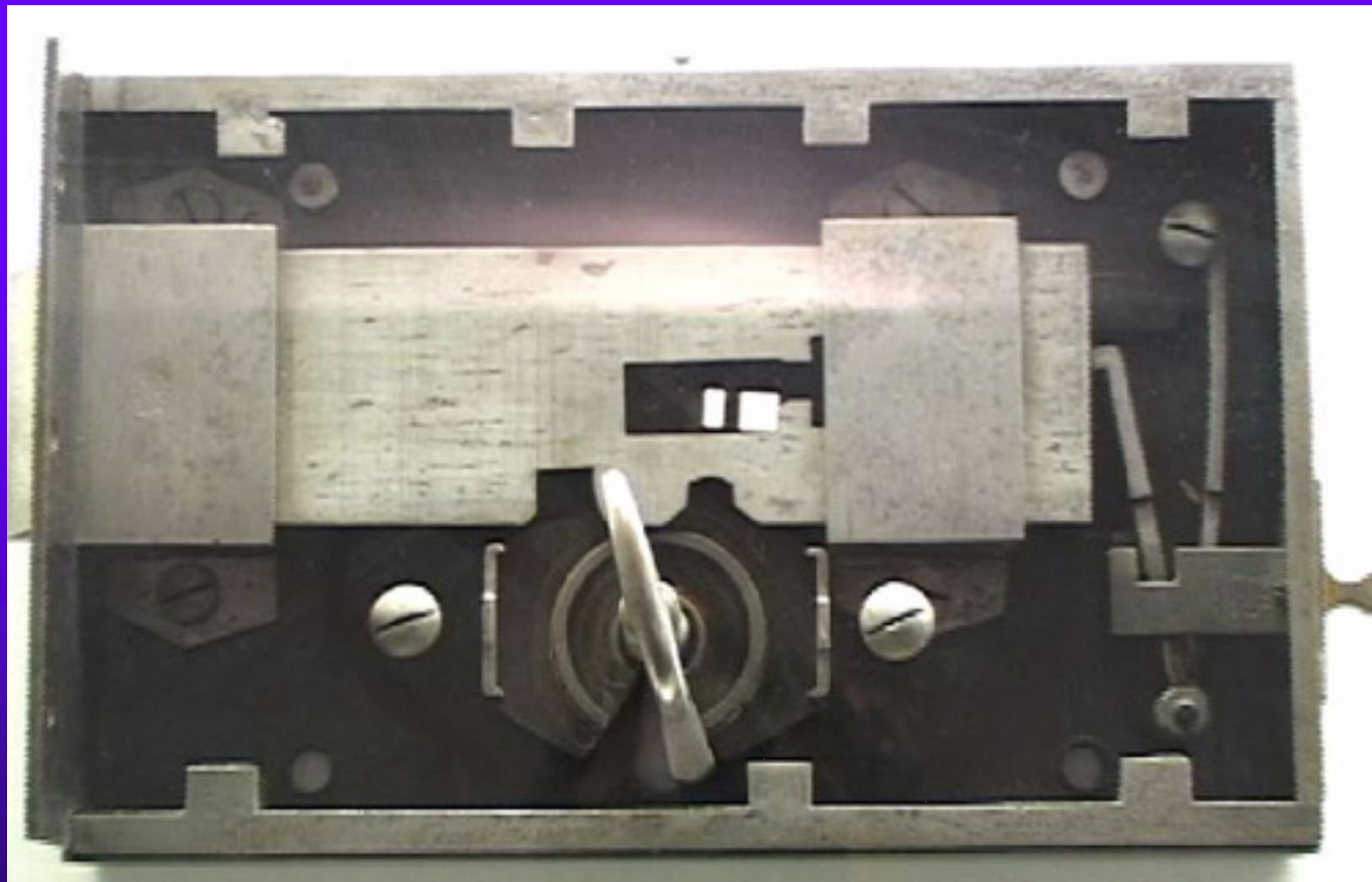


# LEVER LOCK

# LEVER LOCK OPERATION

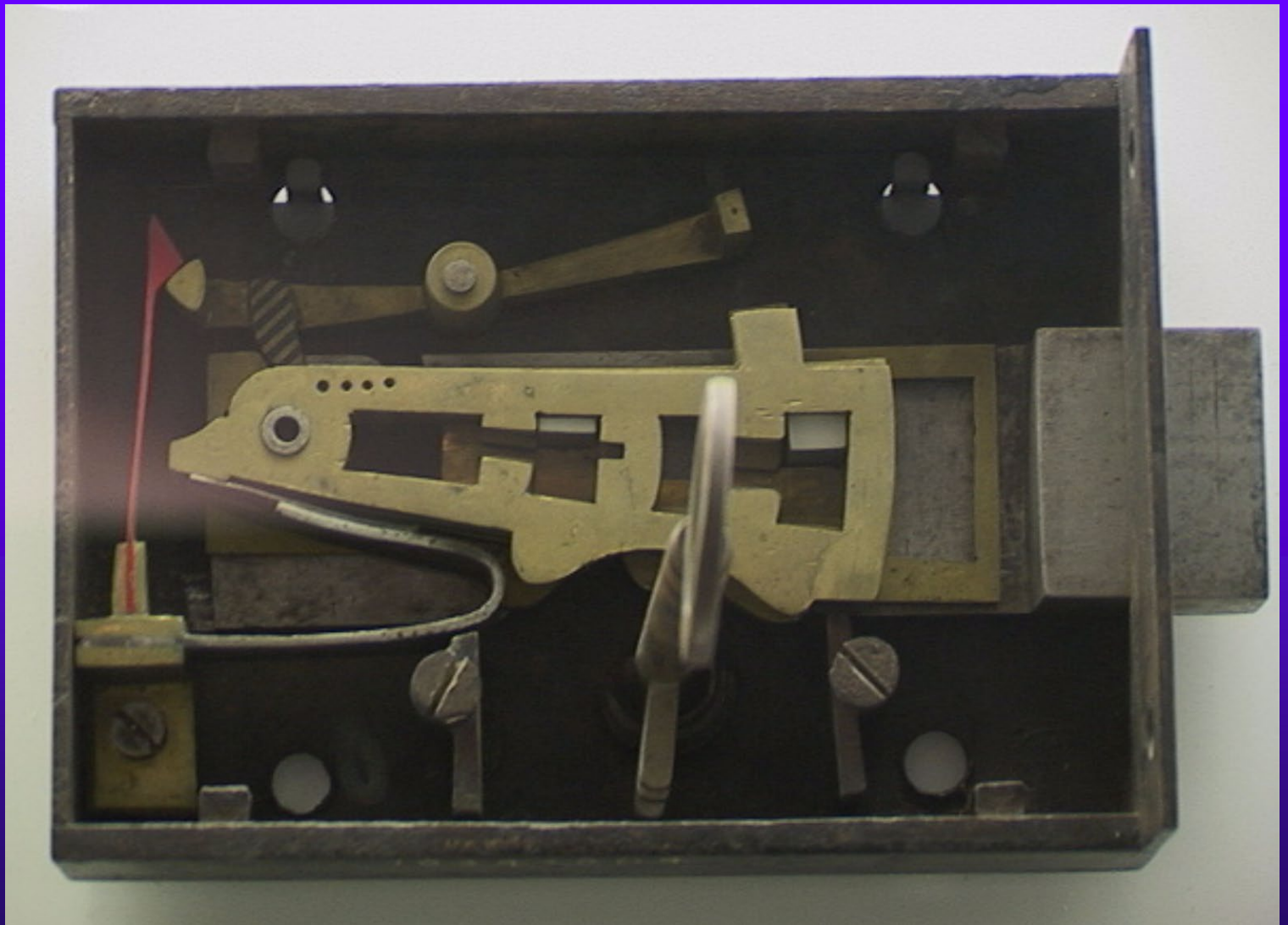


# LEVER LOCK

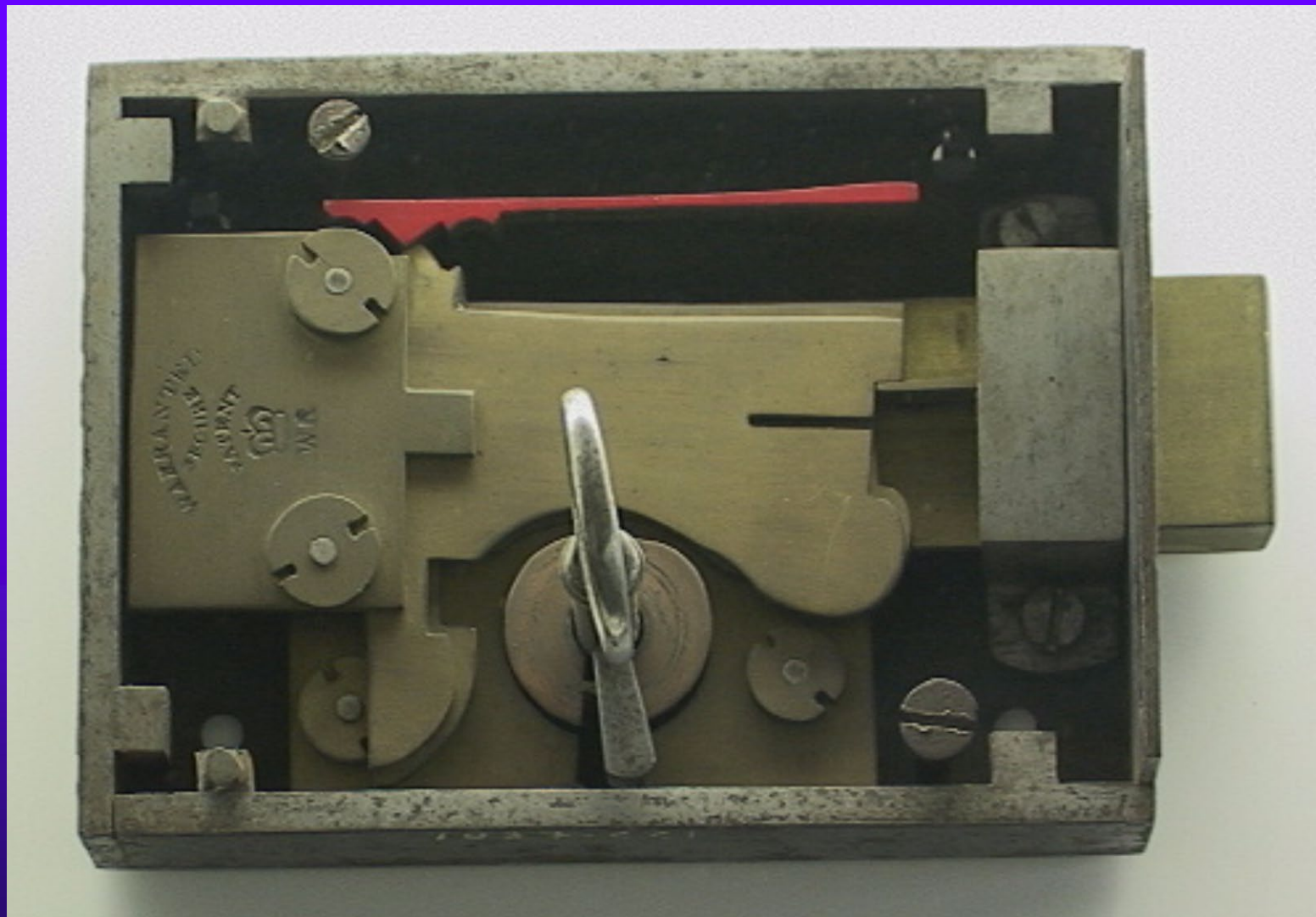




# CHUBB Detector, 1827

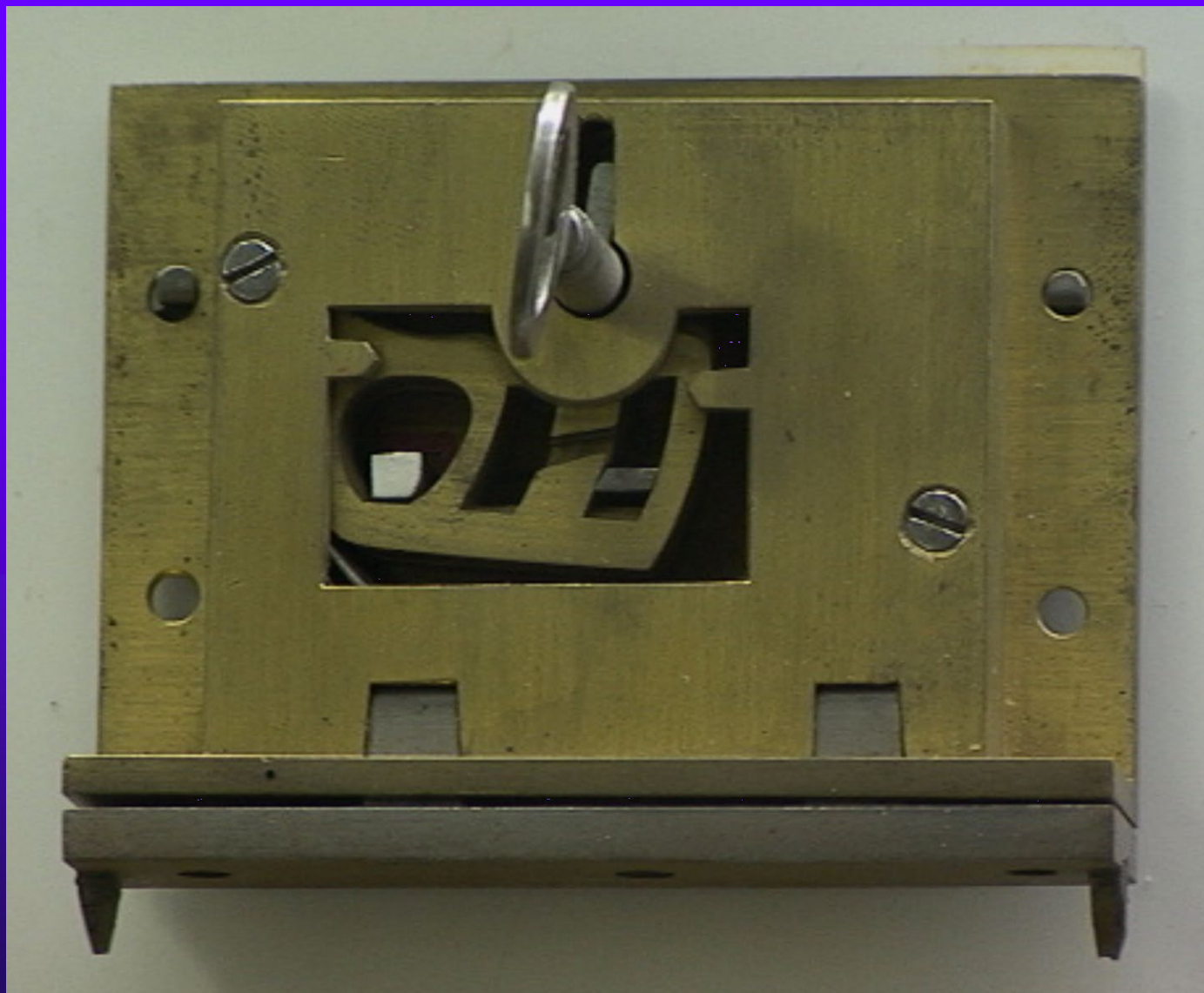


# CHUBB Detector Lock



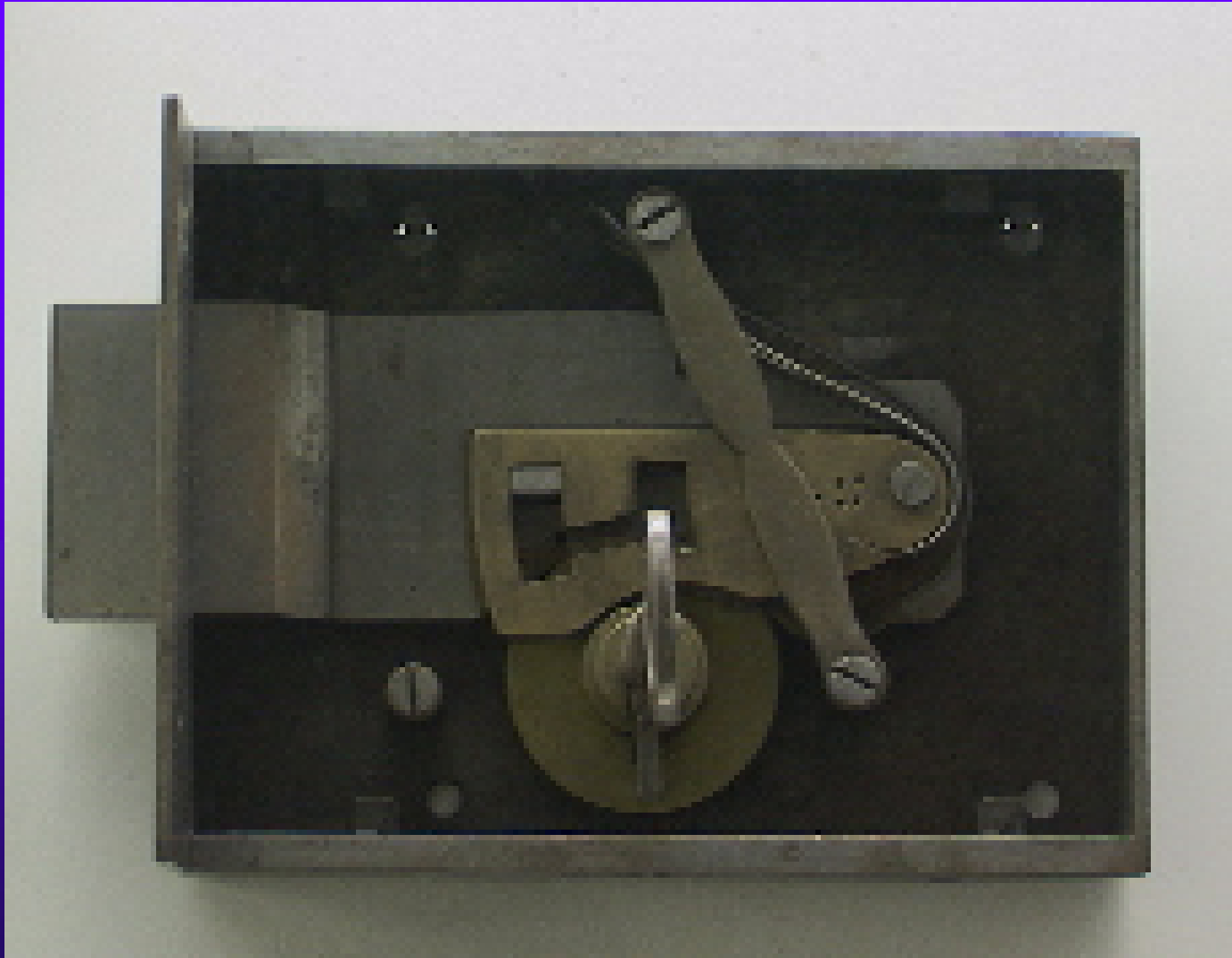


# PRICE Ne Plus Lever Lock





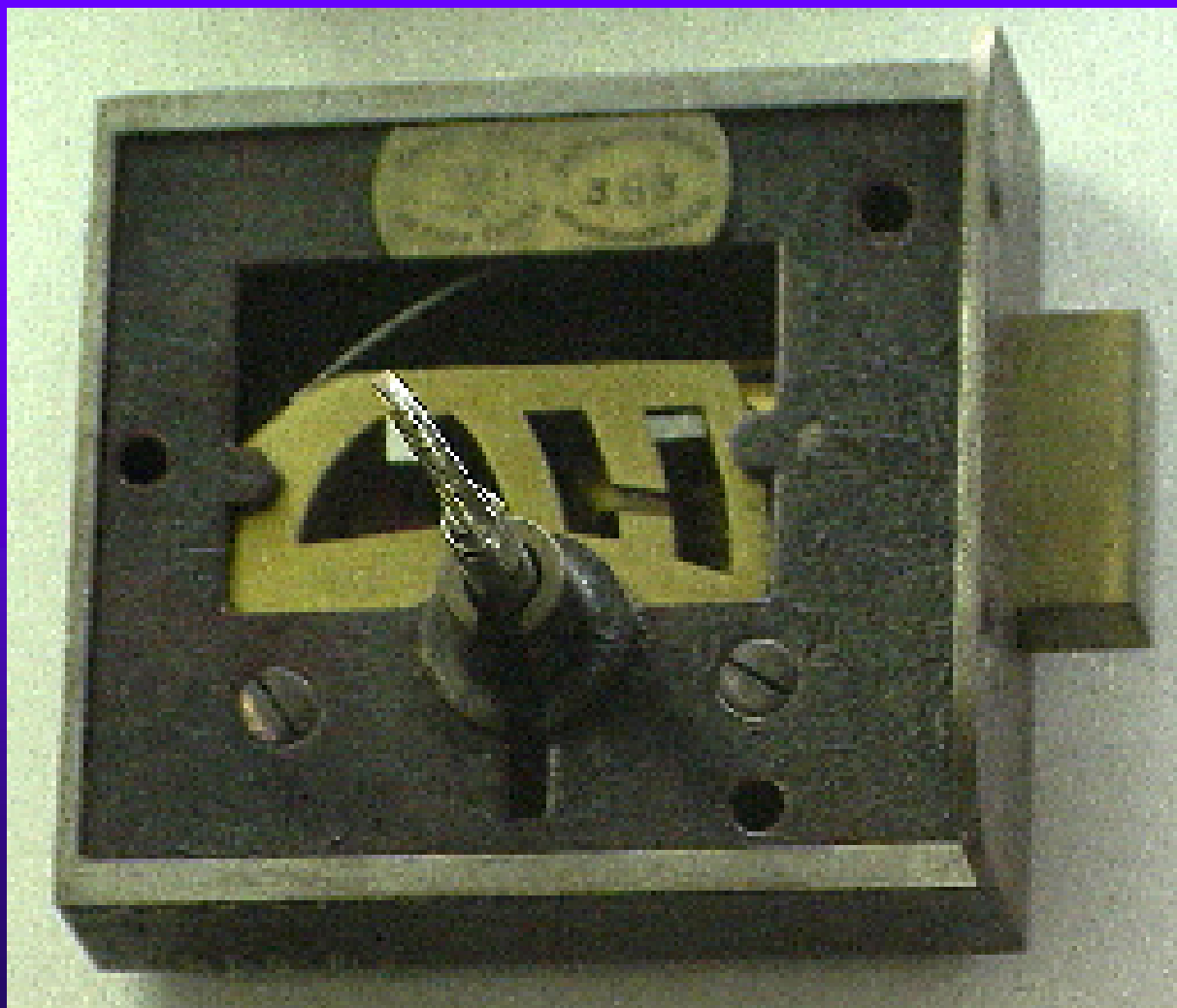
# HOBBS LEVER LOCKS



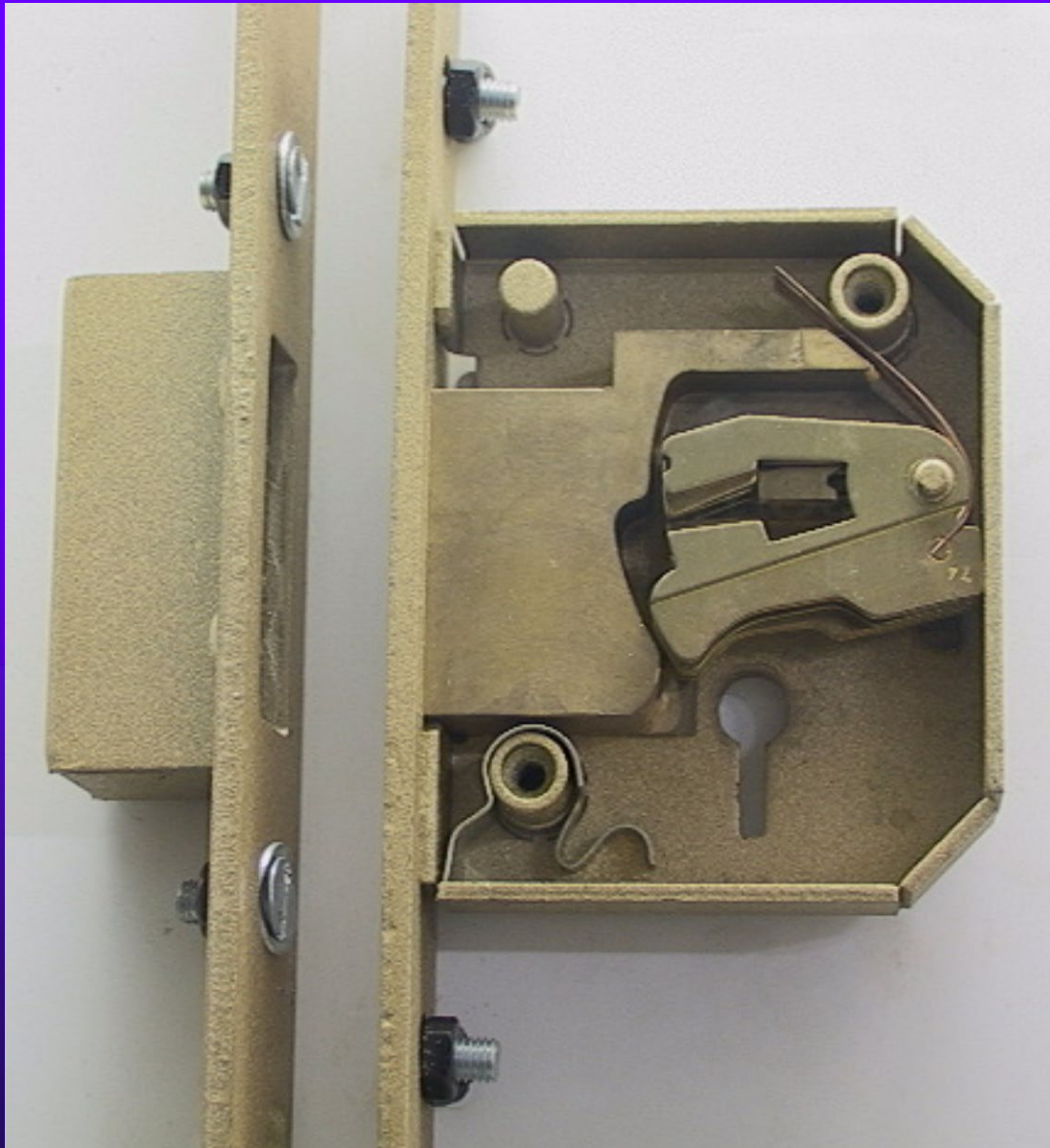
# HOBBS LEVER LOCK



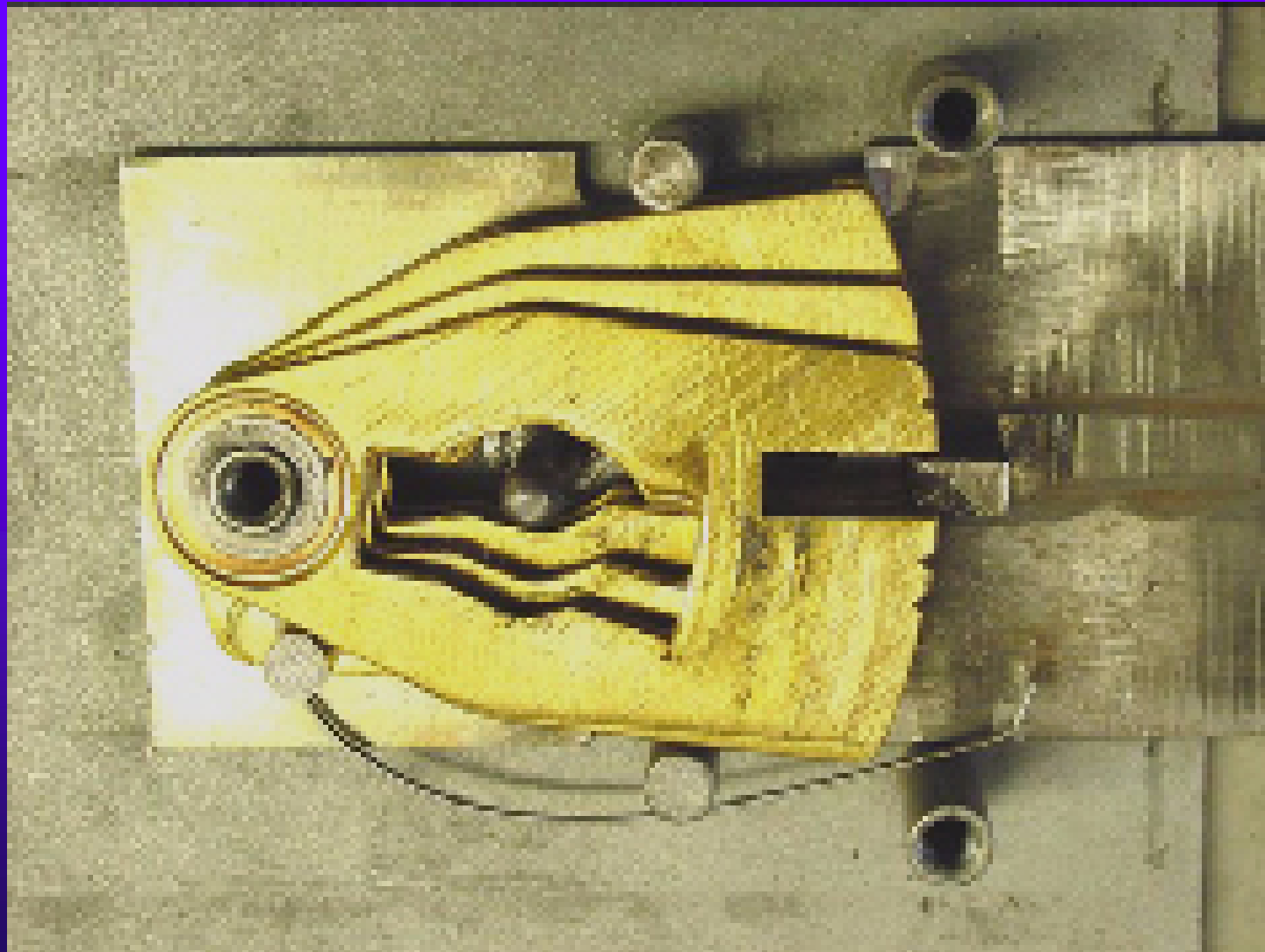
# NePLUS LEVER



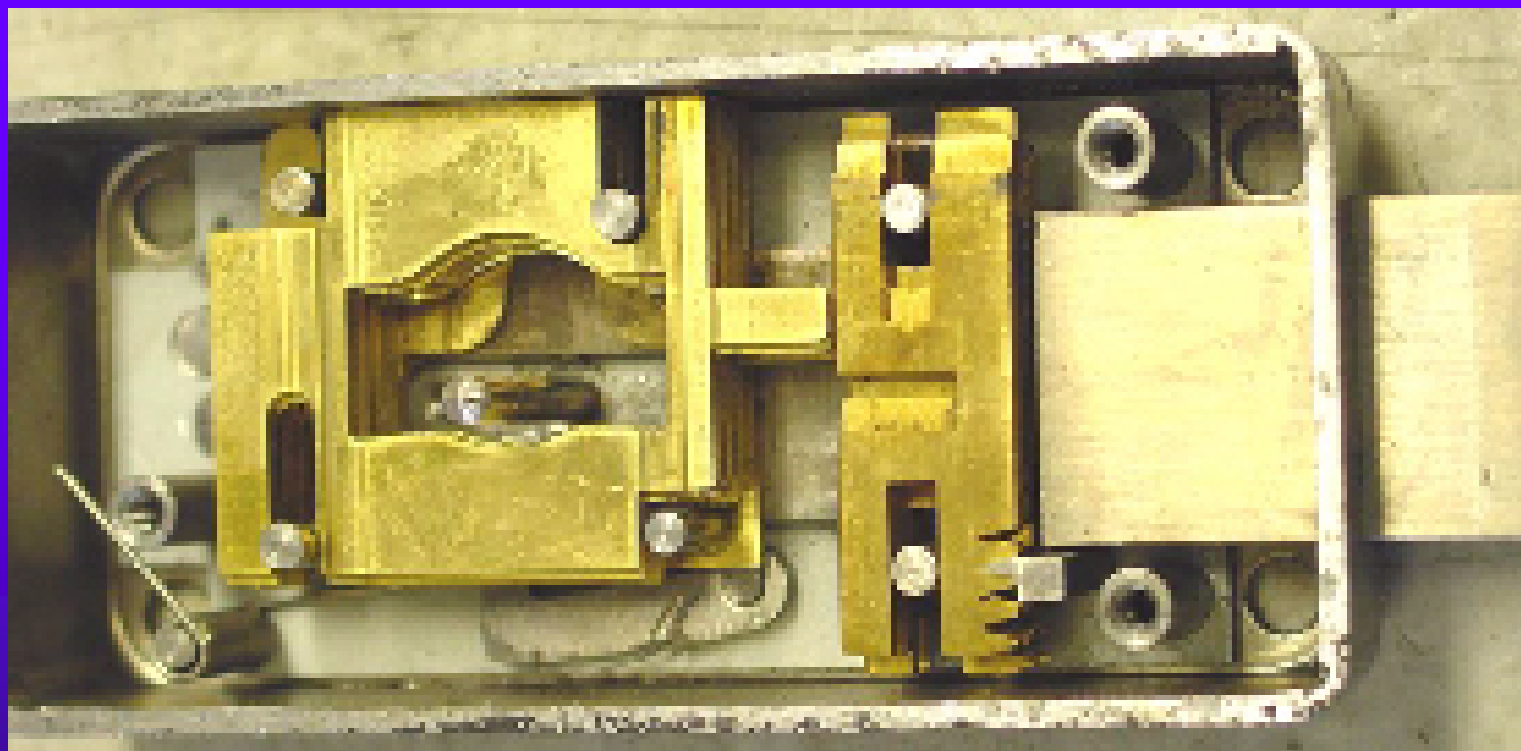
# MODERN CHUBB LEVER



# KROMER HIGH SECURITY



# STUV LEVER LOCK



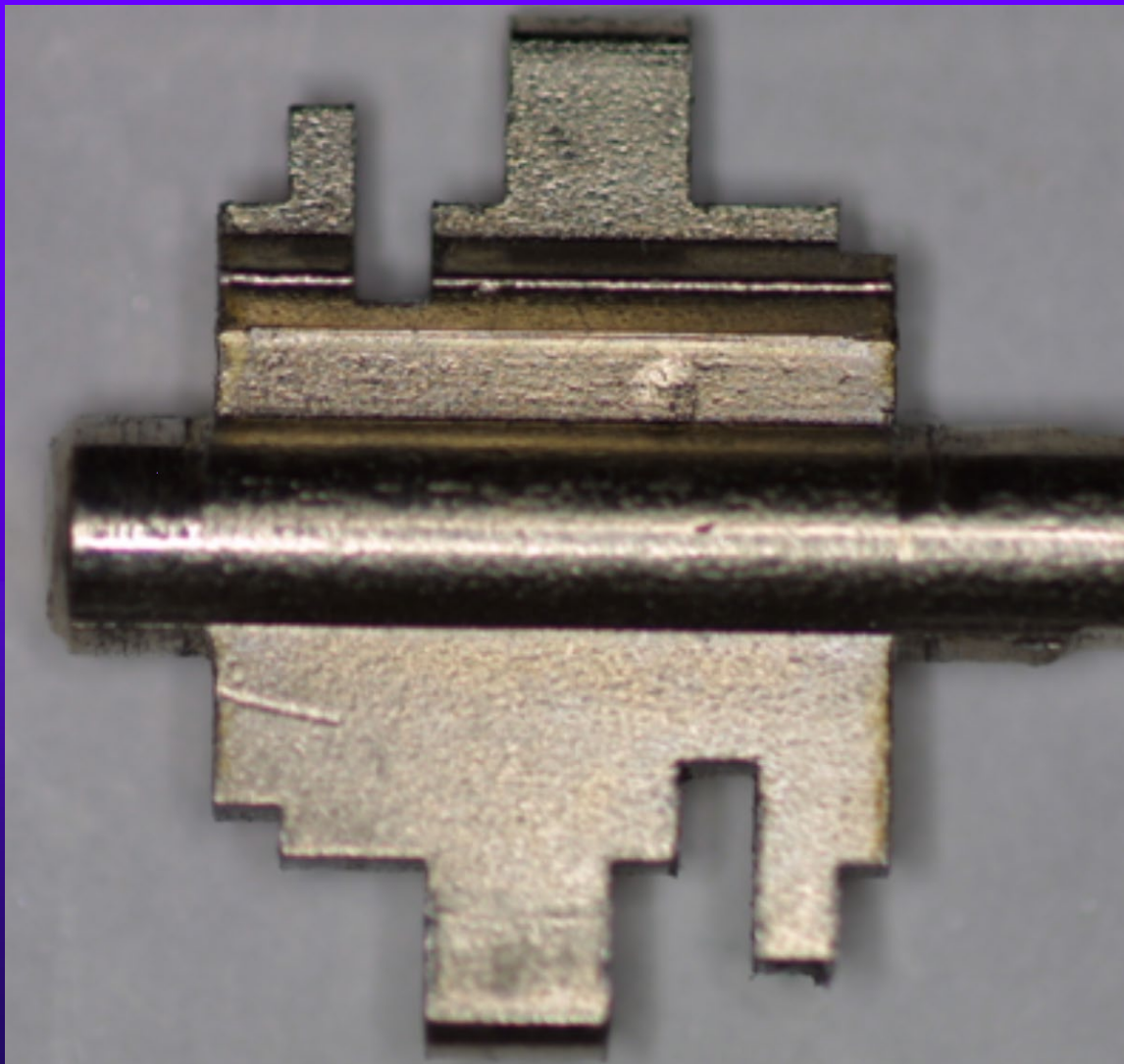


# EUROPEAN LEVER LOCK

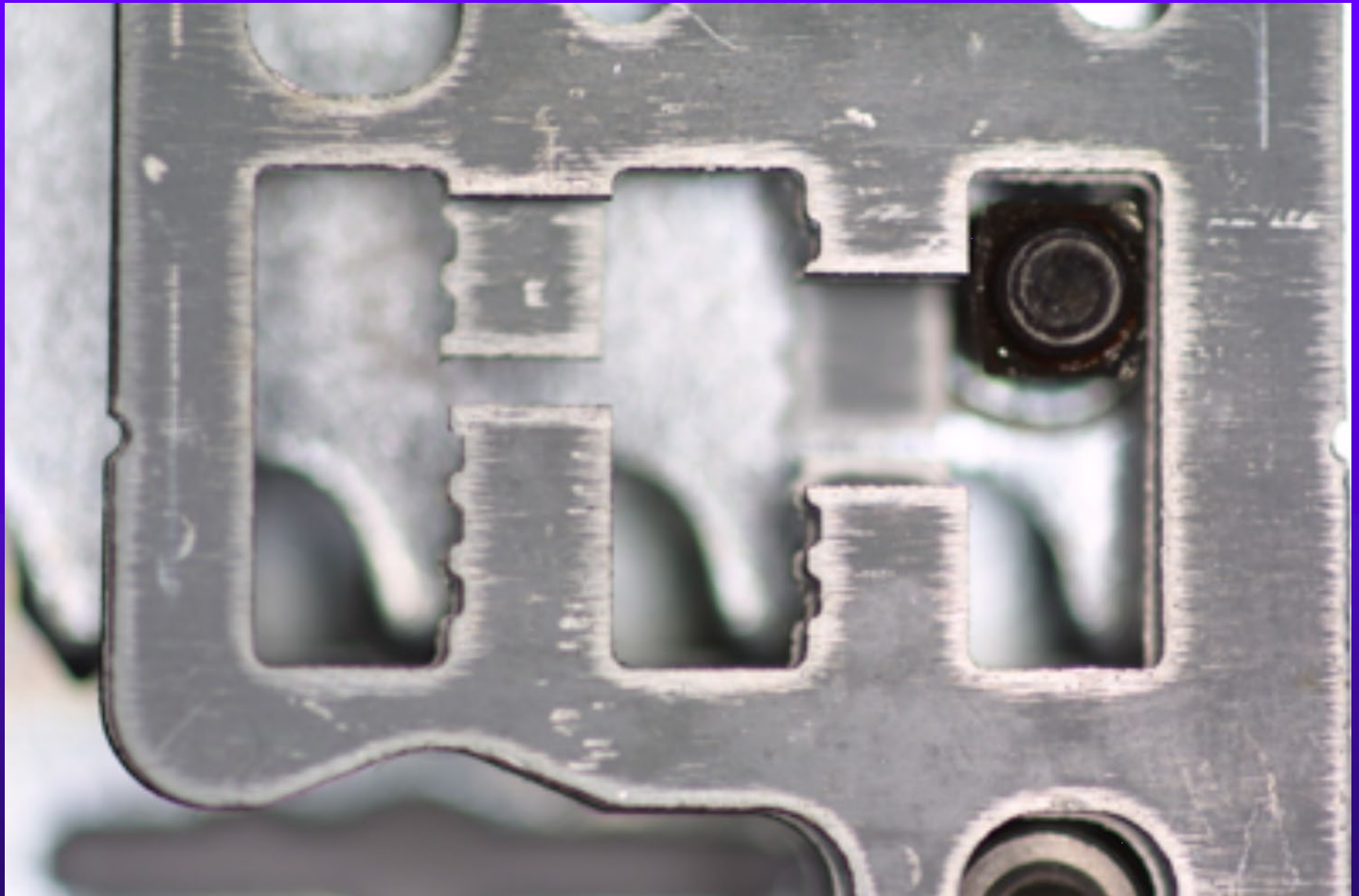




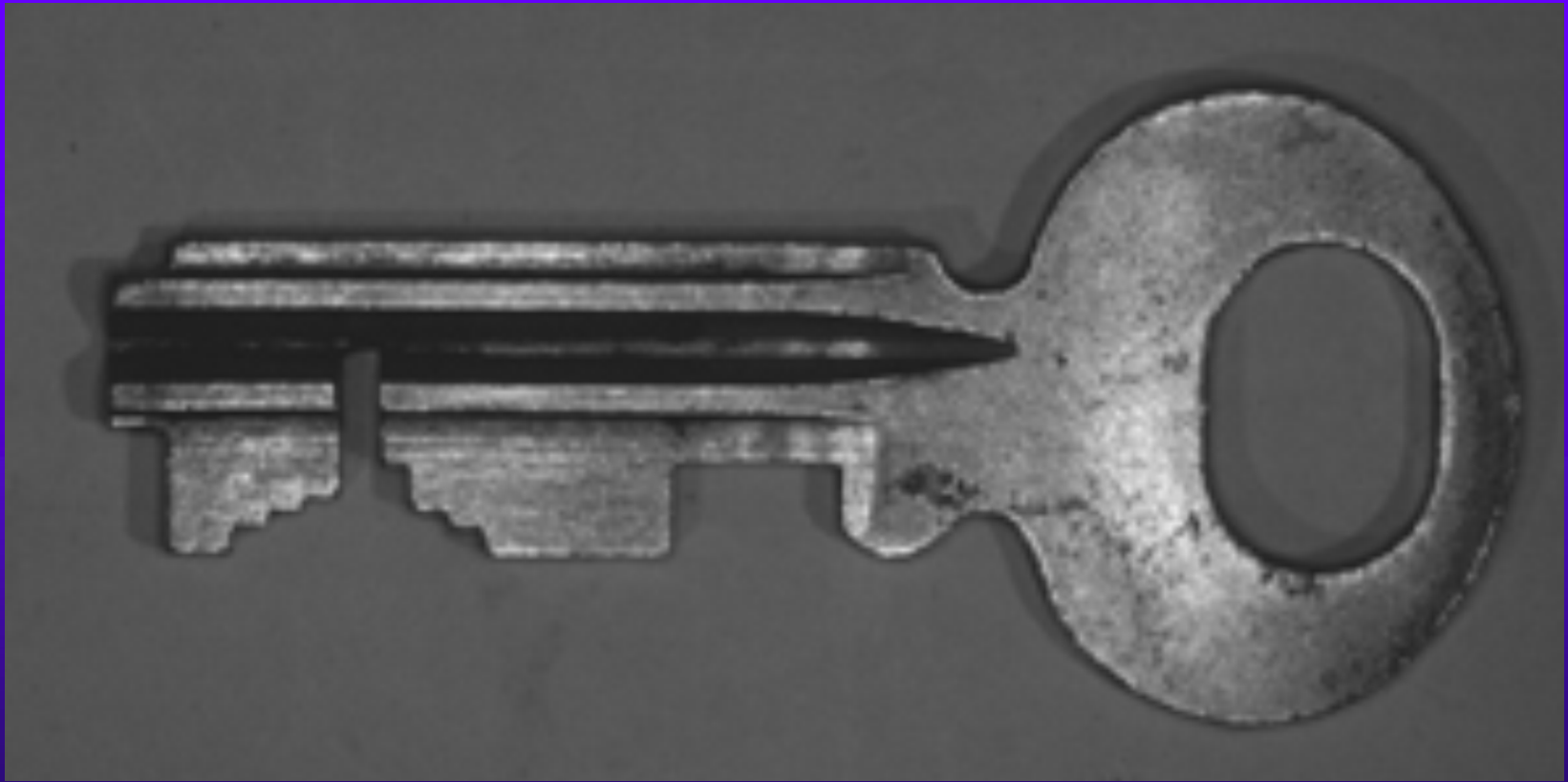
# EUROPEAN LEVER KEY



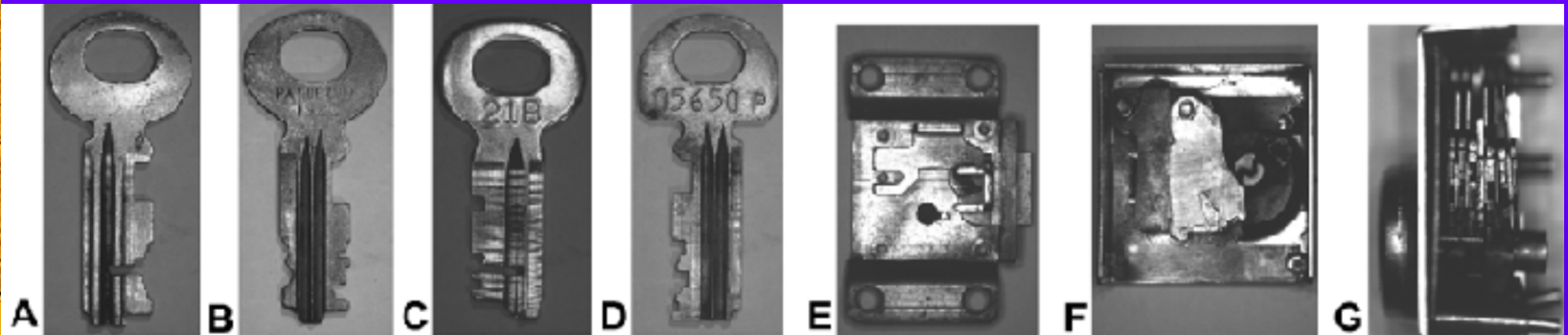
# EUROPEAN LEVER DESIGN



# TELEPHONE LEVER KEY

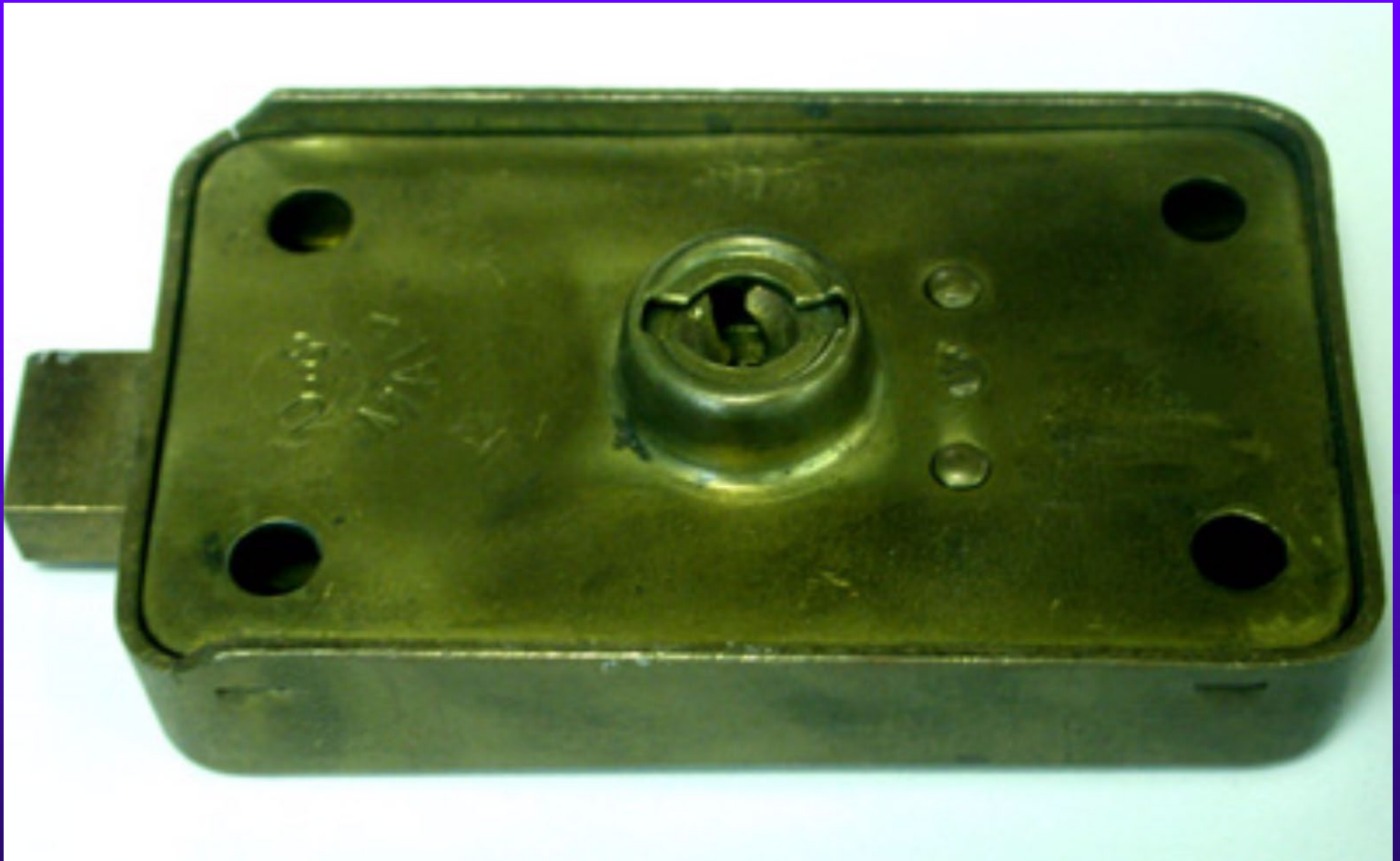


# TELEPHONE LOCK DETAIL





# POST OFFICE LEVER LOCK



# Lever Key Detail – Postal



# Lever Detail – Postal





# POSTAL Registered Mail Key



# Registered Mail Padlock



# NAZI SUBMARINE LEVER LOCK

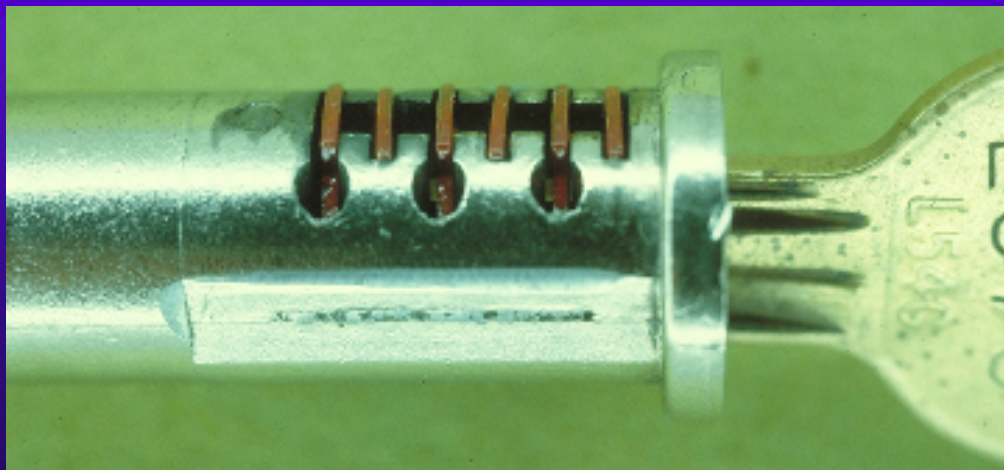
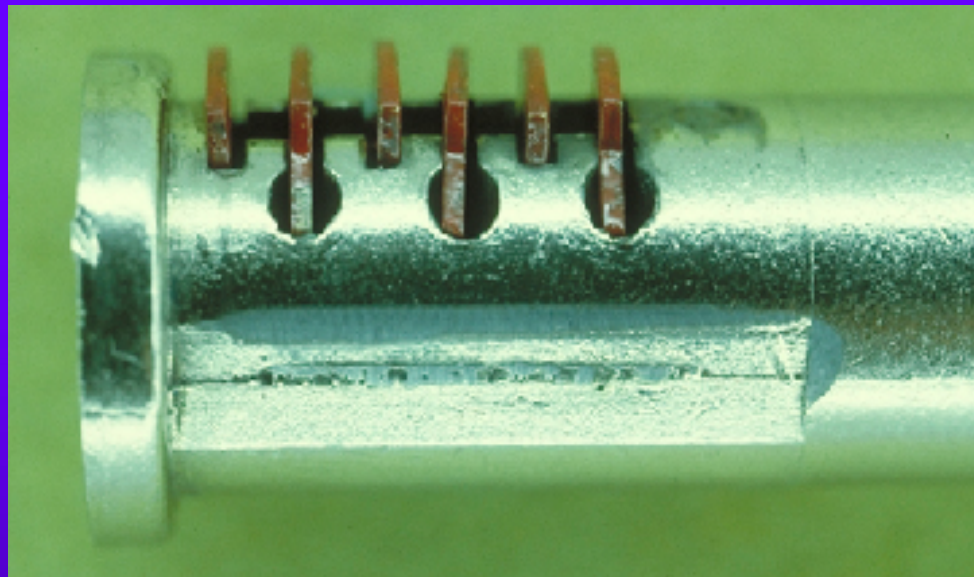




# WAFER LOCK



# WAFER TUMBLER LOCK



# WAFER LOCK – LOCKED

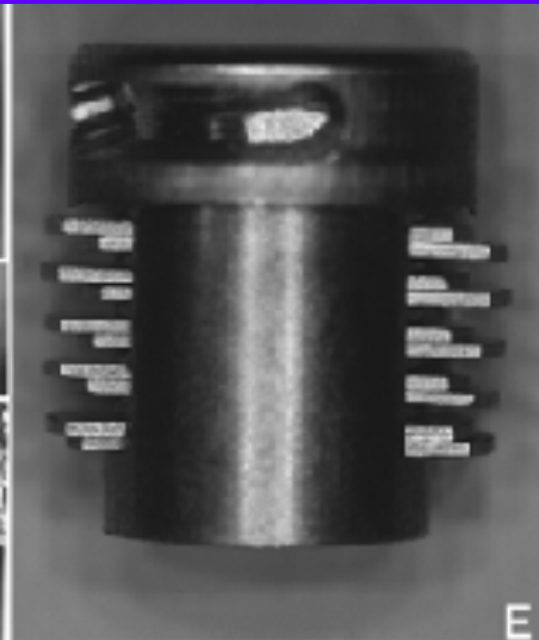
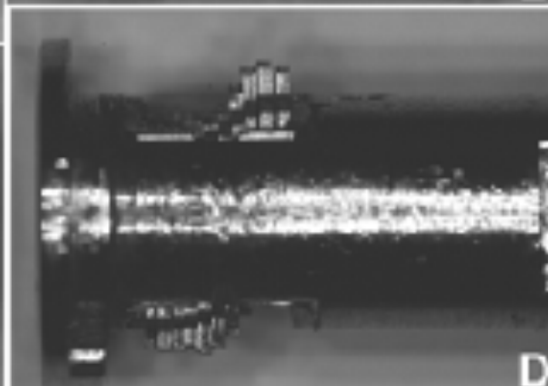
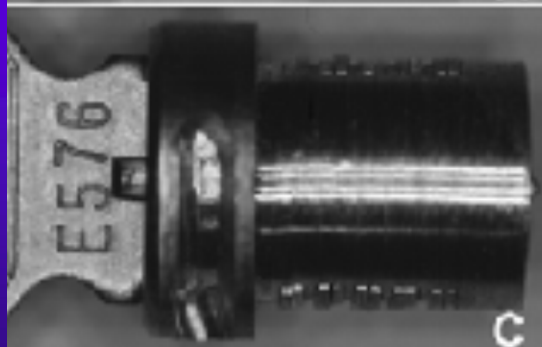
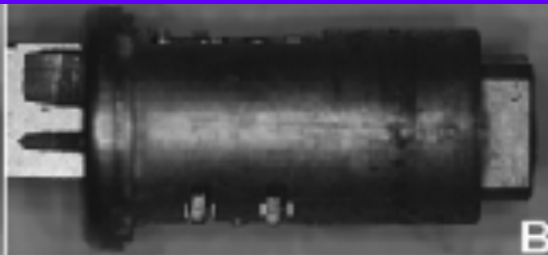
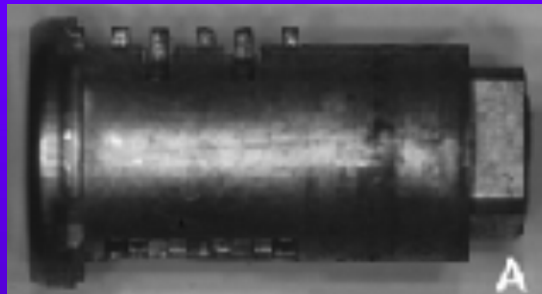




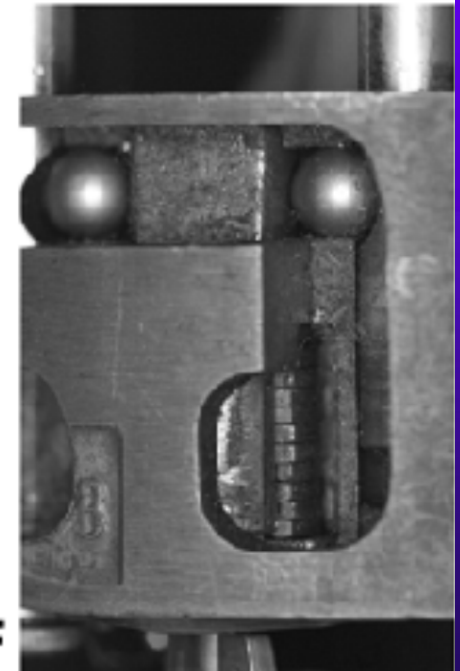
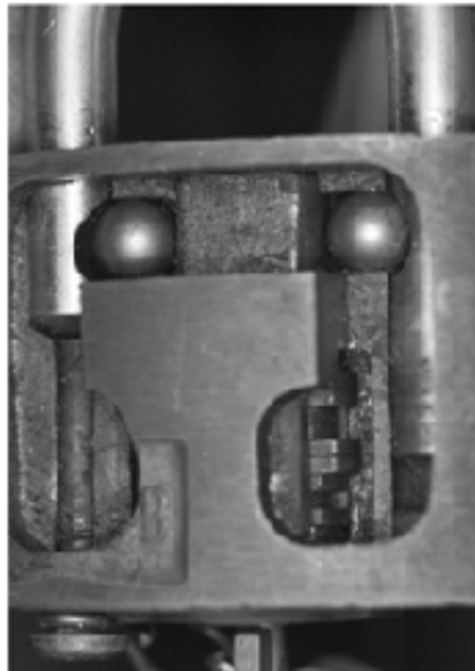
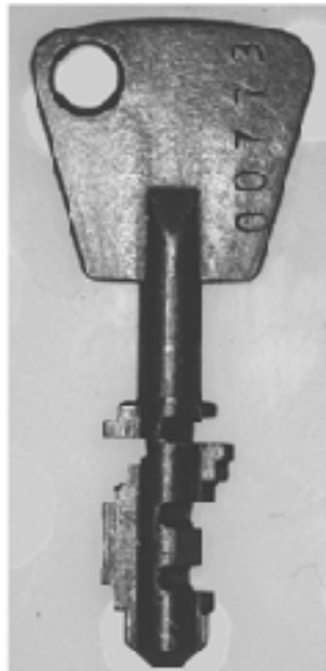
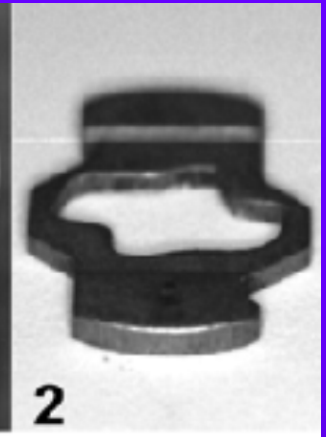
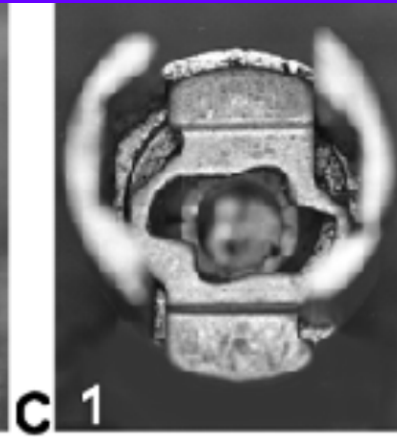
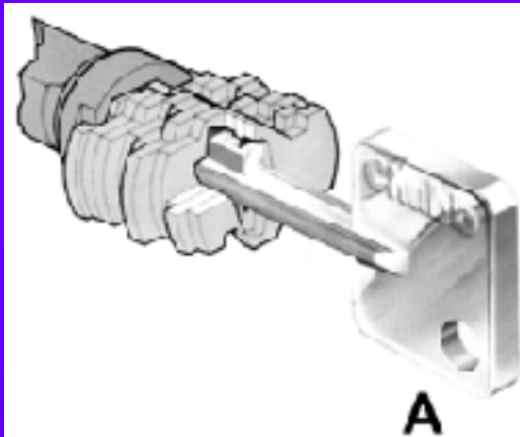
# WAFER LOCK – OPEN



# WAFER LOCKS – DOUBLE BITTED



# CHUBB AVA WAFER





# PIN TUMBLER LOCK



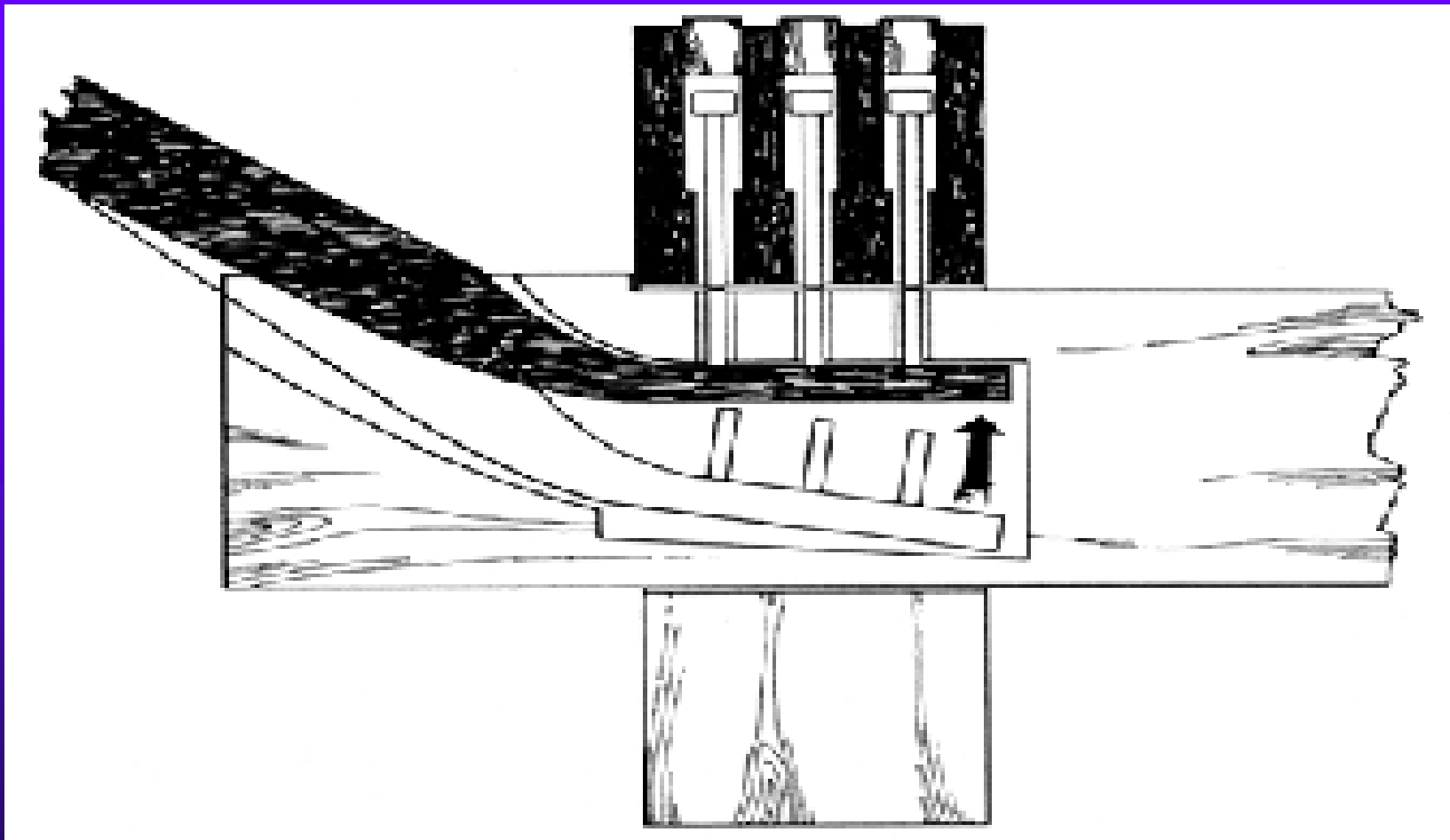


# PIN TUMBLER LOCKS

- ◆ Top pins
- ◆ Bottom pins
- ◆ Master pins
- ◆ Pin stack
- ◆ Shear line



# PIN TUMBLER – EGYPTIAN

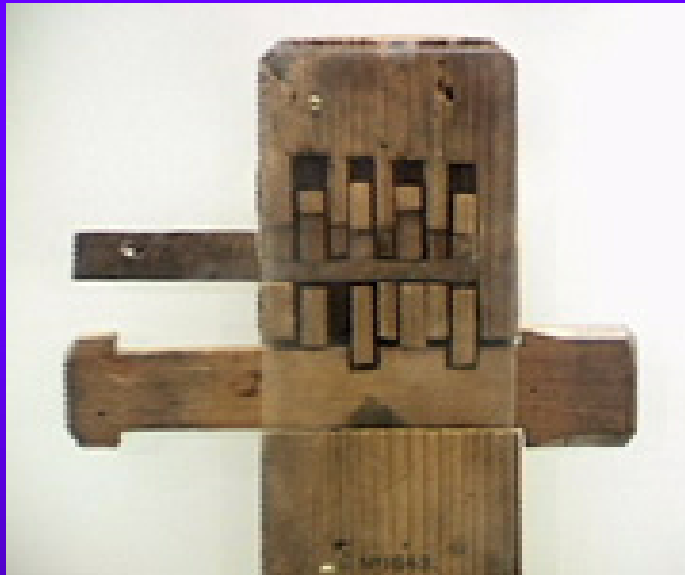


# EGYPTIAN DETAIL





# EGYPTIAN PIN TUMBLER





# MODERN DESIGN





# PIN TUMBLER LOCK PARTS

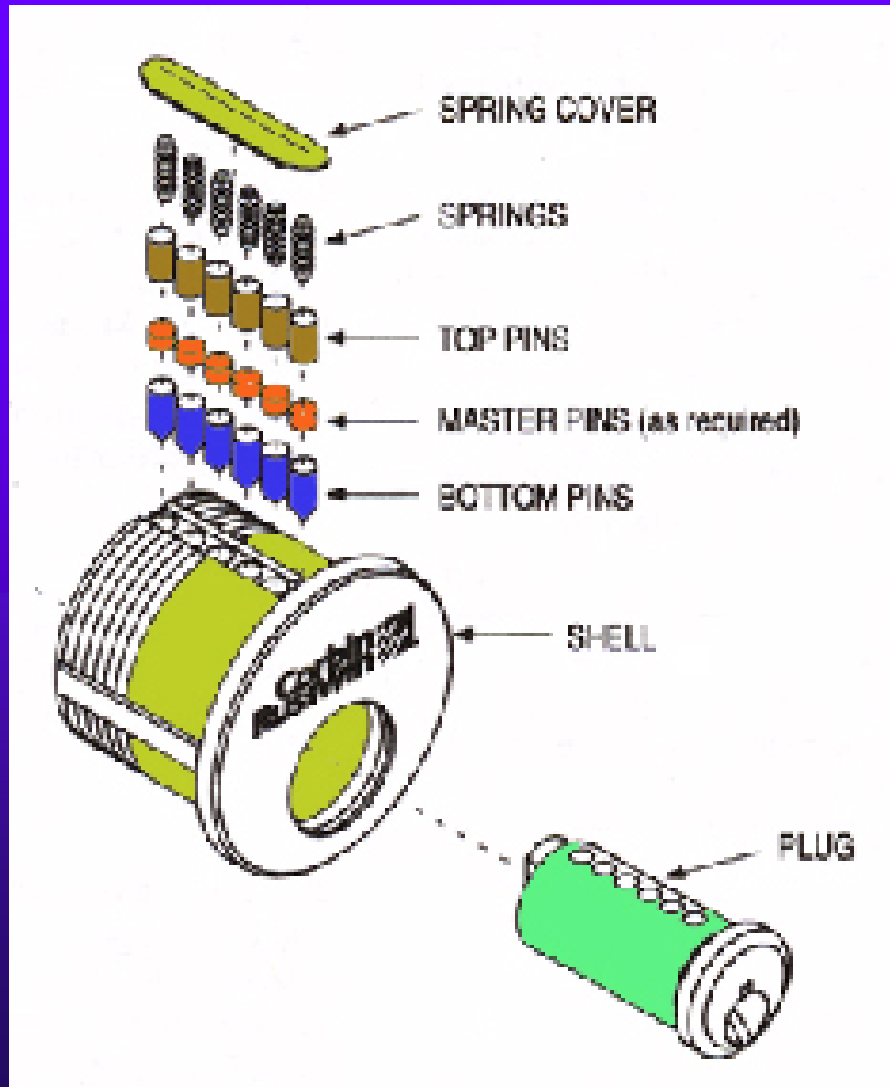
- ◆ Ubiquitous in most parts of the world
  - at least one protects your home and office
- ◆ A *shell*, mounted on the door (or whatever)
- ◆ A *plug*, which can rotate freely within the shell and which is linked to the locking mechanism
- ◆ A *keyway* slot, cut into the front of the plug



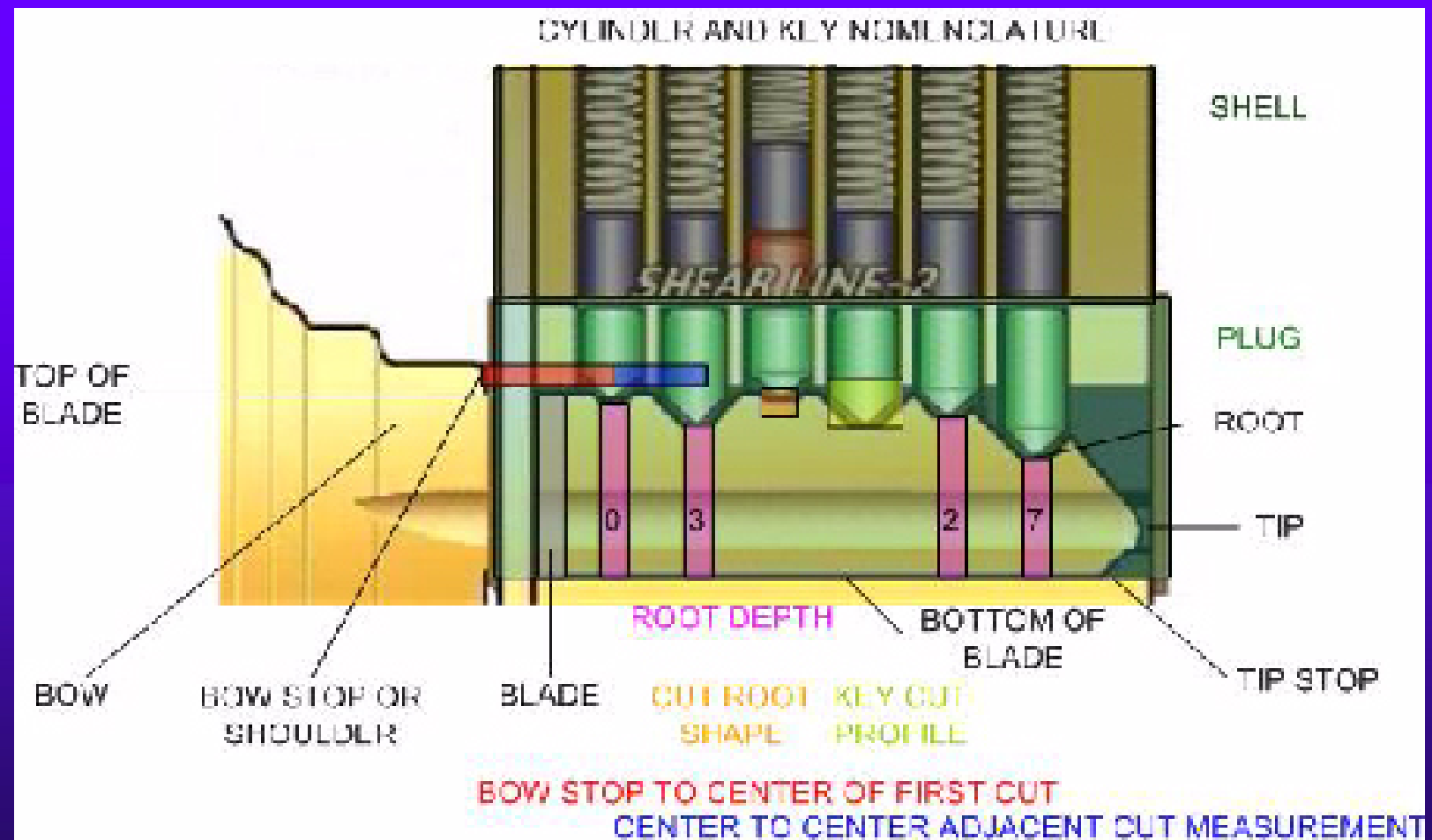
# Pin Tumbler Lock

- ◆ Inside a pin tumbler lock
- ◆ The *shear line* is the plug/shell boundary
- ◆ A set of *pin stacks* protrude from holes in the shell into holes in the plug
  - prevents the plug from rotating
  - typically held down by springs
- ◆ Each pin stack has a corresponding key *cut*
  - height corresponds to the correct key
  - with no key in lock, all cuts sit within the plug
  - when all cuts line up at the shear line, plug can rotate

# PIN TUMBLER DETAIL



# PIN TUMBLER NOMENCLATURE





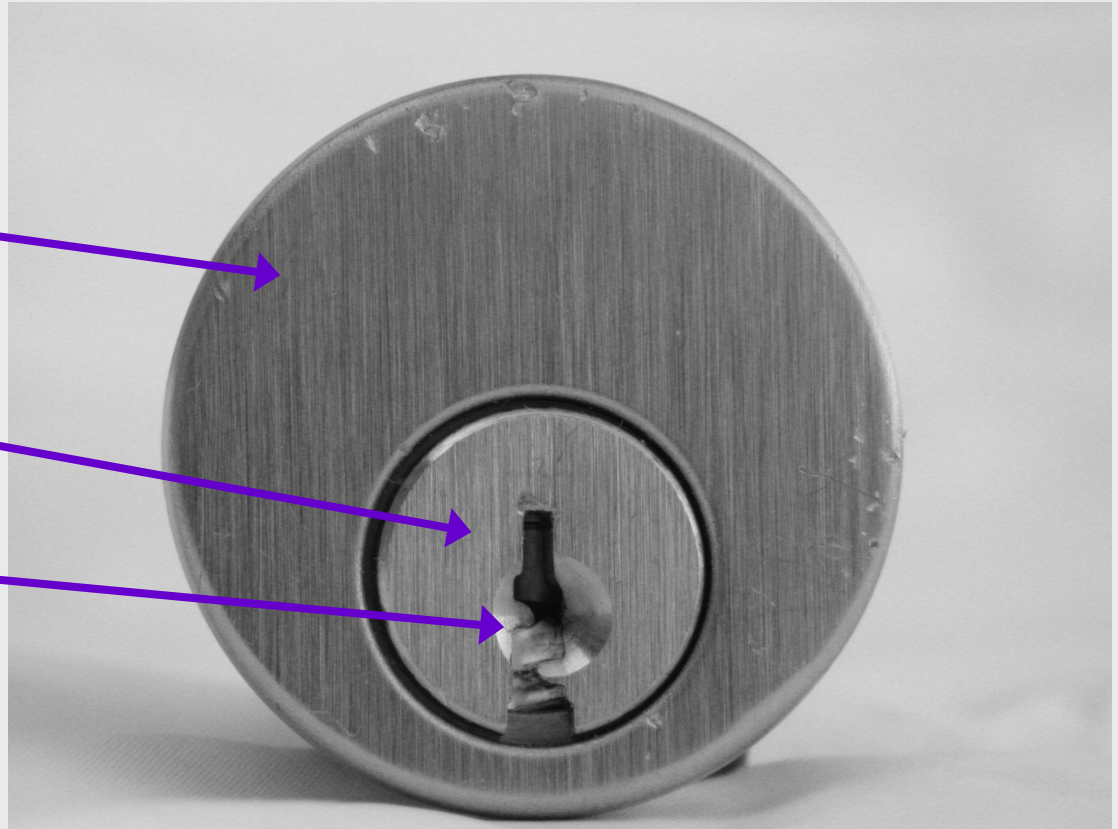
# Pin Tumbler Lock



Shell

Plug

Keyway slot



# Inside the Pin Tumbler Lock



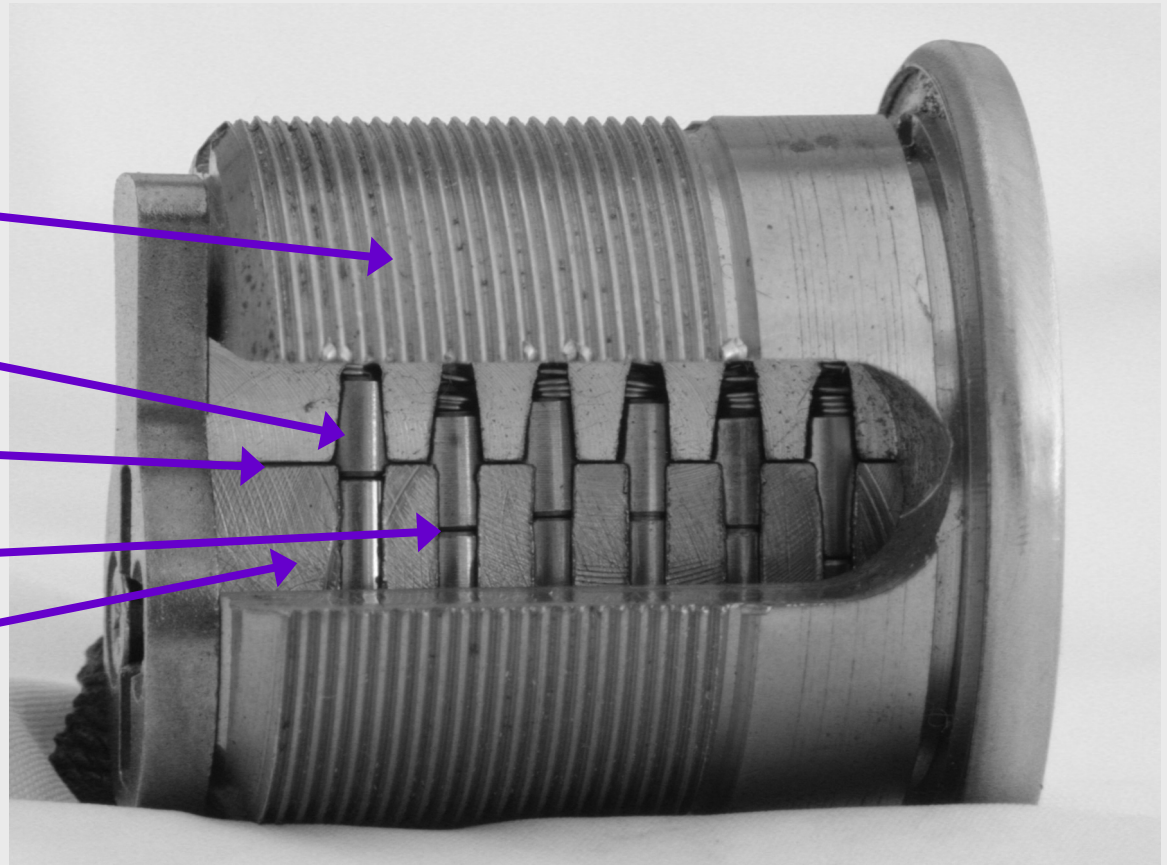
Shell

Pin stack

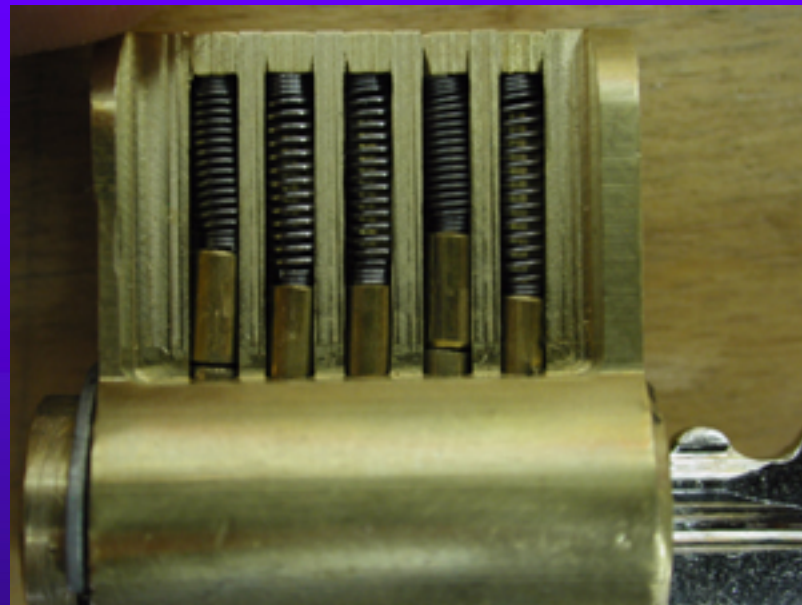
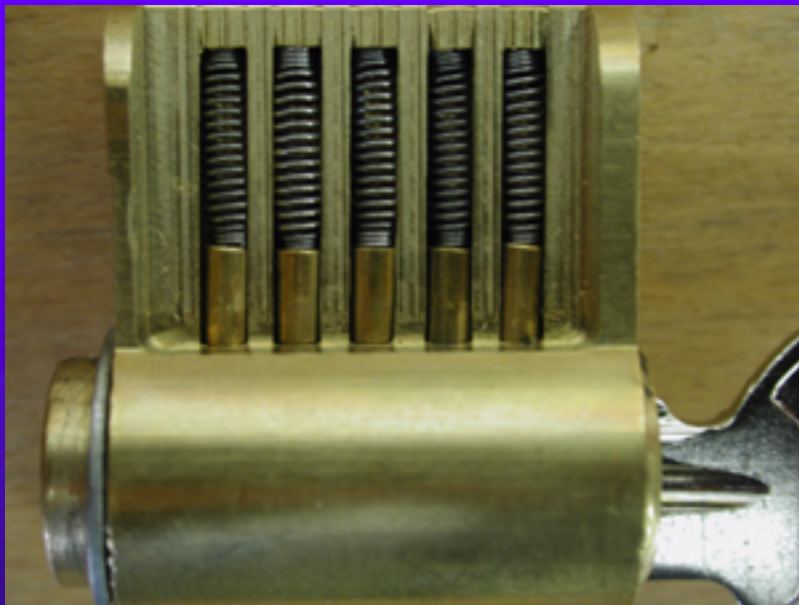
Shear line

Cut

Plug

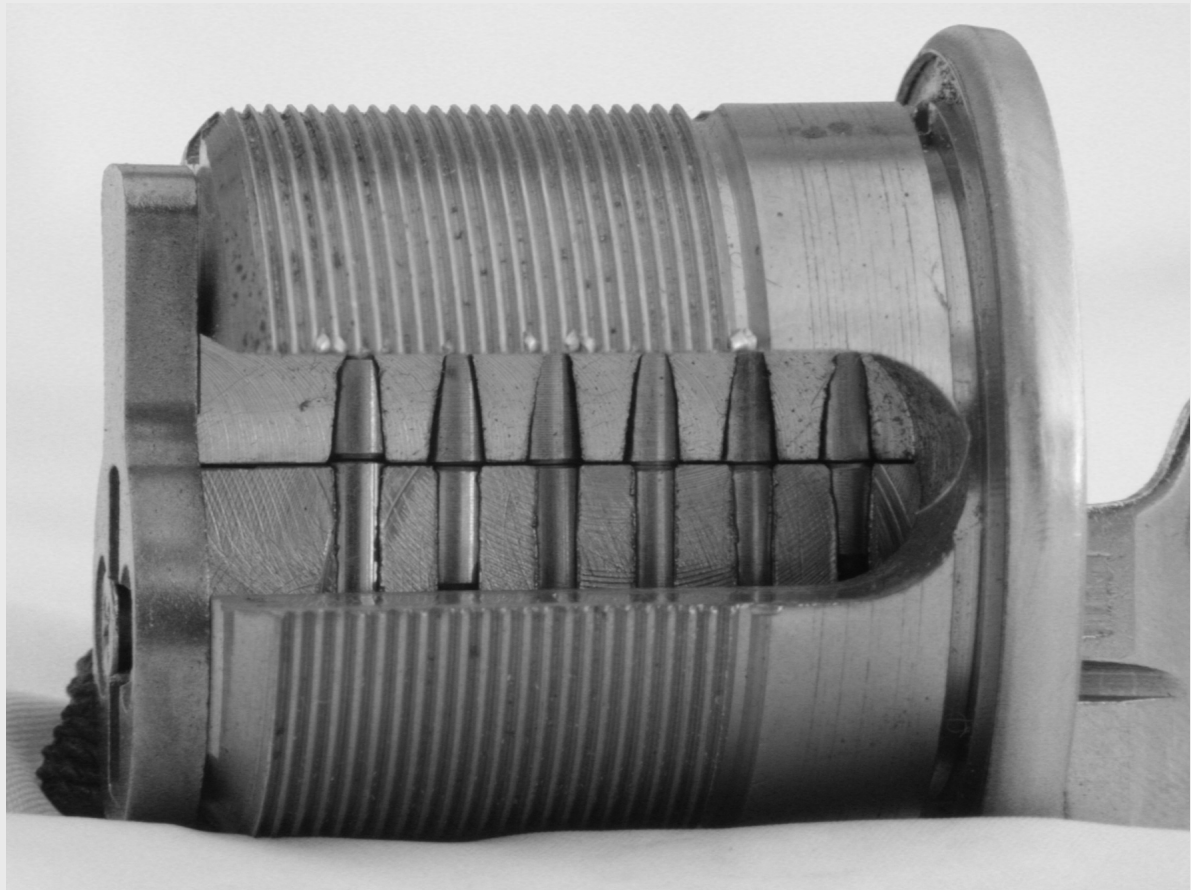


# SHEAR LINE



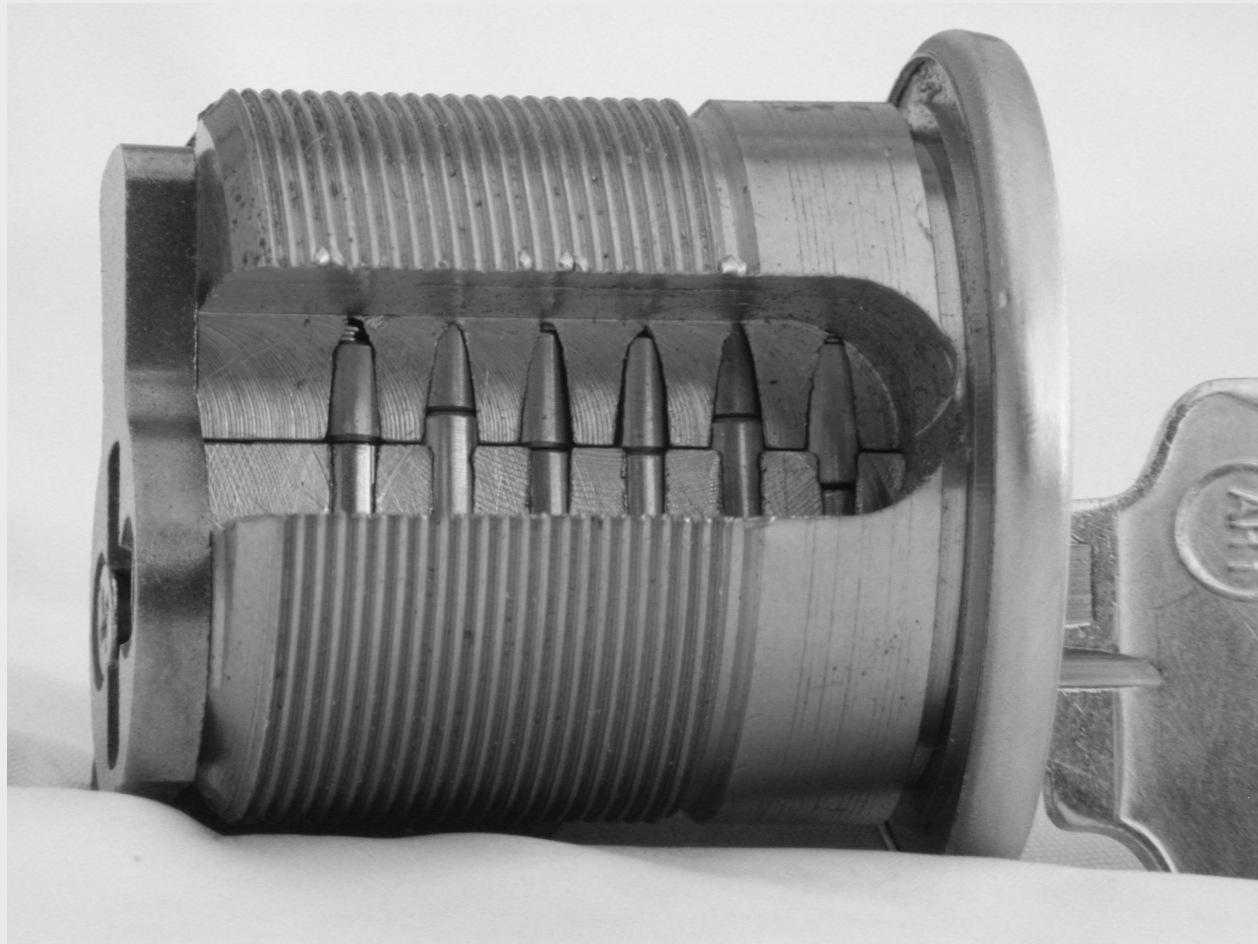


# Correct Key Inserted

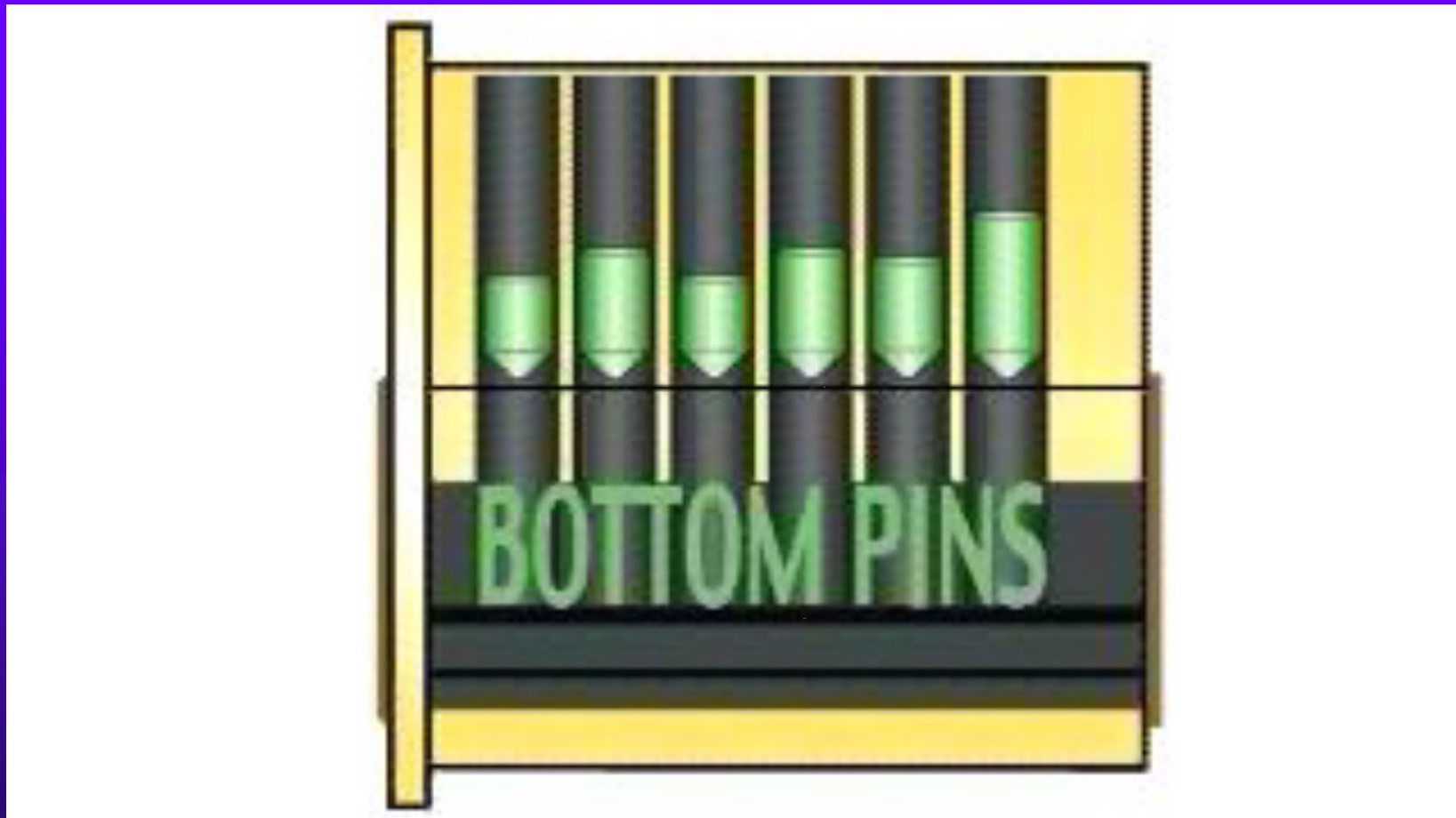




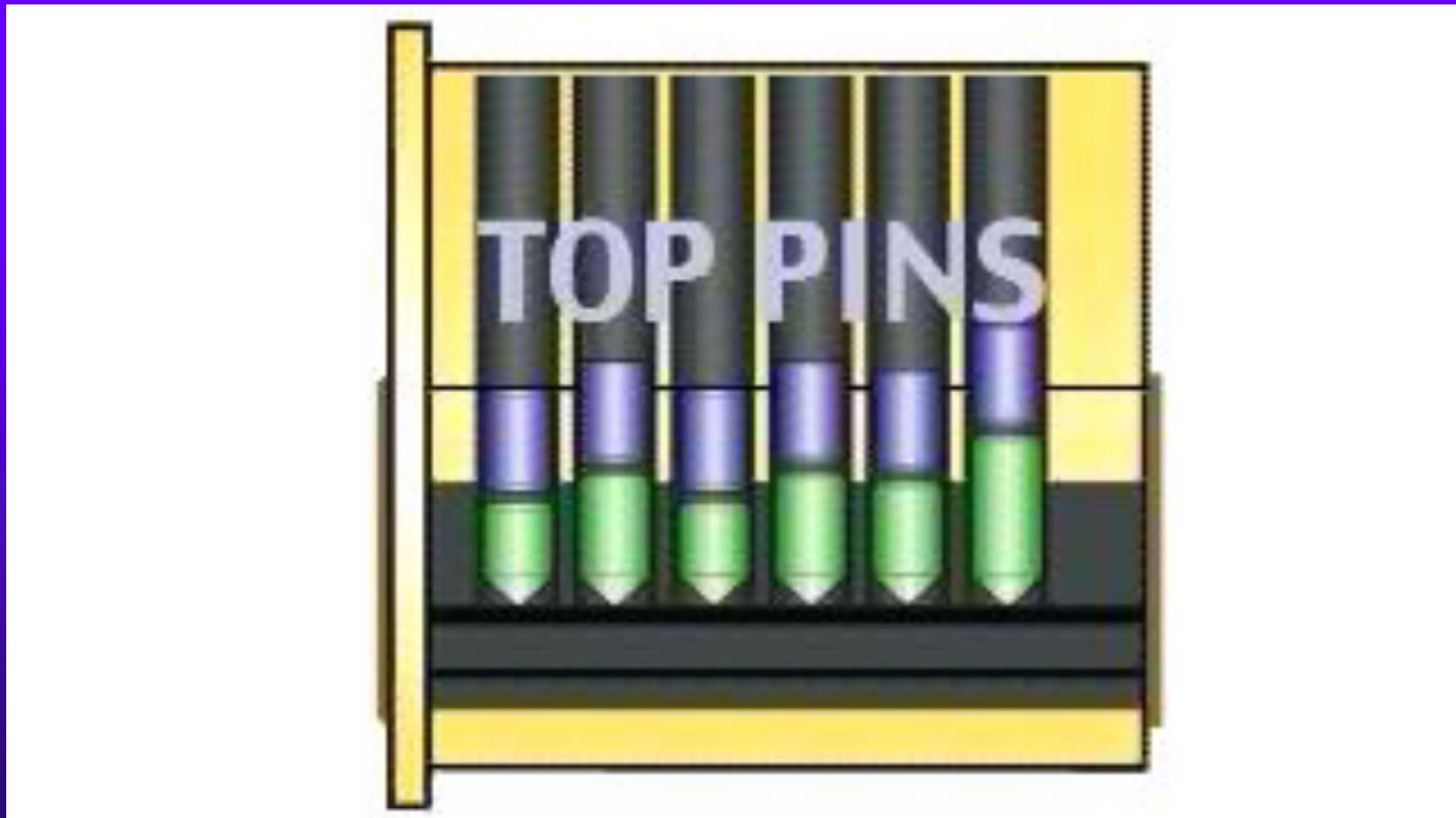
# Incorrect Key Inserted



# Bottom Pin Detail

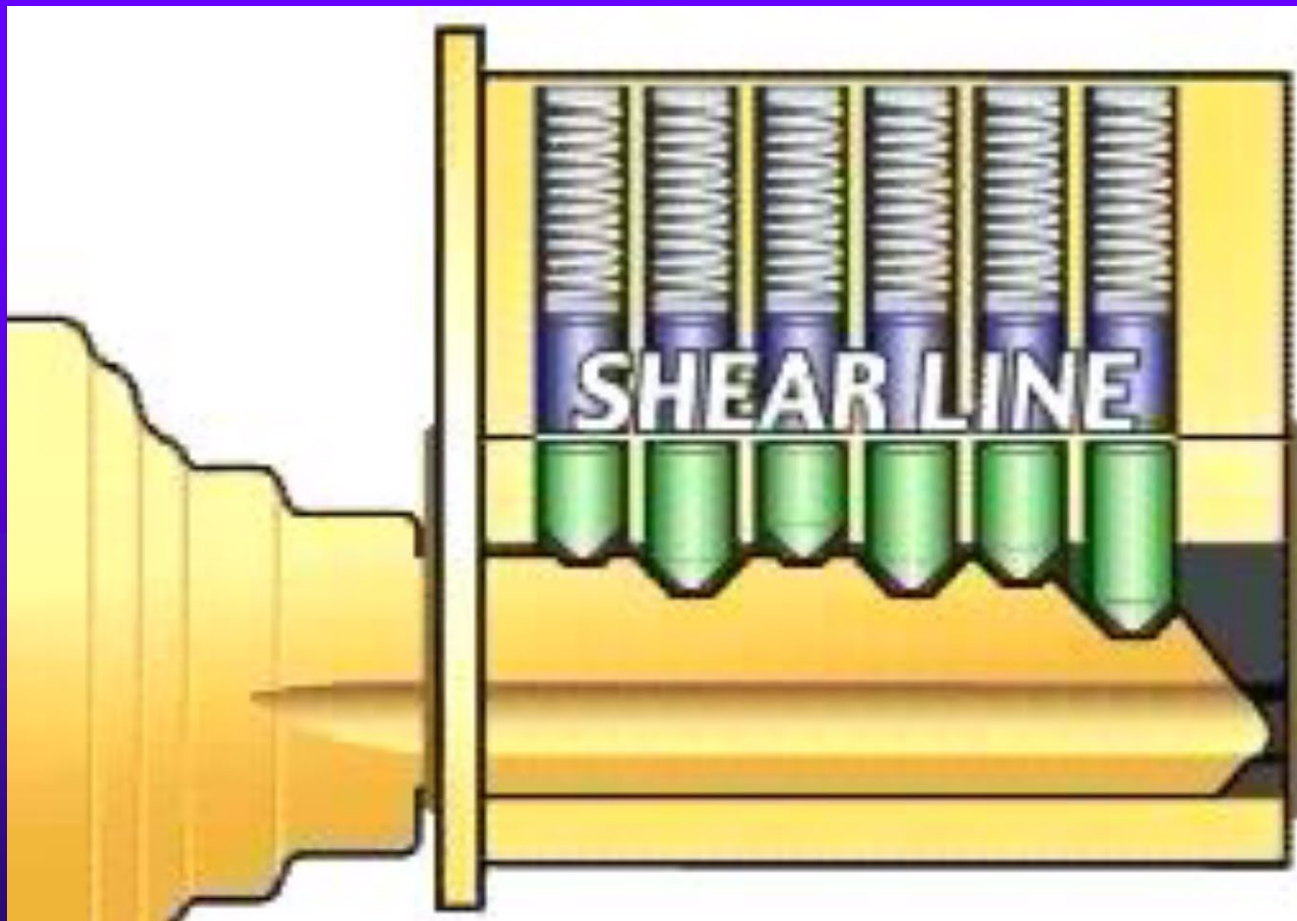


# Top Pin Detail



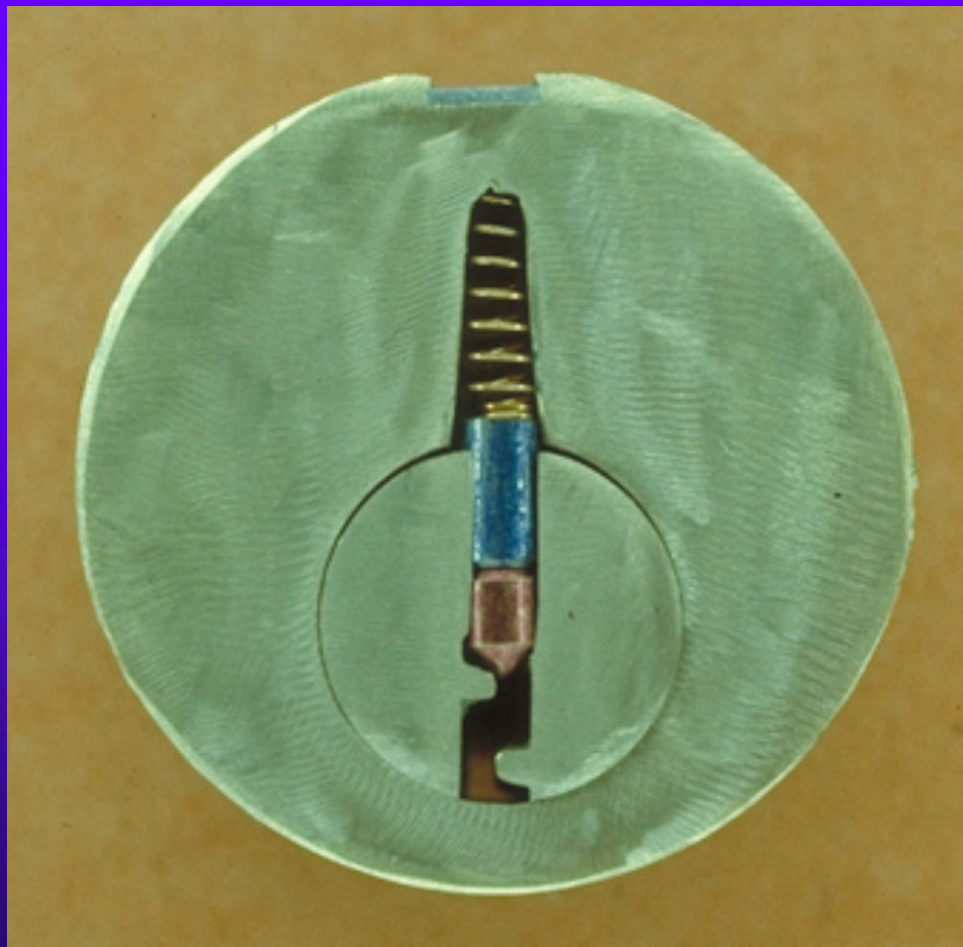


# Shear Line

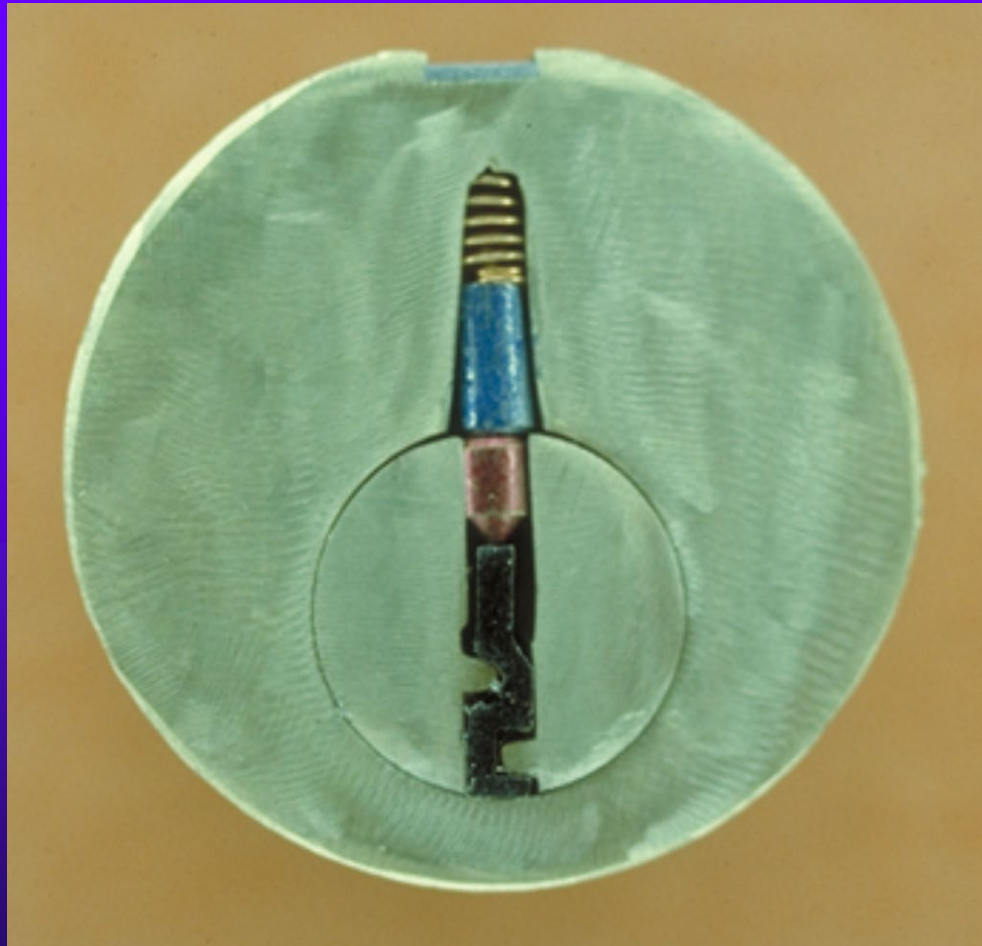




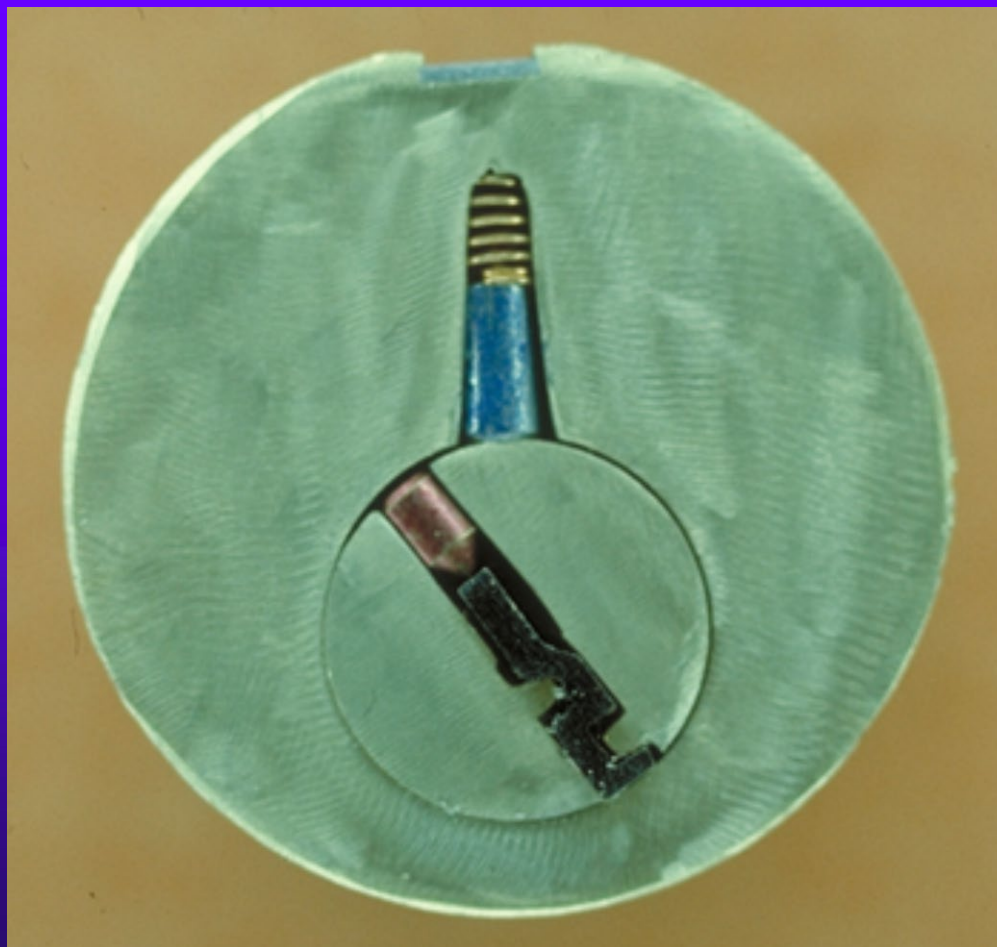
# Locked



# Pins at Shear Line

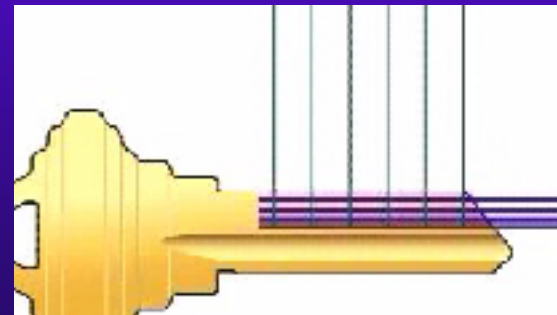
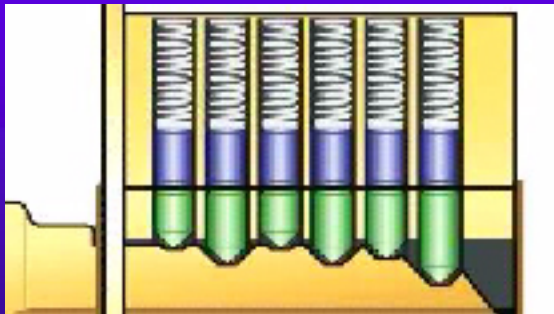
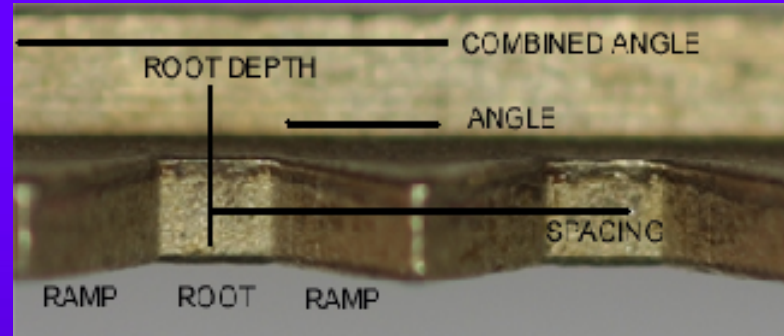
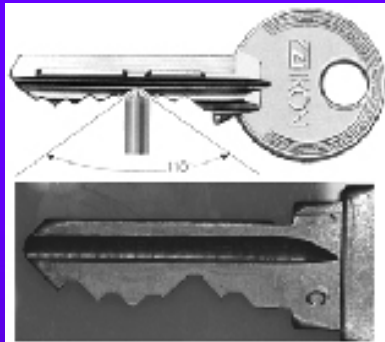


# Plug Rotated



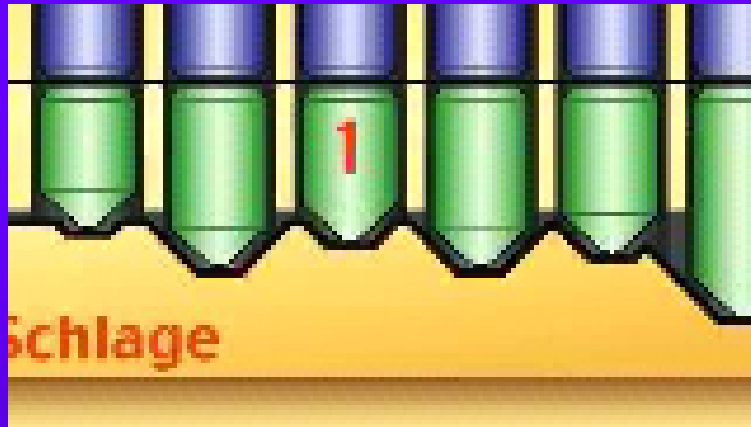


# PIN TUMBLER DEPTHS AND SPACES AND KEY DESIGN

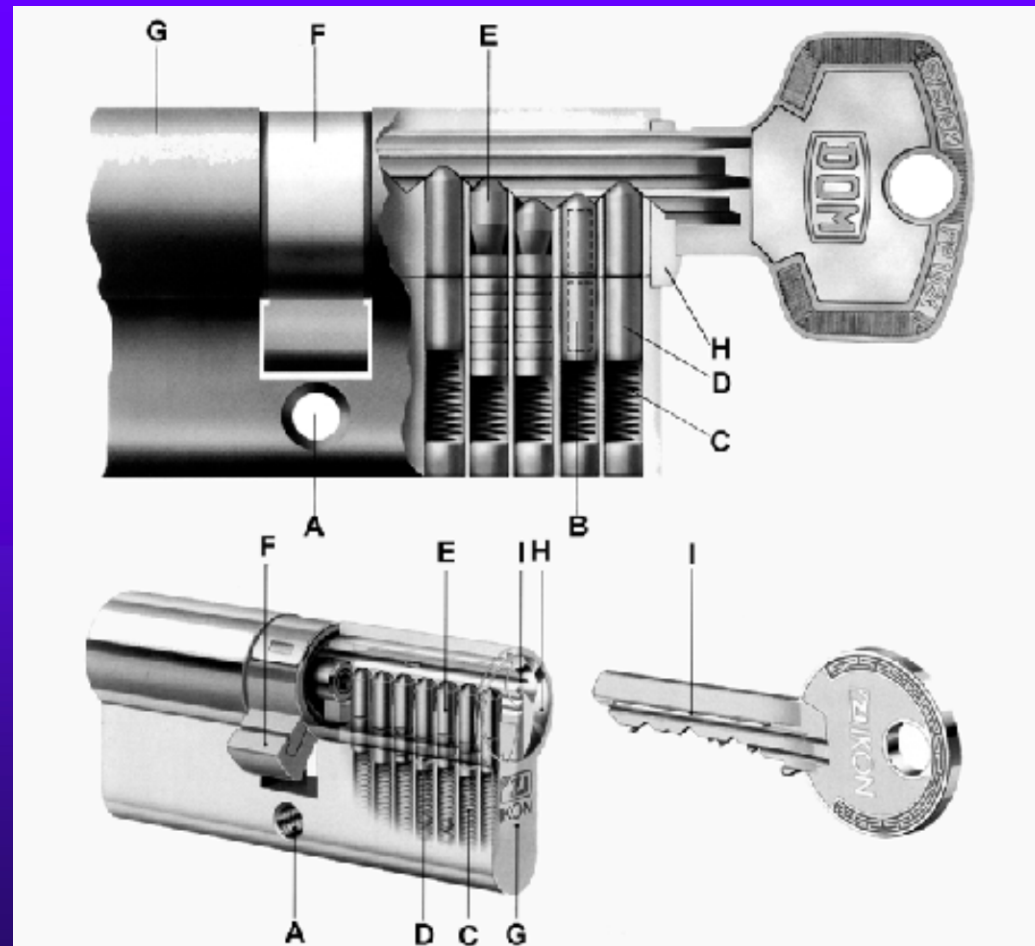




# SCHLAGE DEPTHS



# DOM PIN TUMBLER LOCK





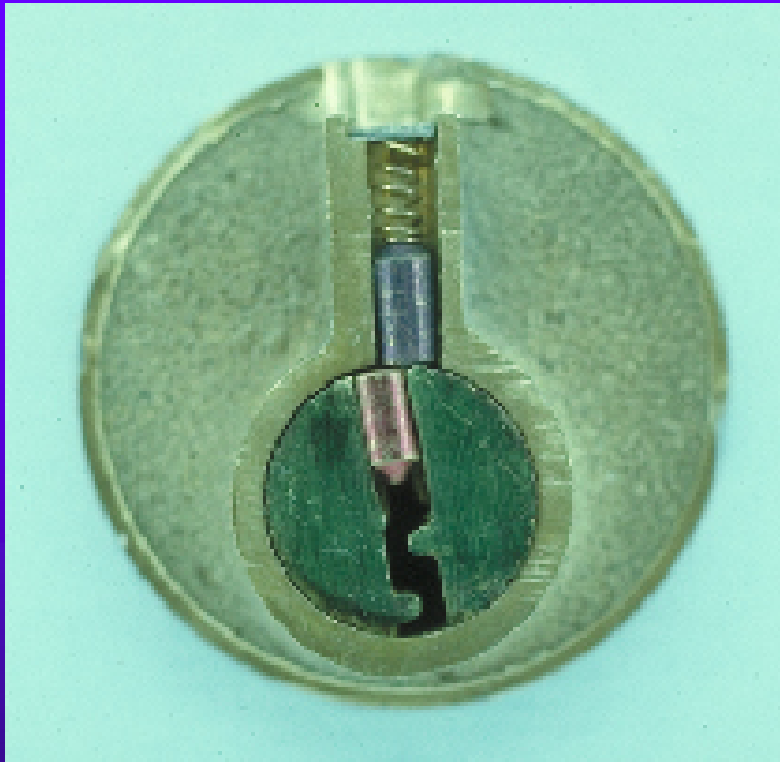
# SECURITY TUMBLERS AND PICK RESISTANCE

# PARACENTRIC KEYWAY

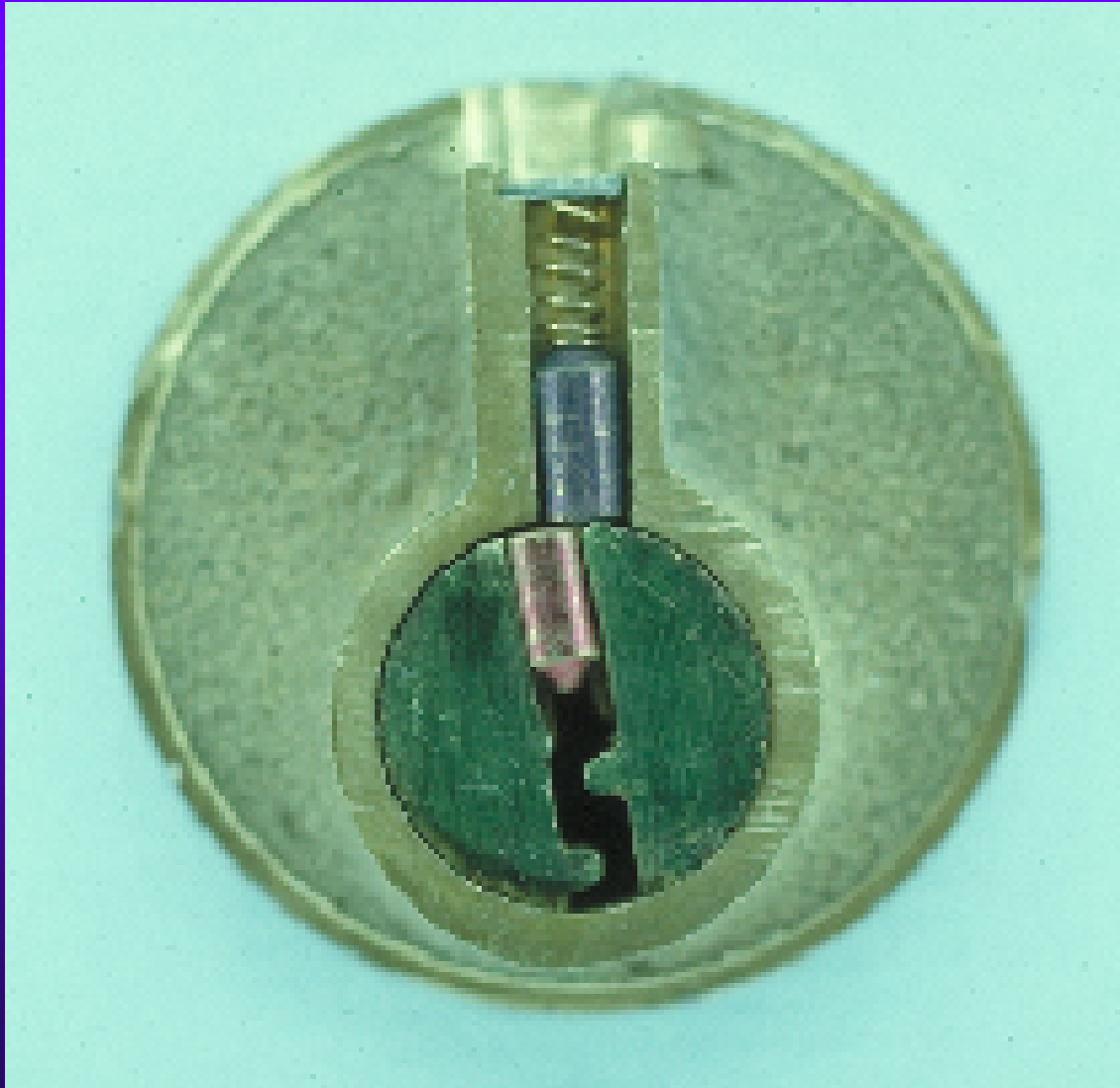




# SECURITY TUMBLERS and PICK RESISTANCE



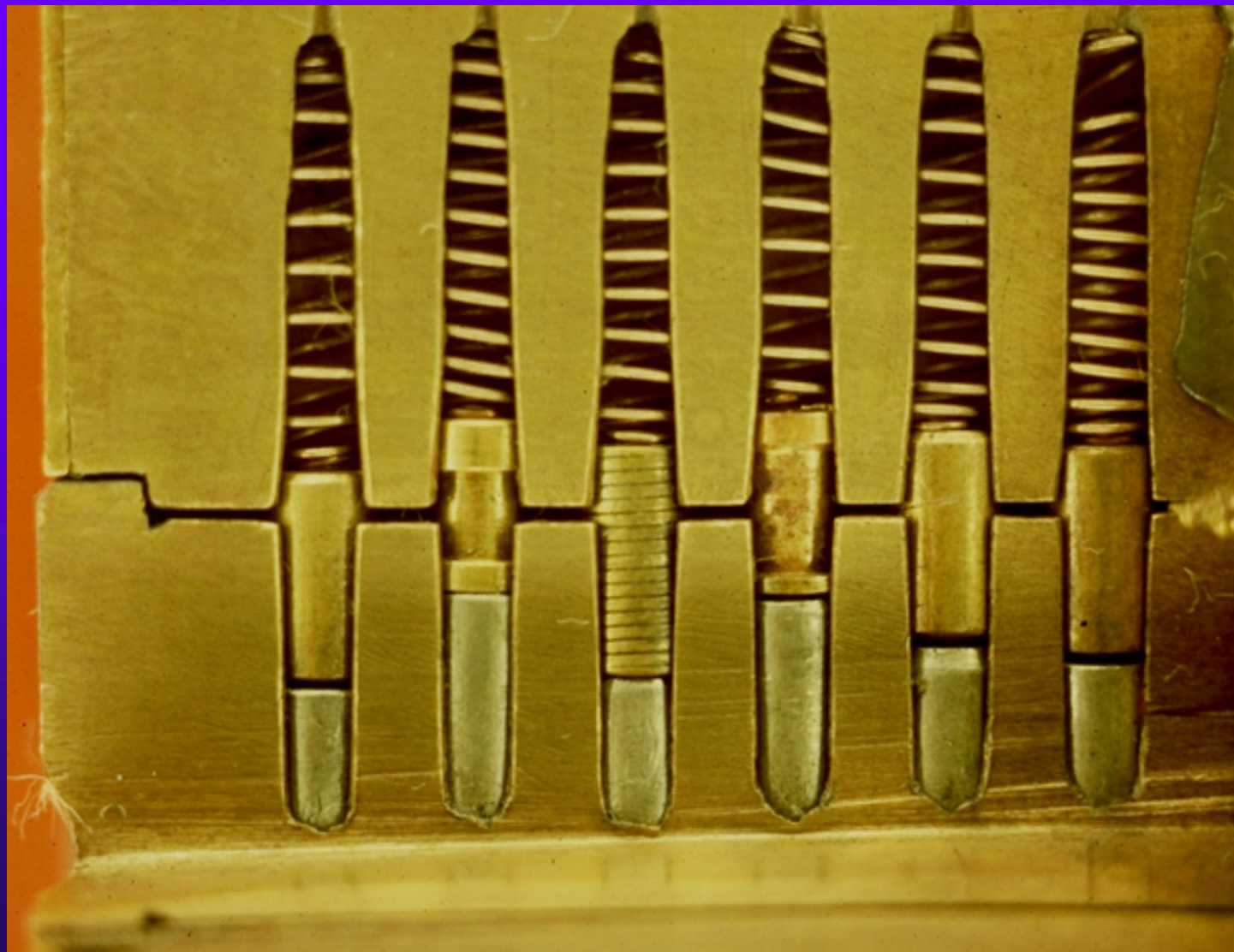
# PLUG CAN ROTATE



# PLUG BLOCKED

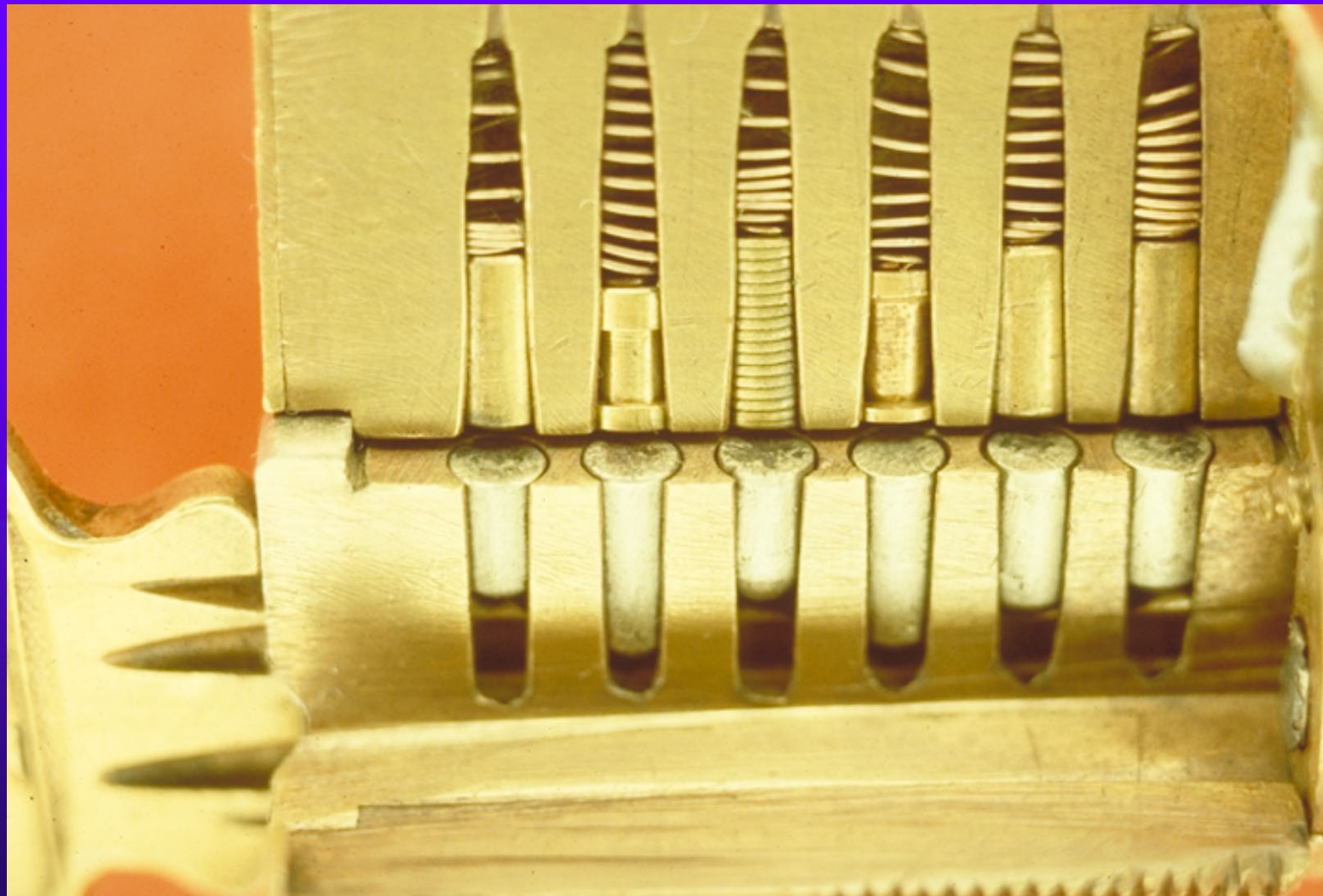


# SECURITY PINS

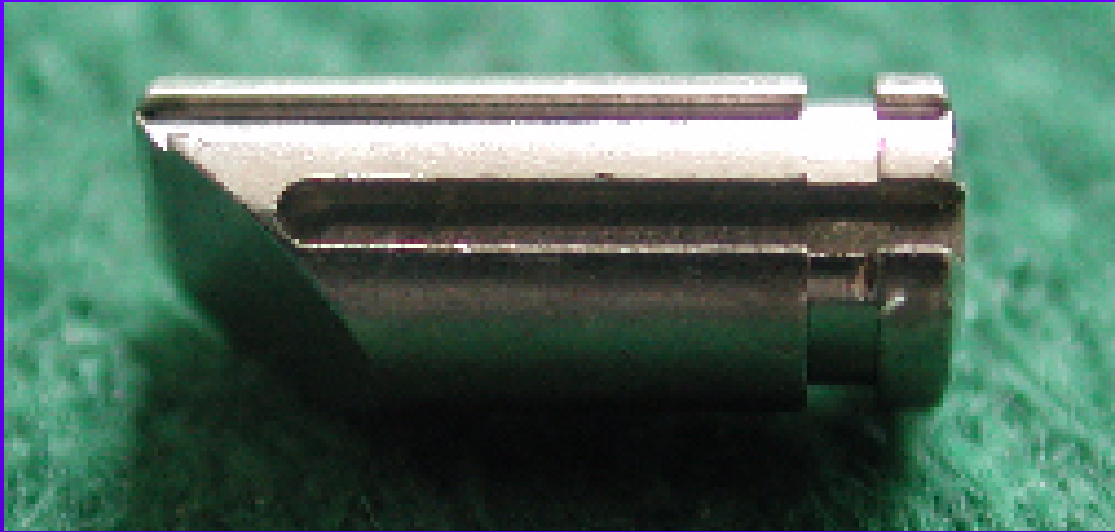




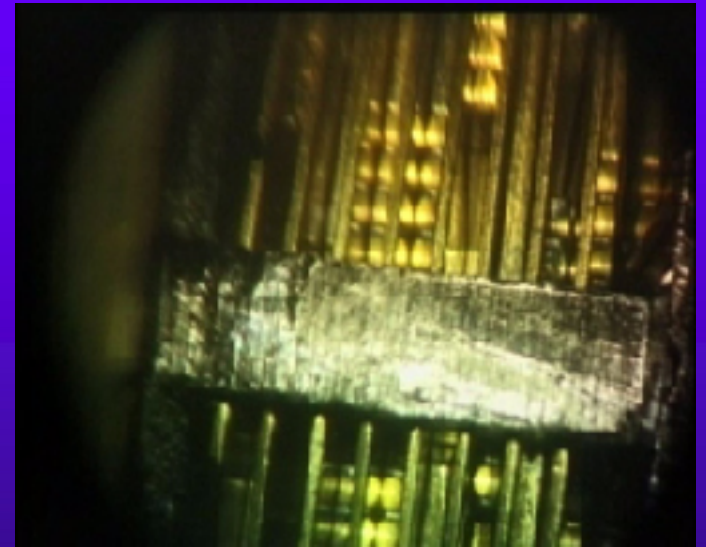
# SECURITY PIN DETAIL



# MEDECO PINS



# LEVER LOCK FALSE NOTCHES: Rosengrens



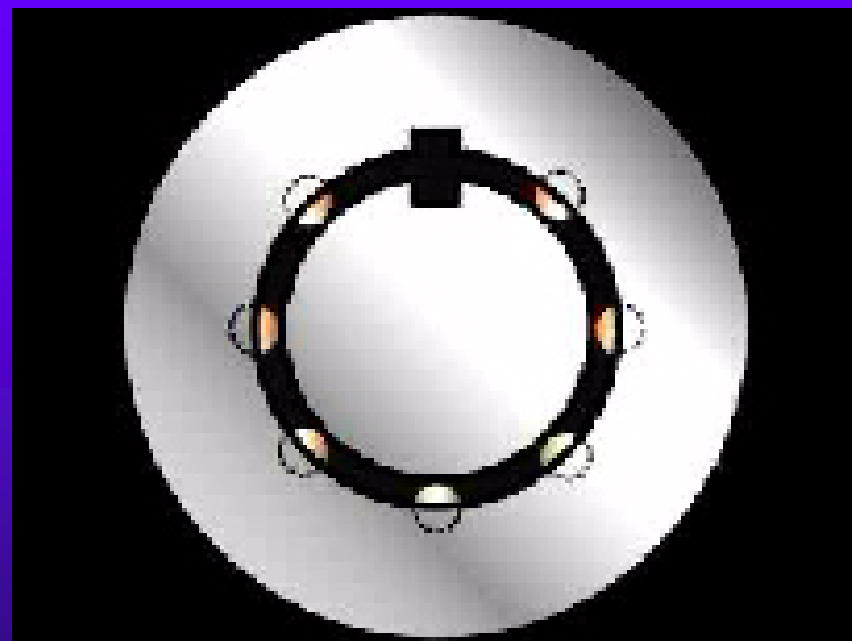


# HYBRID LOCKS

- ◆ Dimple
- ◆ Axial pin tumbler
- ◆ Magnetic
- ◆ Rotating disk
- ◆ Split sidebar
- ◆ Laser track
- ◆ Rotating pin and sidebar: Medeco
- ◆ Finger pins: Assa and Schlage Primus



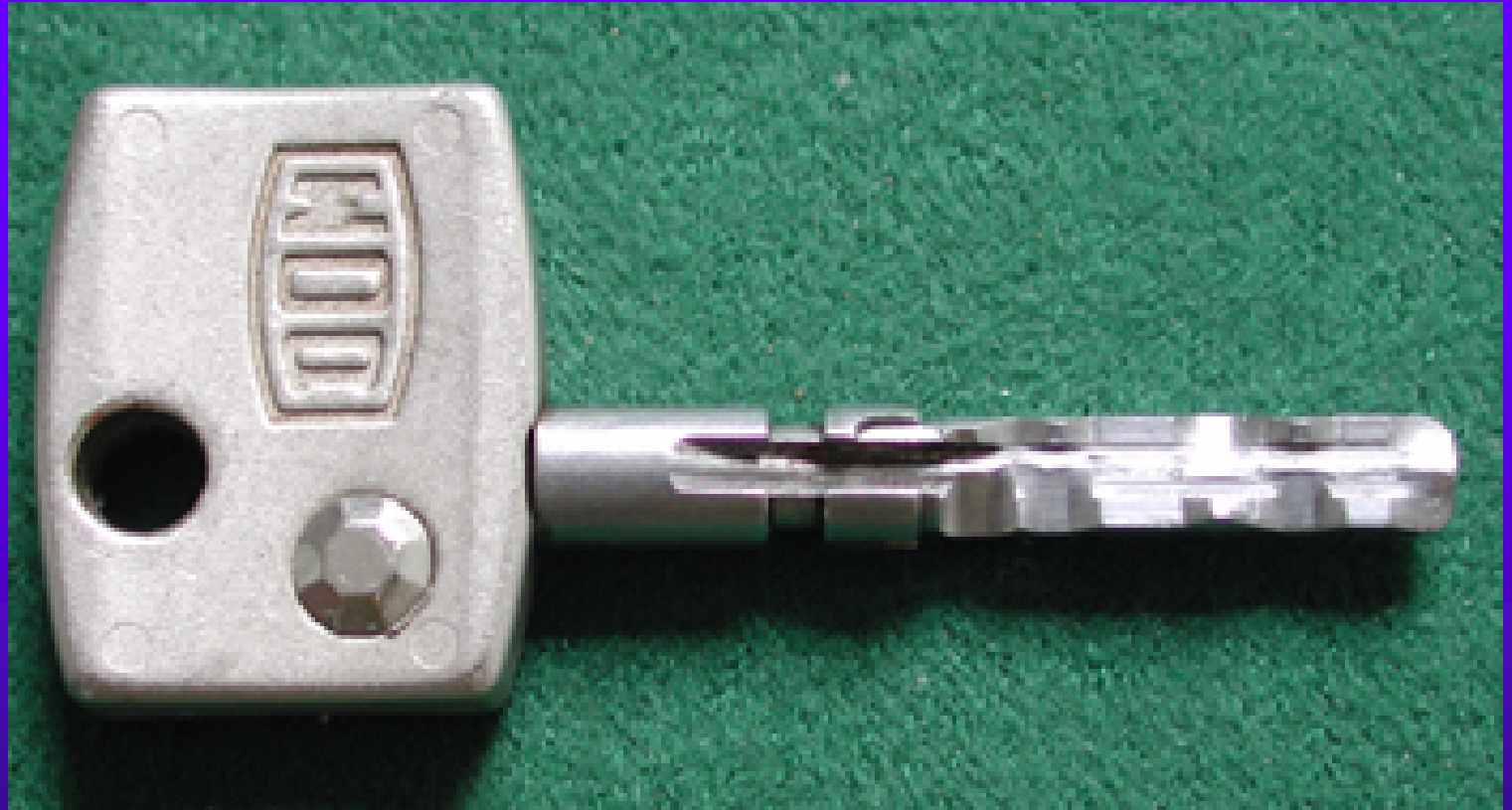
# Axial Pin Tumbler



# EVVA Lasertrack 3KS



# DOM Diamond



# MEDECO Biaxial and Original

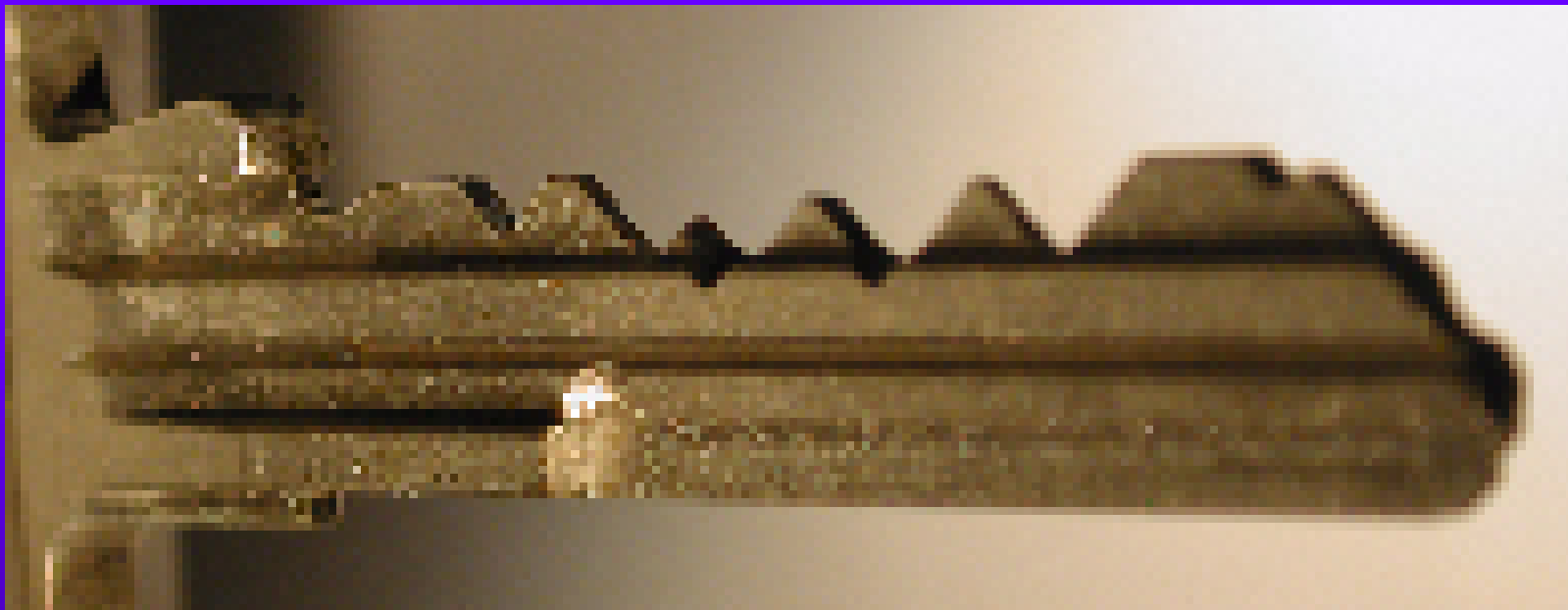
## COMPARISON OF MEDECO ORIGINAL AND BIAxIAL DESIGNS

BIAXIAL  
ORIGINAL

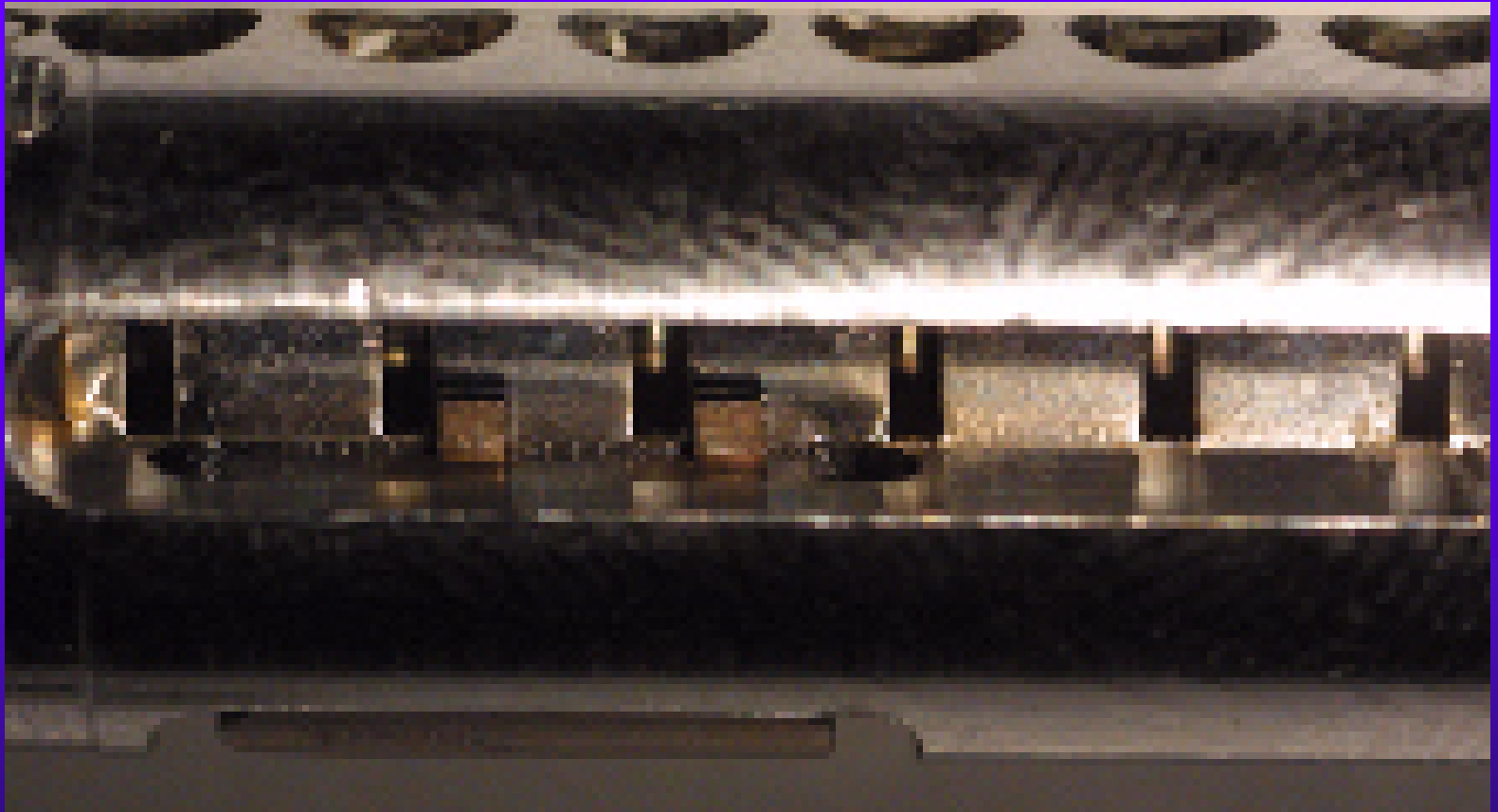




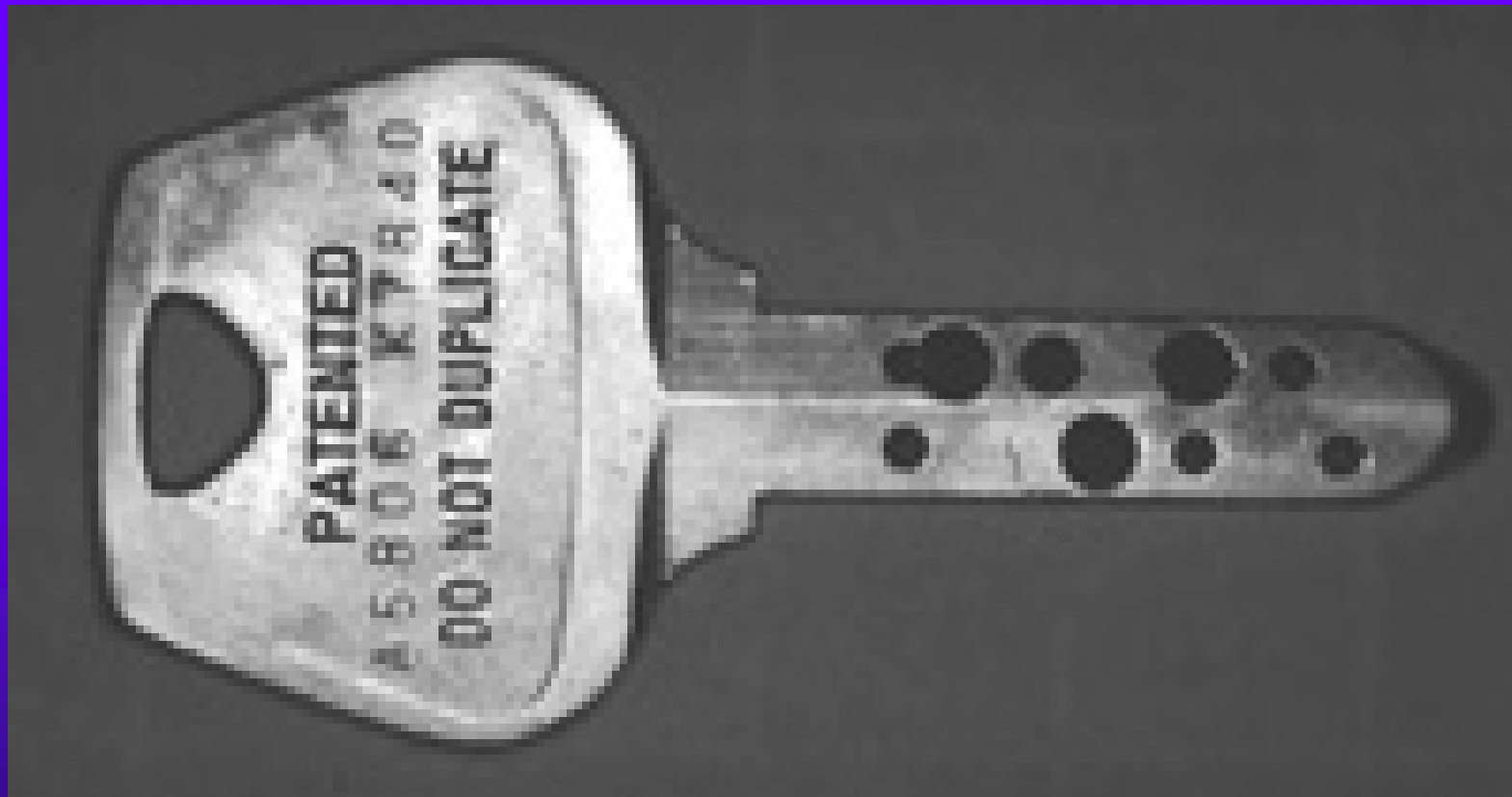
# MEDECO M3



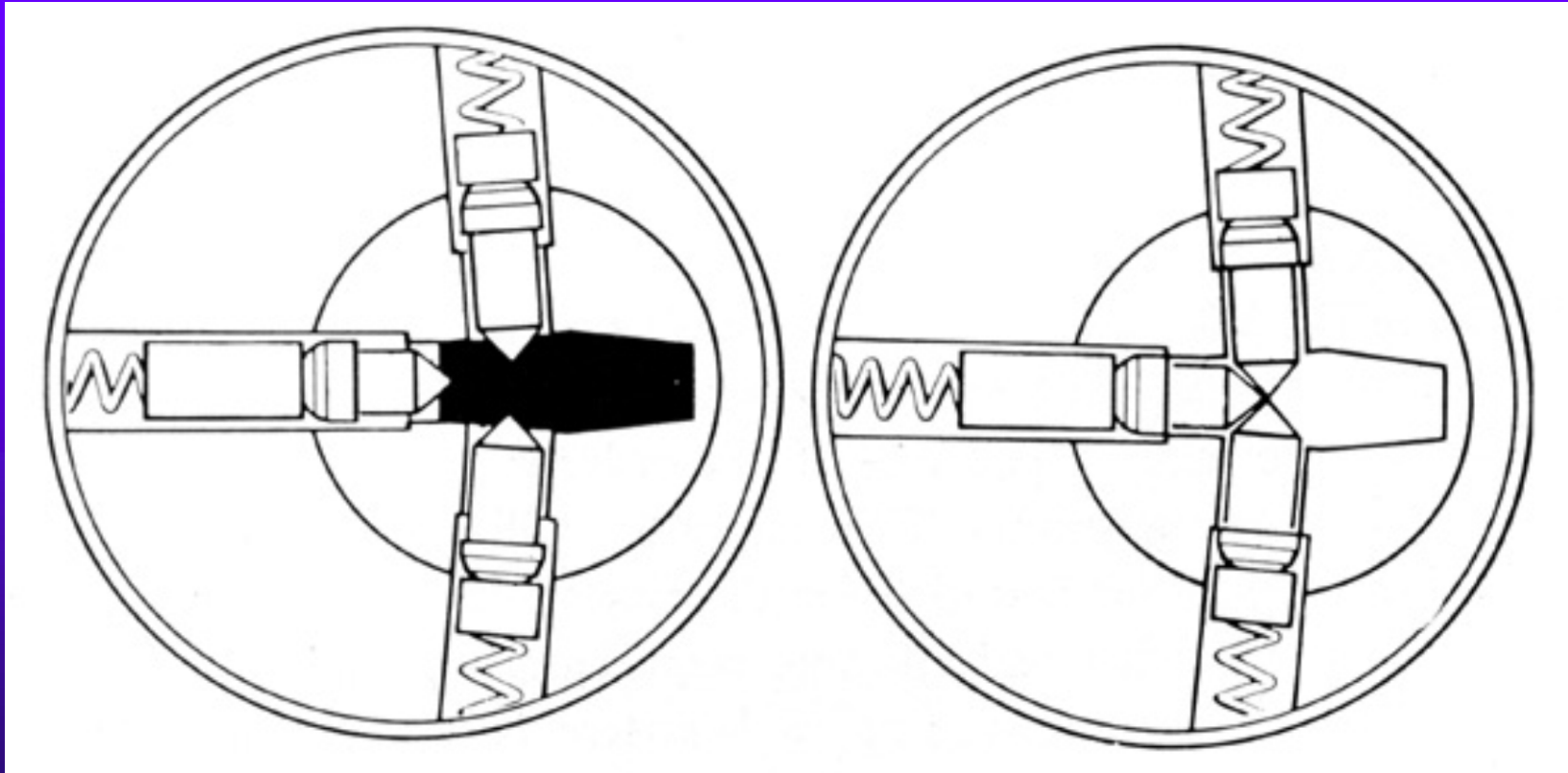
# M3 SLIDER GATES



# Sargent Keso dimple key

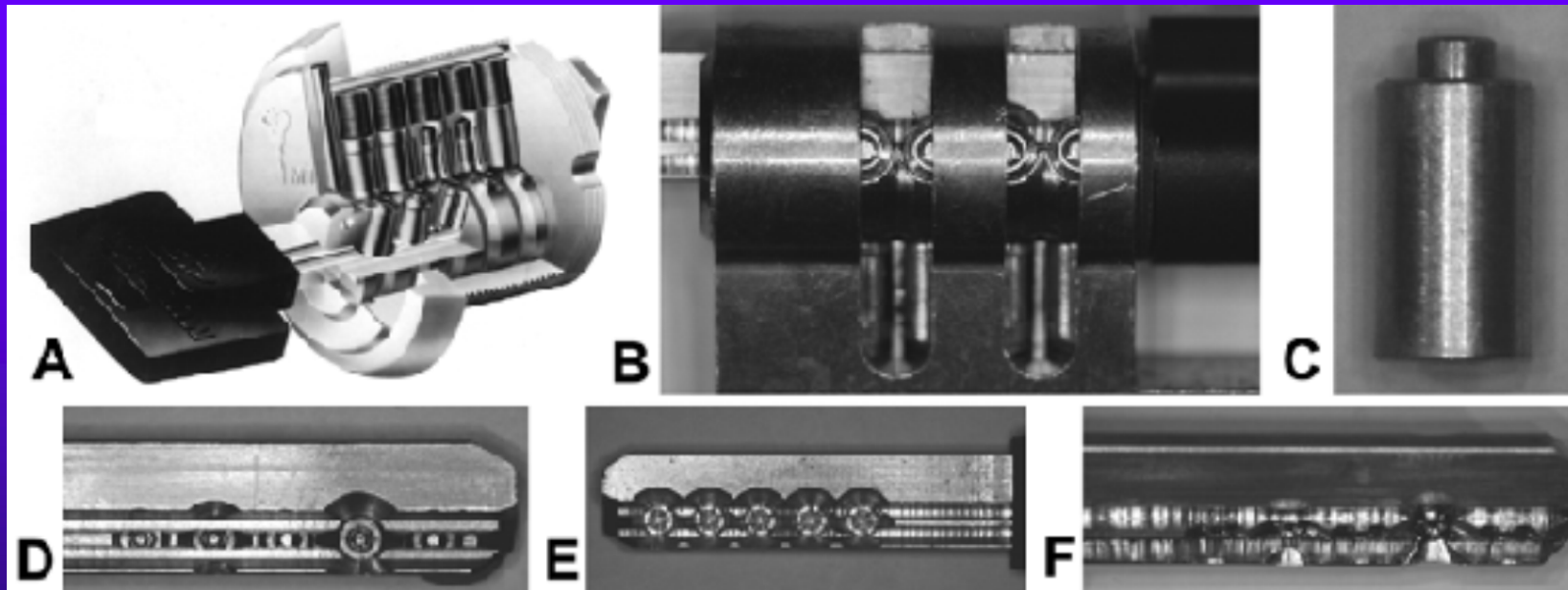


# DIMPLE LOCK PIN DETAIL

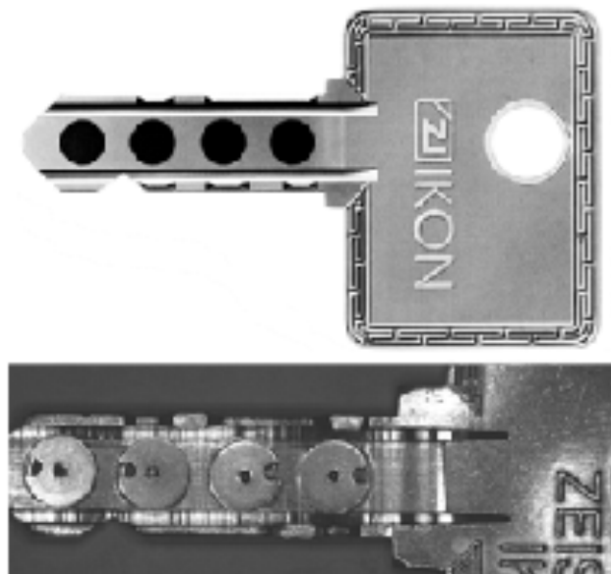
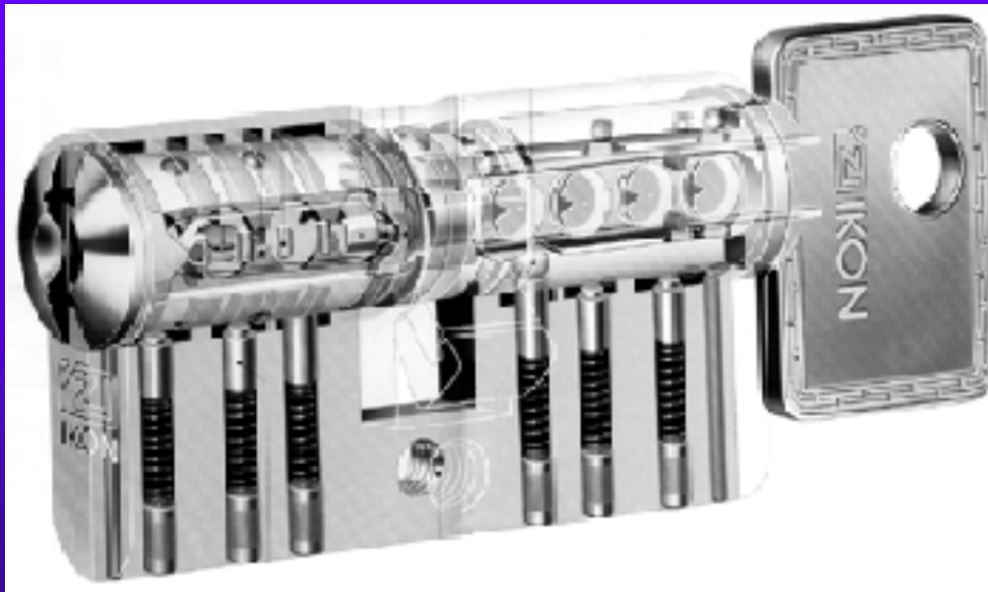




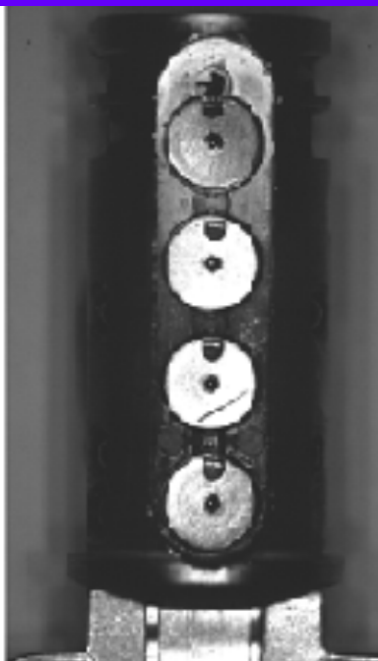
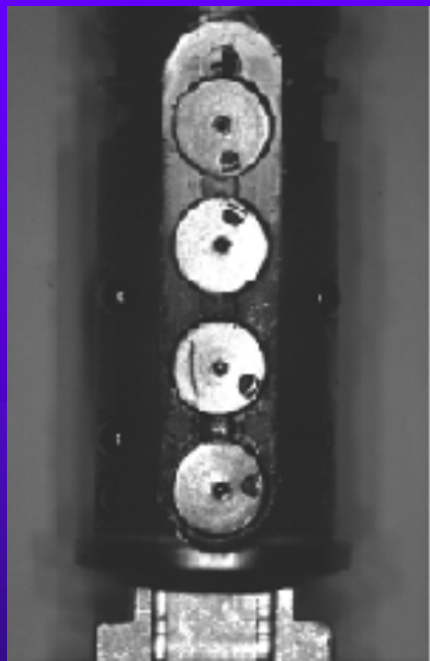
# MUL-T-LOCK DIMPLE



# MAGNETIC SIDEBAR



# IKON Magnetic Detail

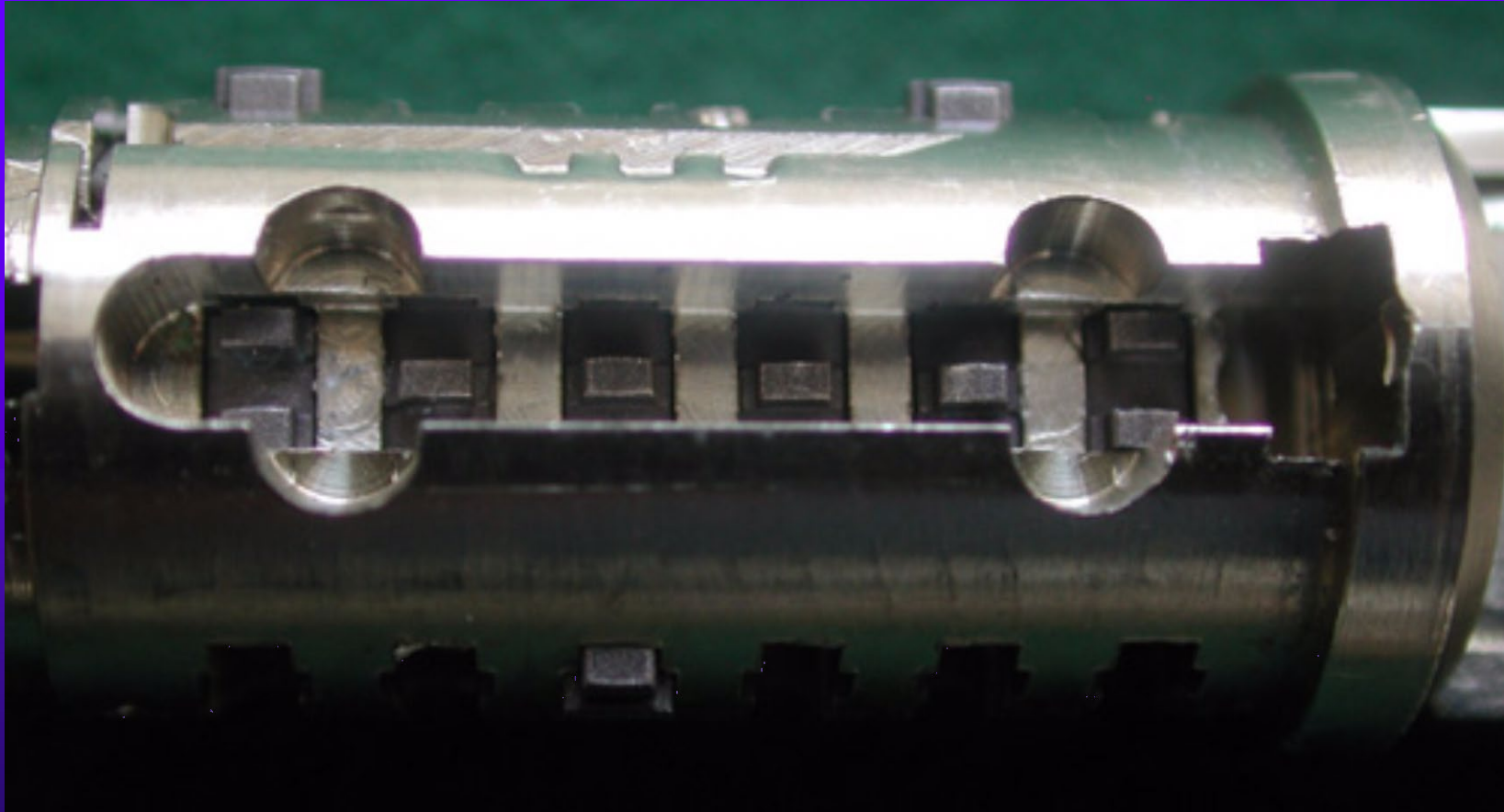


# LASER TRACK – EVVA 3KS

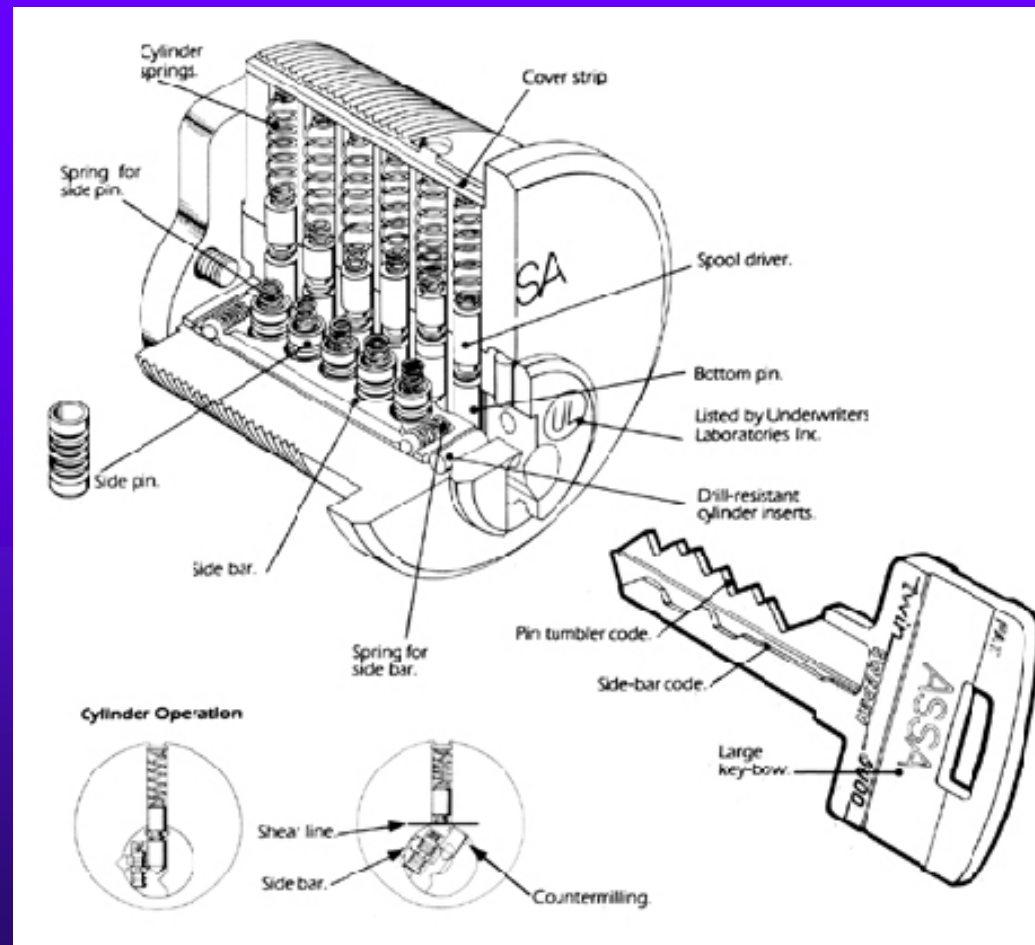




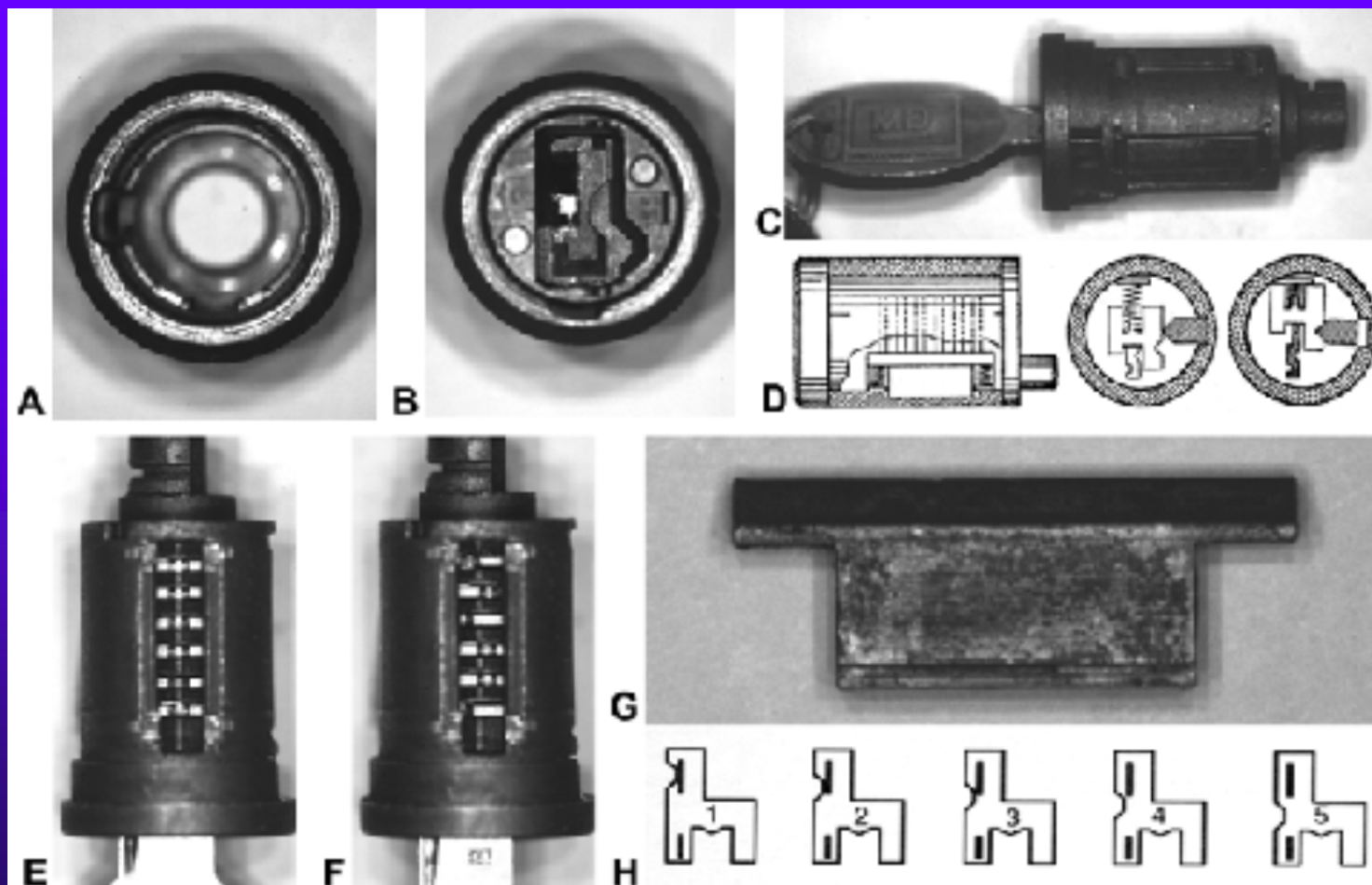
# 3KS Sidebar Locking Principle



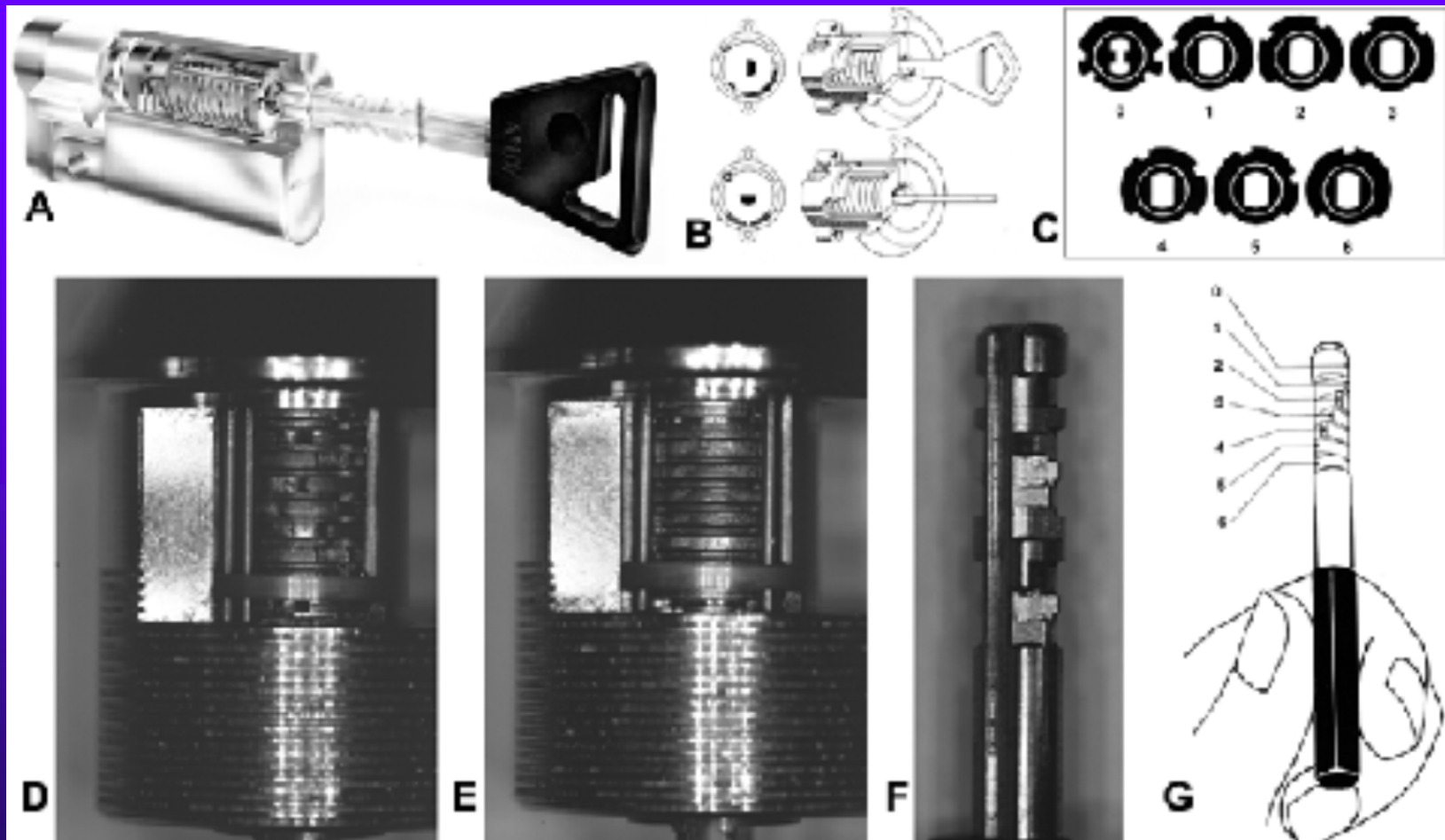
# ASSA SIDEBAR



# G M SIDEBAR



# ABLOY ROTATING DISK

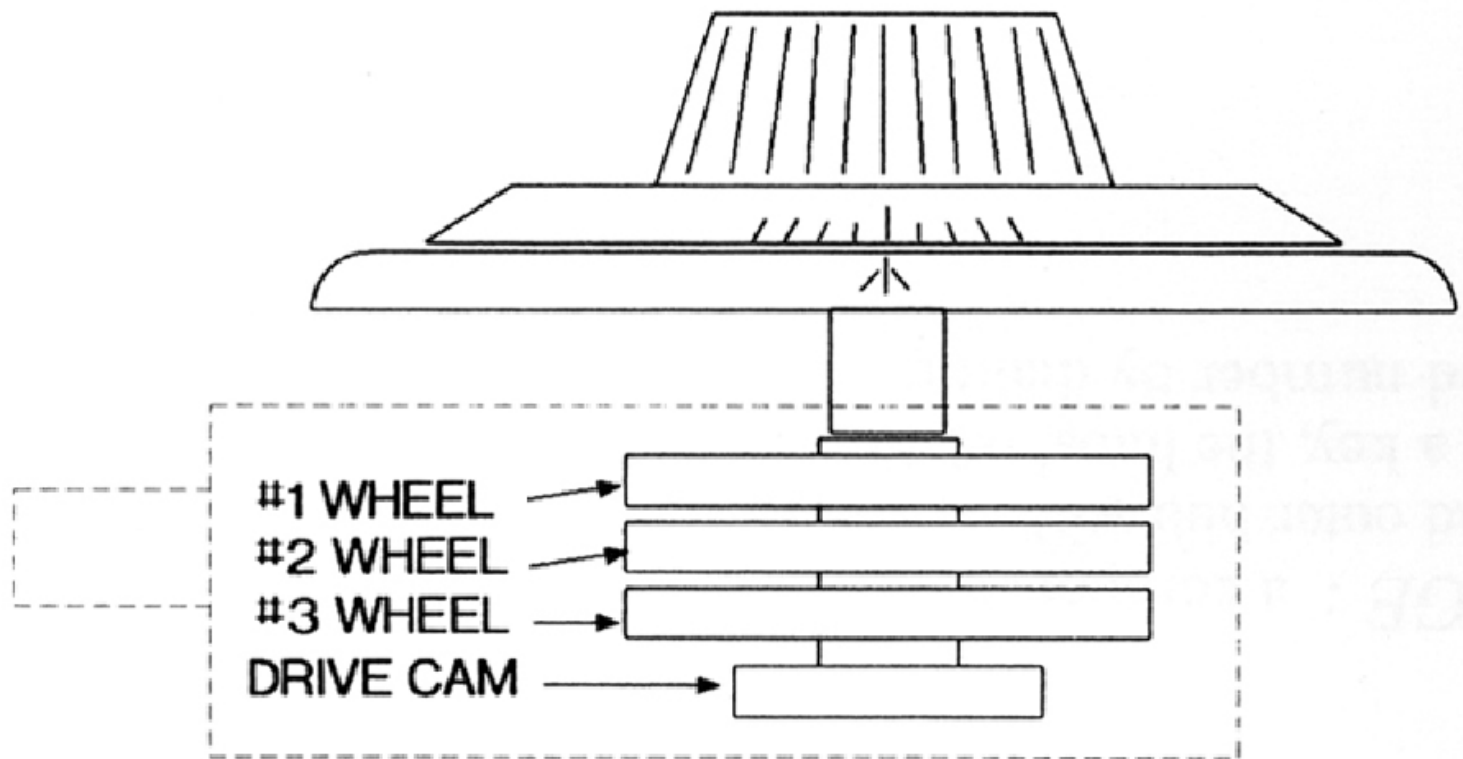




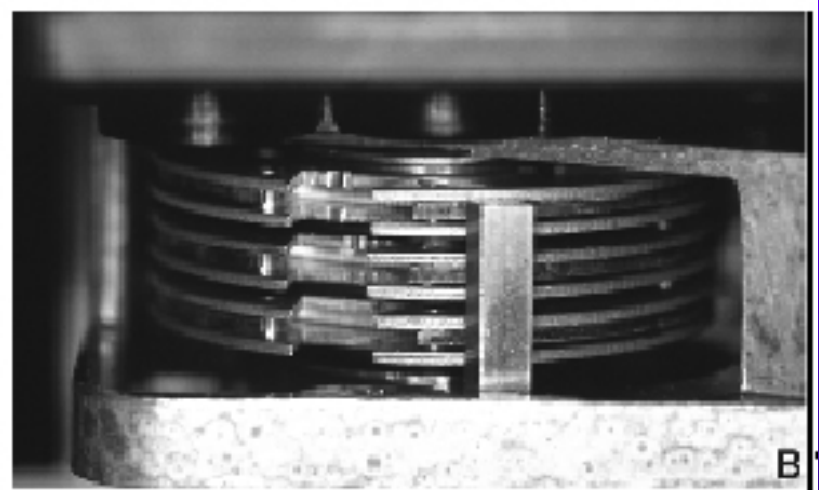
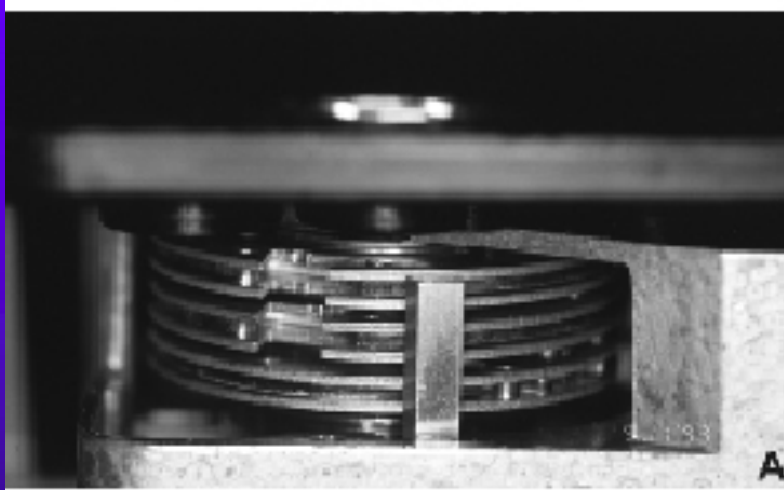
# COMBINATION LOCKS



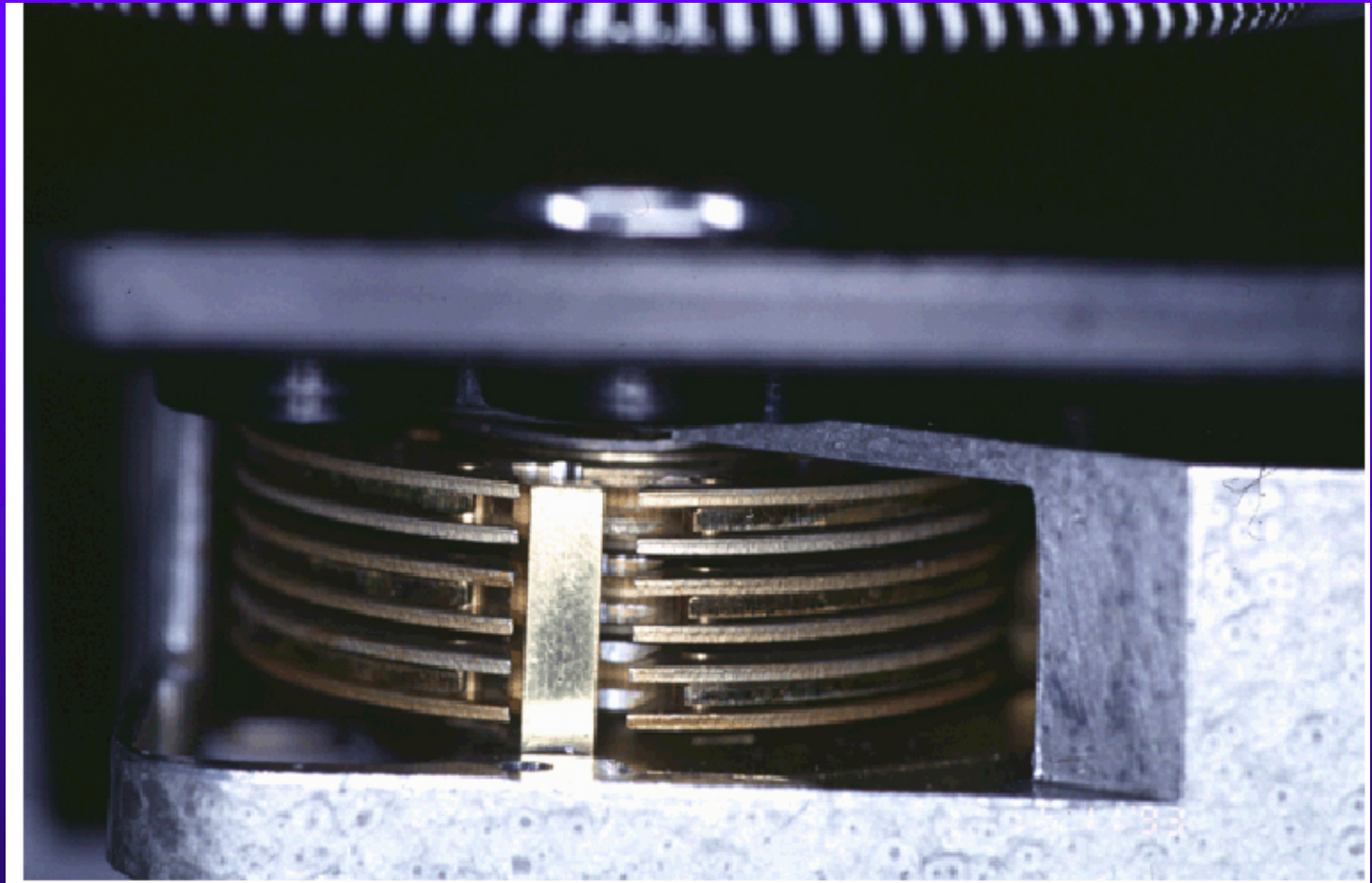
# COMBINATION LOCKS: MODERN DESIGN



# COMBINATION LOCK: WHEEL PACK ALIGNED

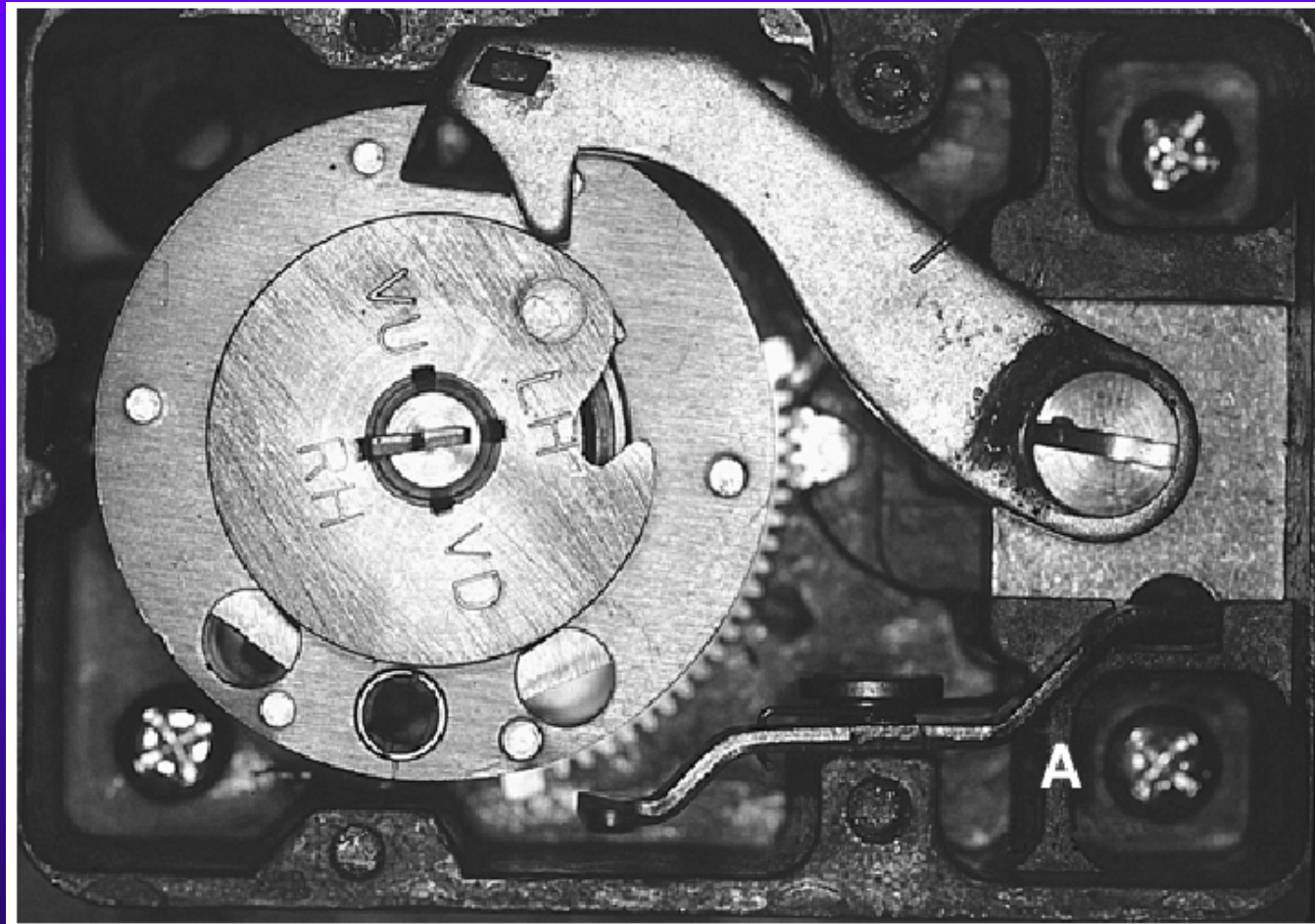


# COMBINATION LOCK





# COMBINATION LOCK: RETRACTING BOLT





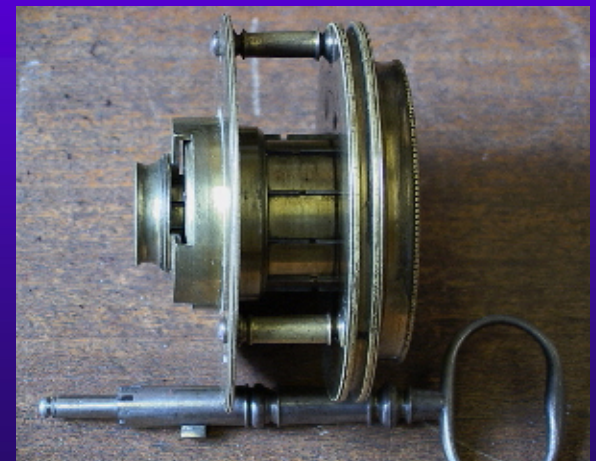
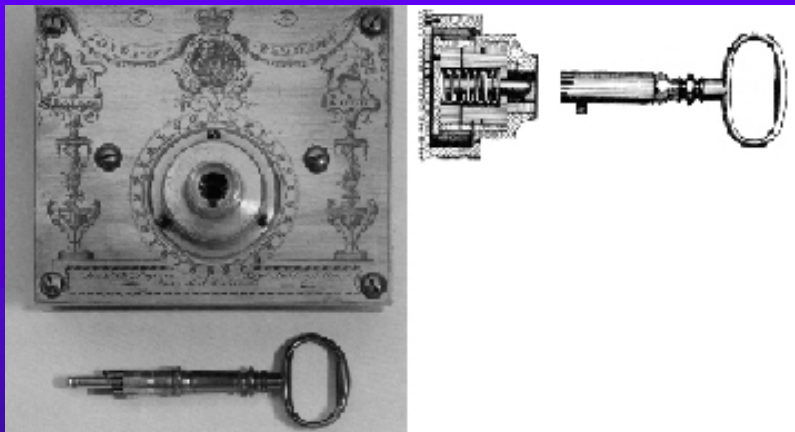
# BYPASS OF LOCKS

# BRAMAH: 124 PICADILLY, LONDON

- ◆ 1851: The Great  
Exposition in London

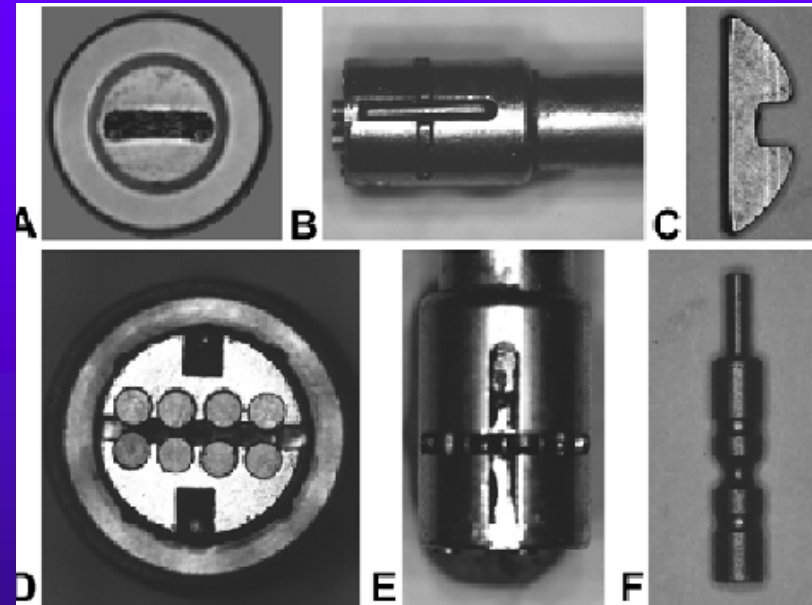
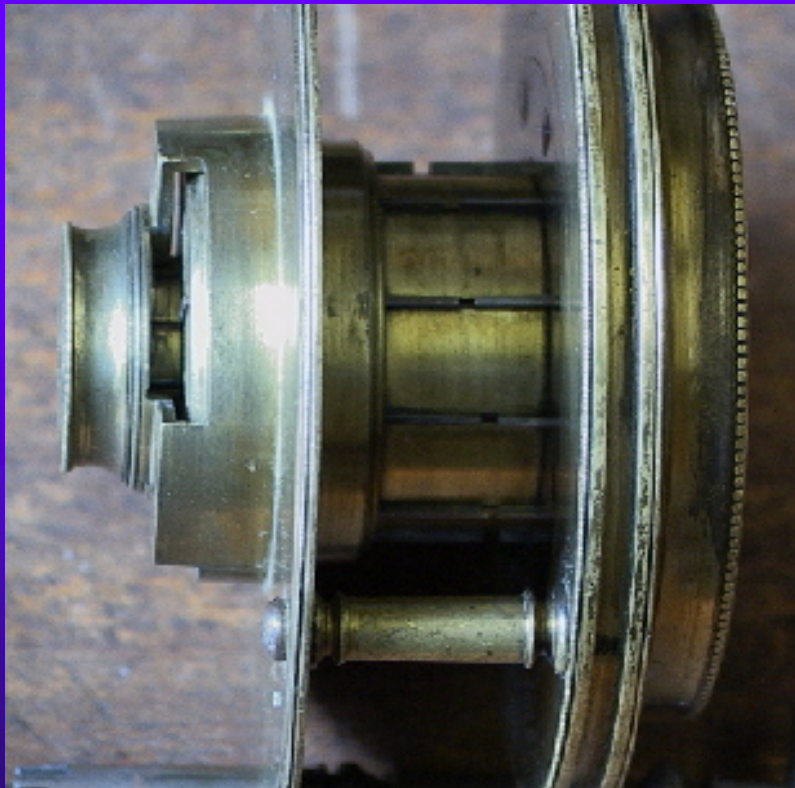


# BRAMAH LOCK COMPANY





# BRAMAH LOCK DETAIL and CHICAGO TUBAR DESIGN





# BYPASS OF LOCKS

- ◆ Many methods
- ◆ Sophisticated and simple
- ◆ Often Manufacturers do not know of techniques
- ◆ Low to high skill
- ◆ Never say Never!



# Threats Against Locks


- ◆ Exhaustive search of key space
- ◆ Brute force
- ◆ Manipulation (picking)
- ◆ Decoding
- ◆ Bypass



# How Secure are Locks Against Exhaustive search for the Key

- ◆ Two parameters
  - $P$ , the number of pin stacks
    - typically between 4 and 7
  - $H$ , the number of different heights used for cuts
    - typically between 4 and 10
- ◆ Number of keys is therefore at most  $H^P$
- ◆ Six Pin lock, 10 depths =  $10^6$ 
  - Sometimes can't have a high cut right next to low cut
    - “Maximum Adjacent Cut Specification” (MACS)
  - Typical lock has between 240 and  $10^7$  distinct keys





# PRIMARY BYPASS TECHNIQUES

- ◆ Picking
- ◆ Decoding
- ◆ Impressioning
- ◆ Brute force attack
- ◆ Mechanical bypass



# MECHANICAL BYPASS

- ◆ Rapping
- ◆ Bump key
- ◆ Comb picking
- ◆ Vibration
- ◆ RF Energy
- ◆ Magnetics
- ◆ Manufacturing standards, i.e. sidebar code



# MECHANICAL BYPASS

- ◆ Shimming
- ◆ Wires and probes
- ◆ Straight wires
- ◆ Retainer attacks



# How secure are locks against brute force attacks?

- ◆ In physical security, brute force does not refer to exhaustive search of the key space...
- ◆ Usually, even a really cheap lock will be one of the strongest parts of the system
  - doors are made of wood, sheet metal, etc
  - windows are made of glass
  - walls are made of drywall
- ◆ Disadvantage: leaves evidence and is noisy
  - some criminals don't mind this





# Secure Against Manipulation

- ◆ Maybe you don't really need a key
- ◆ Several techniques:
  - Lock picking
    - pin-by-pin, impact guns, bump keys
  - Decoding
    - impressioning and other techniques
  - Direct bypass of locking mechanism
    - ...and more



# Lock Picking

- ◆ In a perfect lock, all of the pin holes in the shell line up exactly with holes in the plug
  - so when you turn the plug with no key inserted, all of the pins block rotation exactly equally
- ◆ But real locks aren't perfect
  - in reality, the pin stacks are slightly misaligned
  - one of the pins stacks is the *most* misaligned
  - .001 inches or so of misalignment, typically



# How to Pick Locks

- ◆ Put slight torque on the plug
  - just enough to *bind* the most misaligned pin
- ◆ Gently push up each of the pins until you find the one that resists (that's the most misaligned one)
- ◆ Push that pin up until the cut reaches the shear line
  - plug will turn slightly – you can feel it
  - top pin will be trapped above the shear line as long as torque is applied
- ◆ Repeat with the new most misaligned pin
- ◆ There are special tools for this



# Countermeasures to Picking

- ◆ Try to minimize misalignment
  - this is difficult and expensive
- ◆ Use more pin stacks
  - better locks have 6 or 7; typical locks have just 5
- ◆ Use a narrow keyway with many wards
  - makes it difficult to insert picking tools
- ◆ Use pick-resistant pins
  - Mushroom, spool, serrated
- ◆ Special lock designs (sidebars, rotating pins, etc)





# Decoding or “Reading” the Lock

- ◆ Disassemble lock and measure the pin cut heights
  - but if you can do this, you don’t *need* a key
- ◆ Use a special tool that fits in keyway and probes each pin stack to measure the cut height
- ◆ Impressioning: exploit the fact that pins at the wrong height tend to leave marks on key
  - keep filing at each pin position until marks disappear
  - common technique used by locksmiths



# Mechanical Bypass of Mechanism

- ◆ Sometimes the lock isn't the only way to operate the locking mechanism
  - Credit card or knife can push latch open
  - Tools inserted through keyway can manipulate lock
  - Prying doorframe past deadbolt strike can open door
  - Bent wire pushed under door can turn interior knob
  - Padlock “shims” can retract latch
  - Car “slim-jims” can manipulate lock linkage
- ◆ These techniques work surprisingly often!



# Picking locks and Burglars

- ◆ Good news and bad news
- ◆ Good news: most burglars don't pick locks
  - picking locks can be hard – requires skill and tools
  - brute force or getting a copy of the key are the main attacks used by real criminals
- ◆ Bad news
  - getting a key is often surprisingly easy
  - Information on the Internet
  - Tools on the Internet



# Covert Entry Methods and Burglars

- ◆ High value targets:
  - Locks are picked
  - Keys are impressioned
  - Locks are decoded
  - Master key systems are extrapolated
  - Antwerp: real life example





# BYPASS TECHNIQUES

- ◆ Mechanical Bypass
- ◆ Core Shimming
- ◆ Pin and Cam
- ◆ Pick and form – foil
- ◆ Stack Probing – length of pin stack
- ◆ Sac probing – break points



# More Bypass Techniques

- ◆ Electronic decoding
- ◆ Ultrasonic decoding
- ◆ Plasticine reading
- ◆ Auto impressioning using foil
- ◆ Tryout keys
- ◆ Shim wire decoding
- ◆ Radioscopy
- ◆ Borescope



# More Bypass Techniques

- ◆ Belly Reading
- ◆ Skeleton keys
- ◆ Comb pick
- ◆ Rapping
- ◆ Scratch reading of levers
- ◆ Vibration techniques
- ◆ Auto manipulation of components
- ◆ Combination of techniques



# More Bypass Techniques

- ◆ Rocking with computer picks
- ◆ Pick guns
- ◆ Special pick and decode tools
- ◆ Cross keys
- ◆ Electronic signature analysis
- ◆ TMK Extrapolation
- ◆ Lock bumping

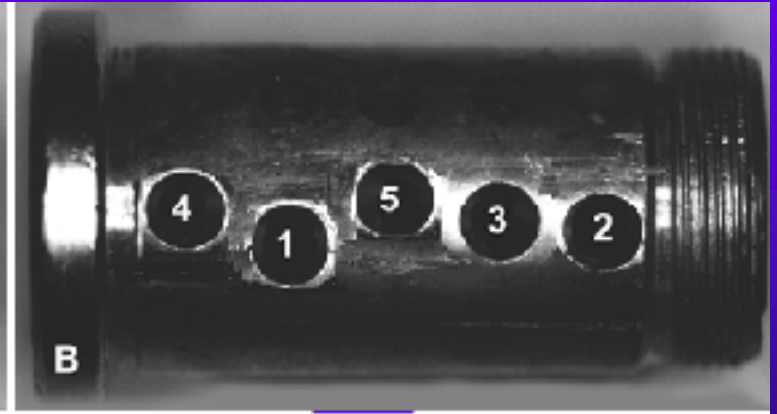
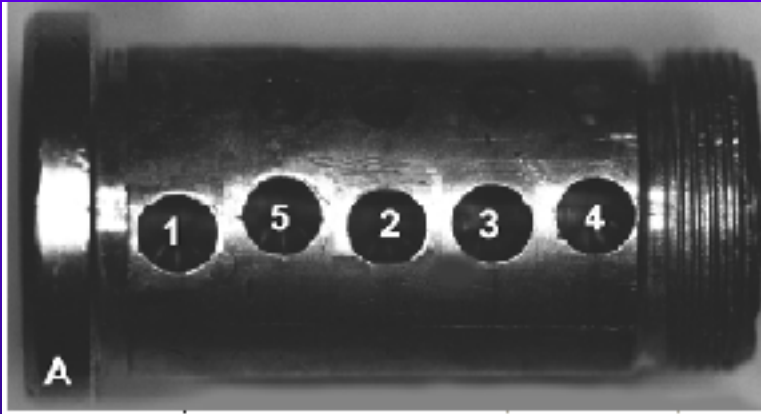




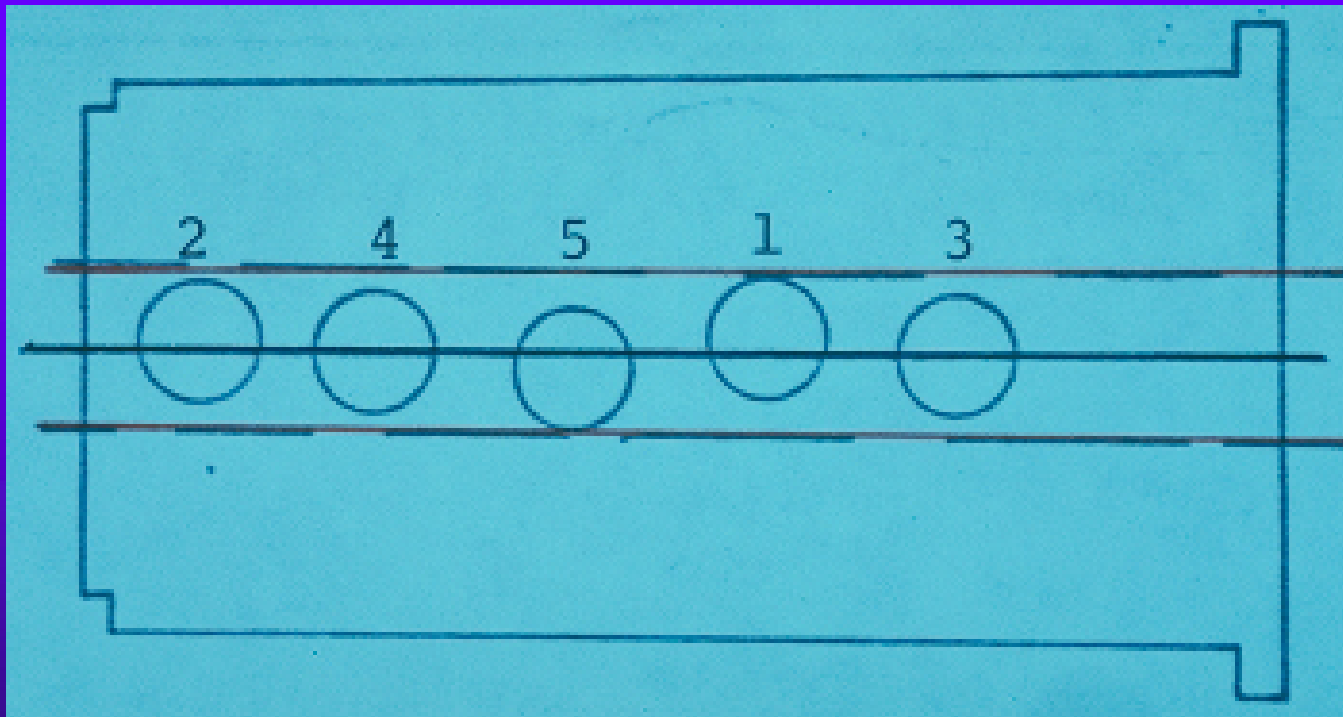
# PICKING PIN TUMBLER LOCKS

# PICKING TOOLS

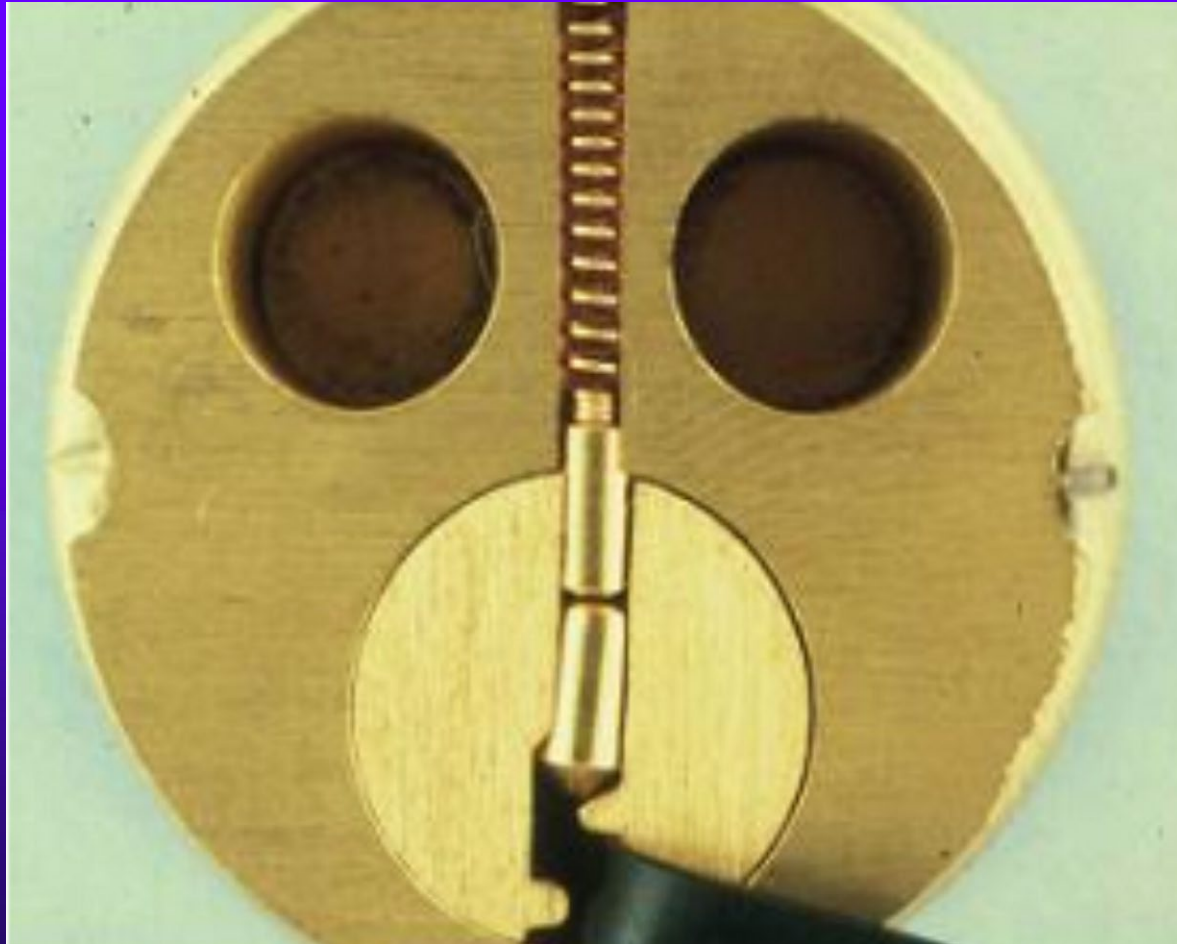
## ◆ What is Picking?



# Order of Picking



# PICKING A CYLINDER APPLY TENSION

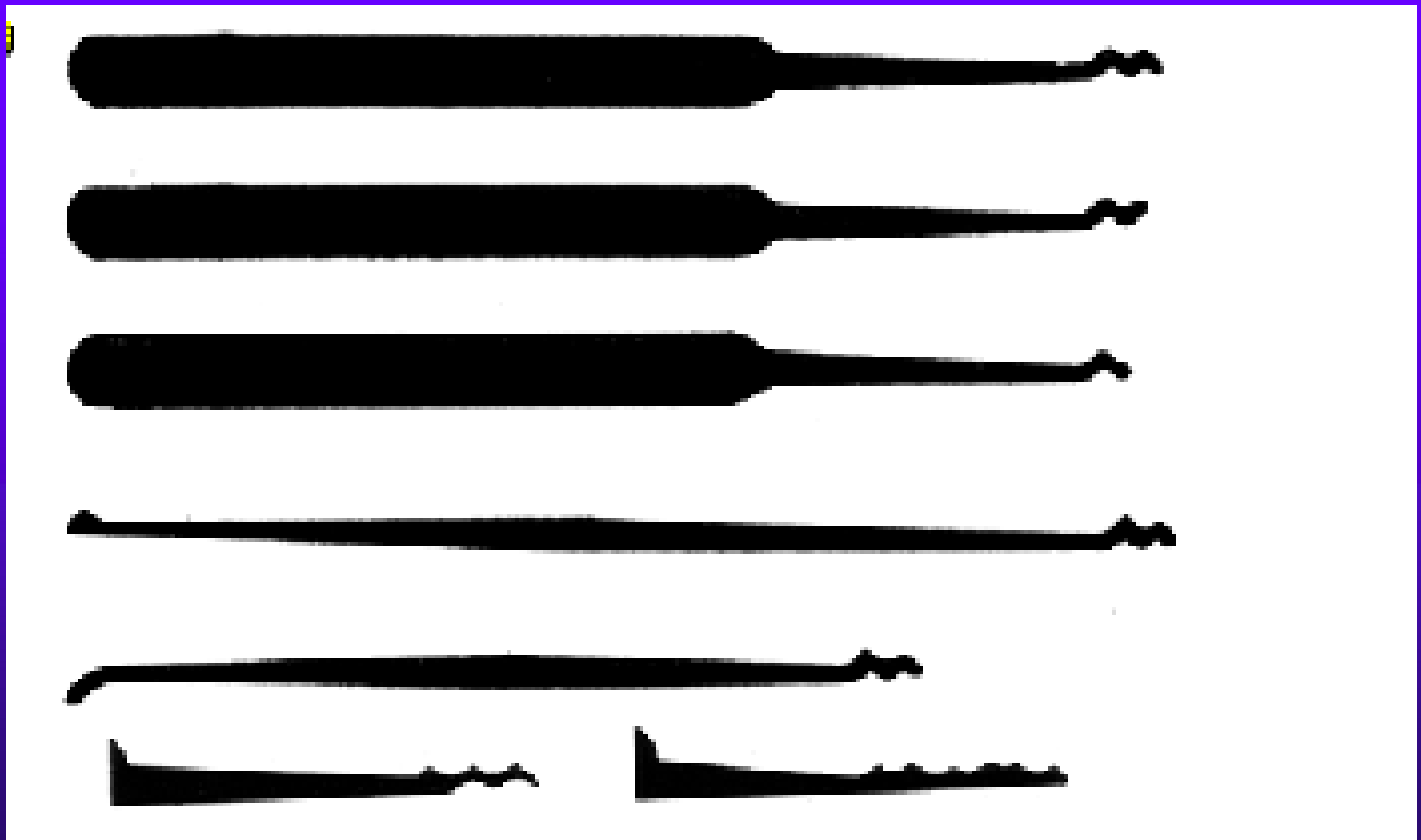


# Move Pins with Pick



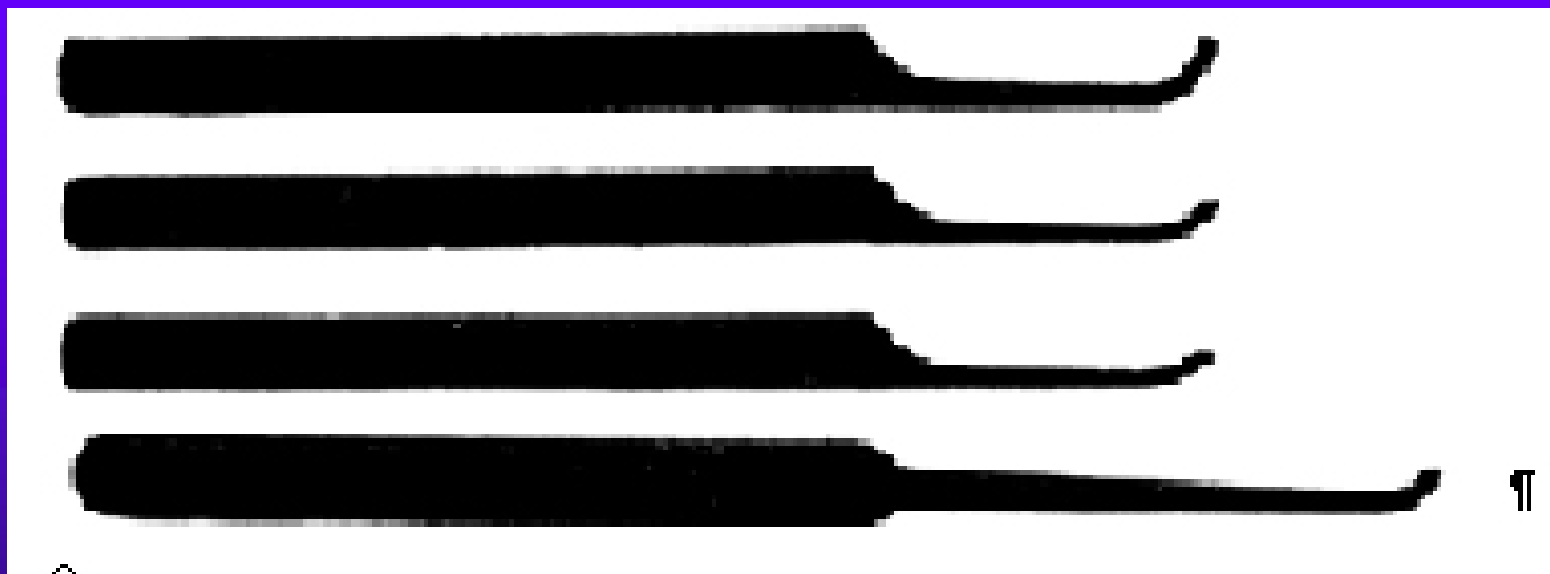


# BASIC PICKS





# More Picks

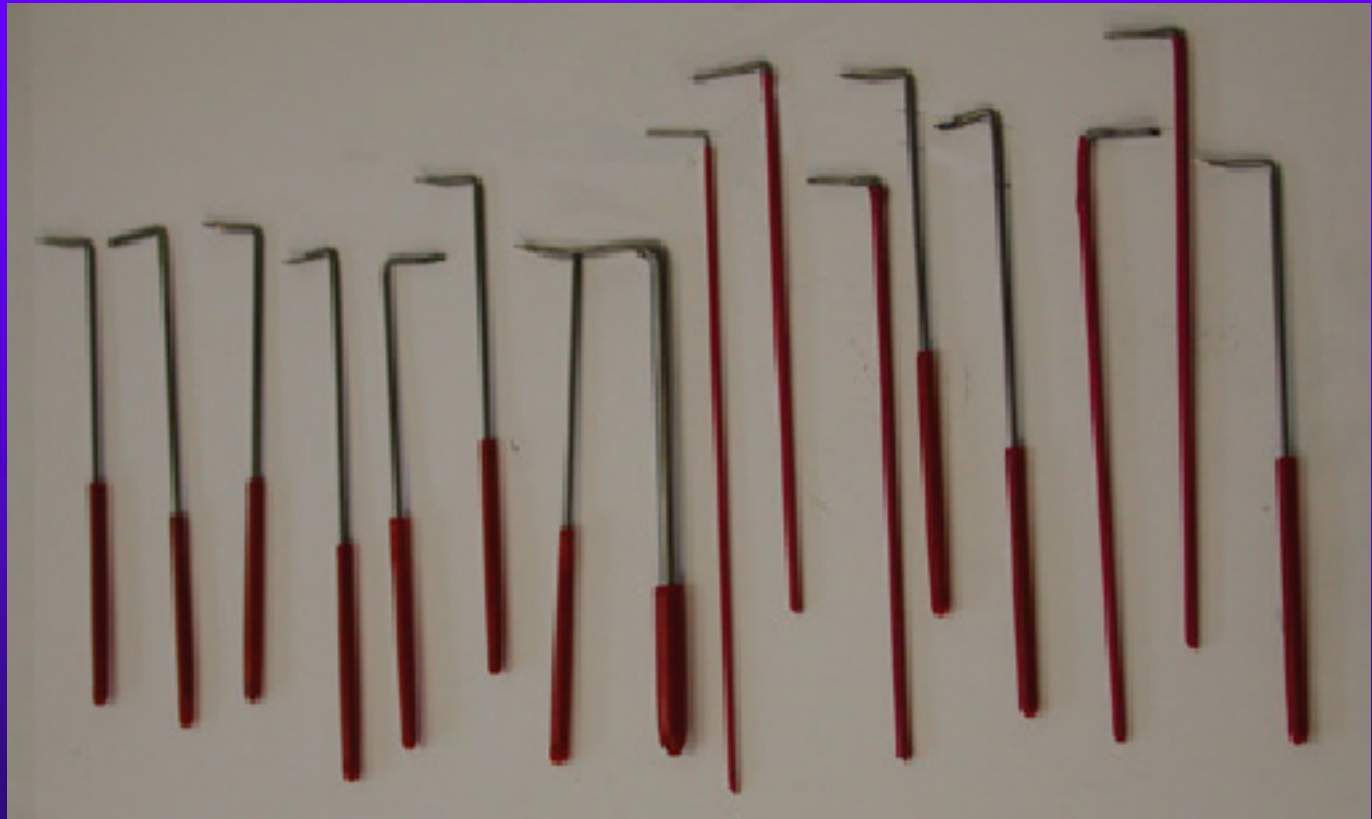


# Pick sets





# Tension wrench

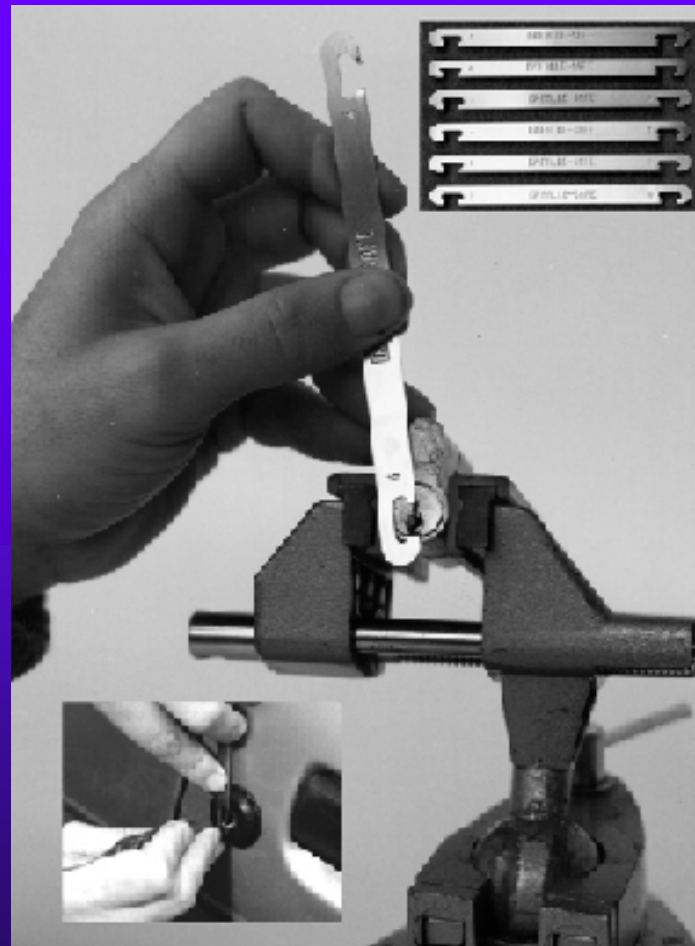


# Tension ring for cylinder



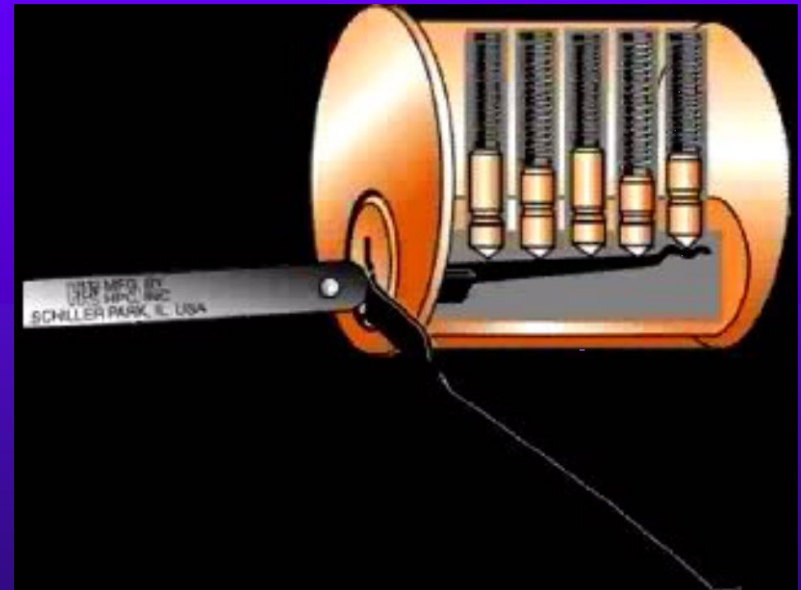
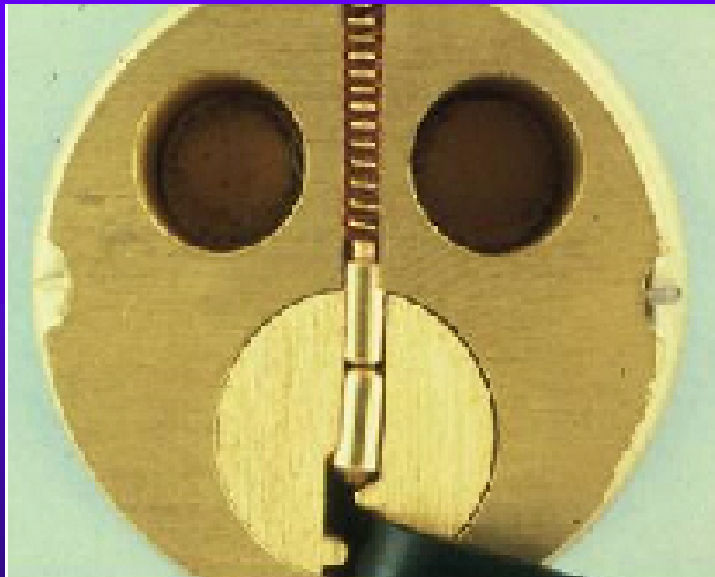


# Falle tension wrenches



# Plug rotation blocked

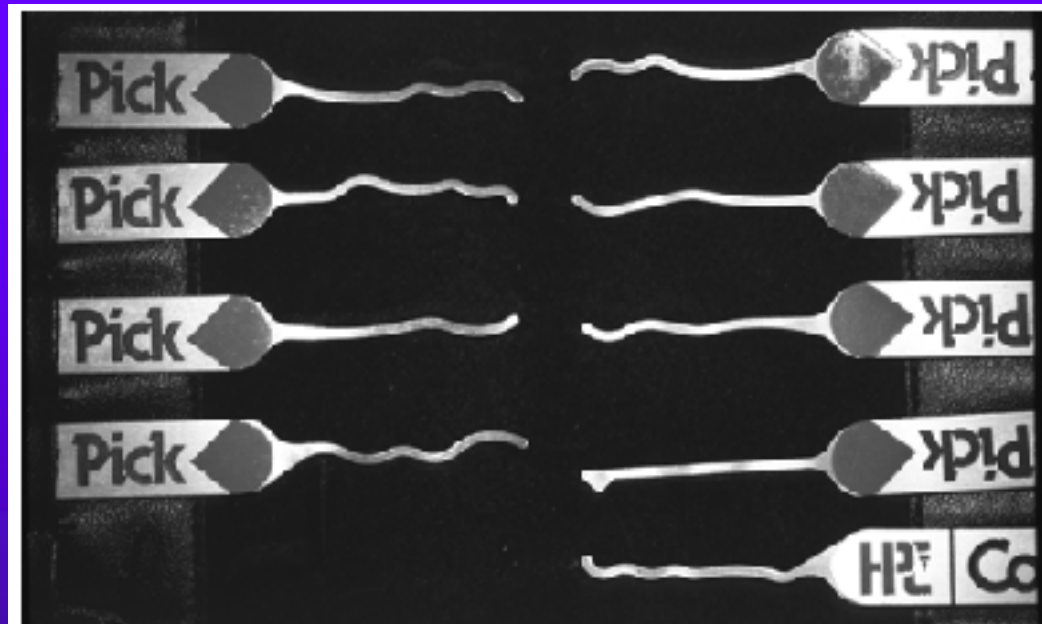
- ◆ Plug cannot turn with tension applied



# PICK SET – PROFESSIONAL

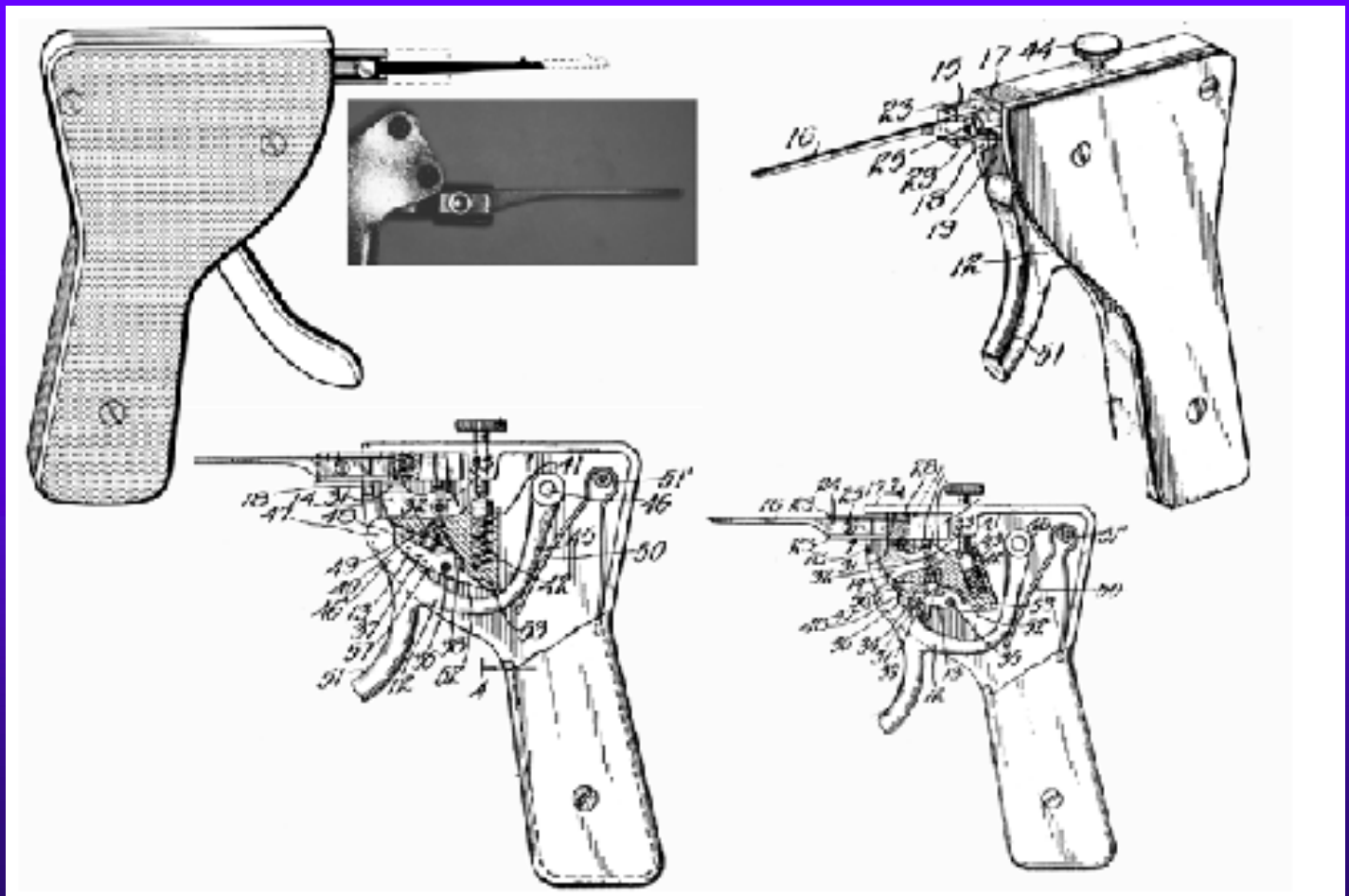


# COMPUTER PICKS



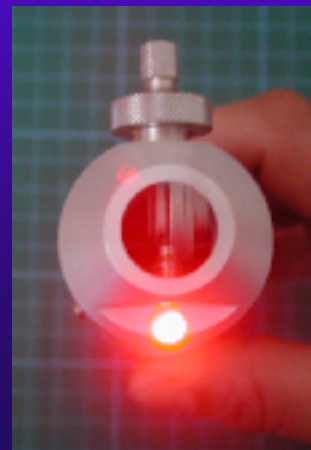
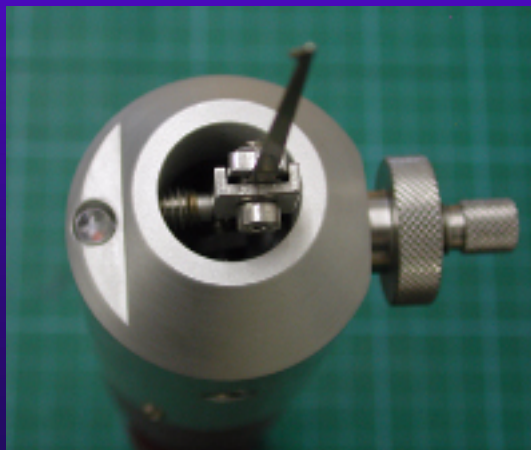
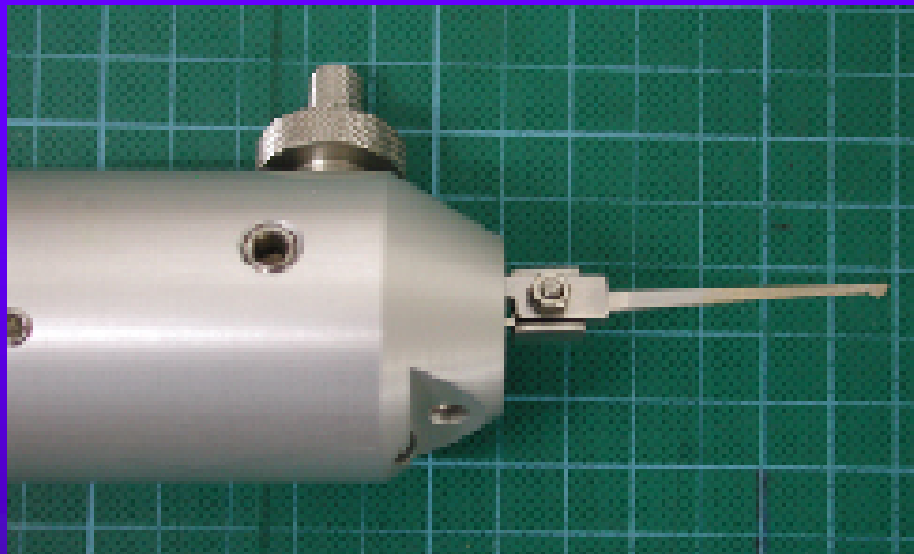


# PICK GUNS





# Vibration pick gun



# Axial lock picks



# Peterson Pro-1 Axial pick



# Acoustic Pick





# 999 Bump Key





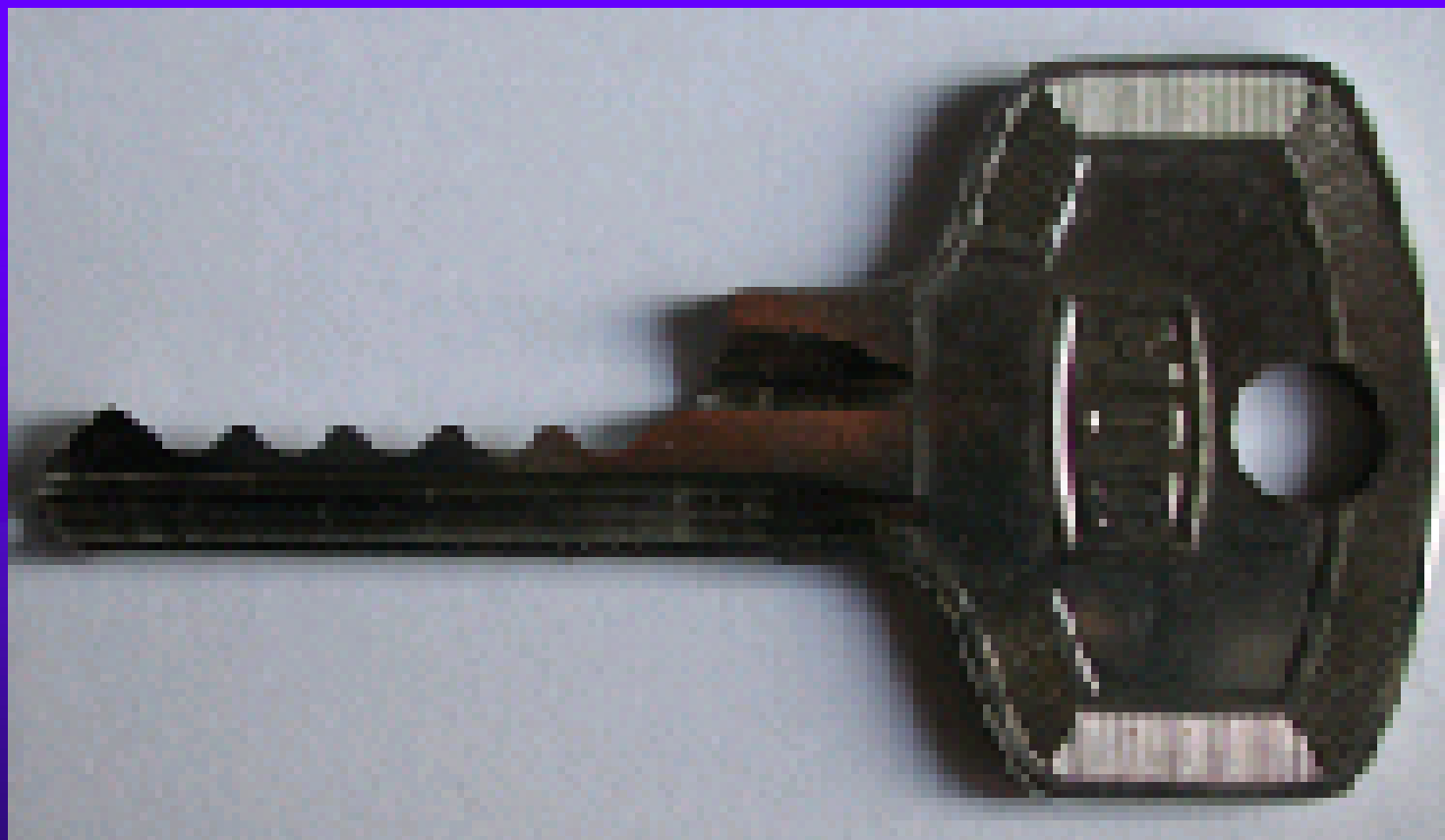
# Bump Keys



# Sidebar Locks



# 999 Key



# Dimple lock



# Dimple Locks

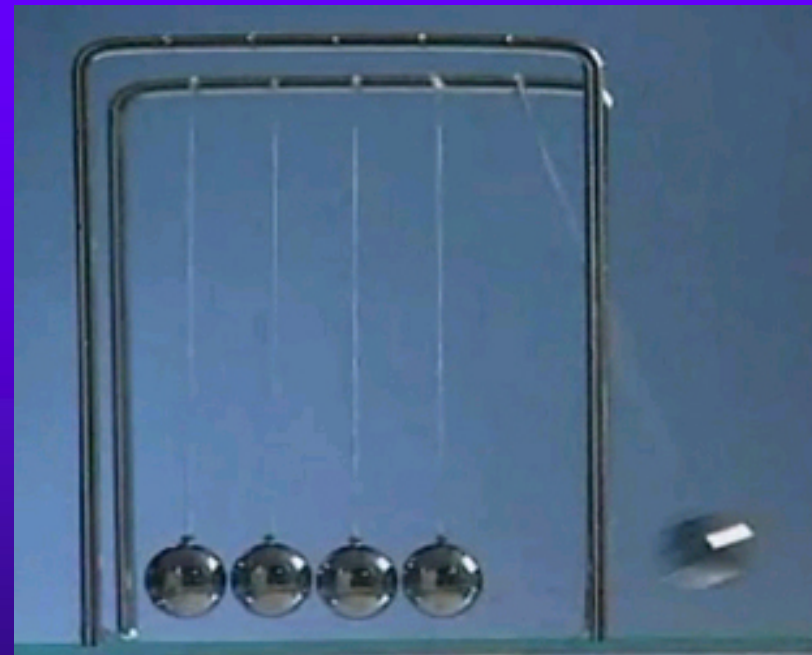
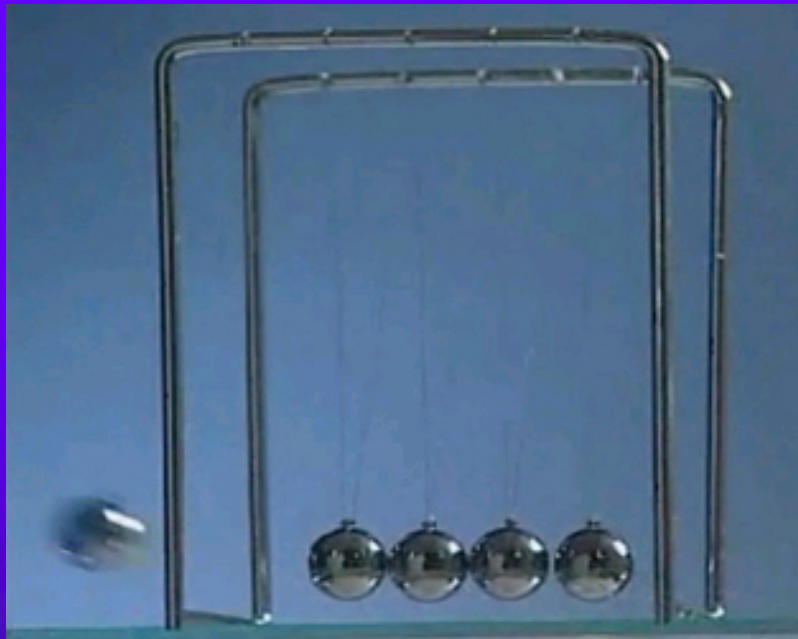




# Axial Pin Tumbler



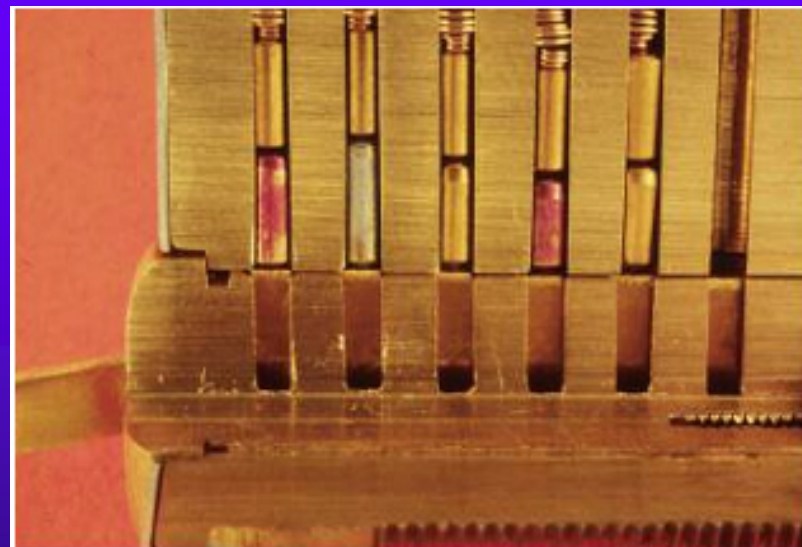
# Bump Key Theory



# Negative Shoulder



# Comb picking

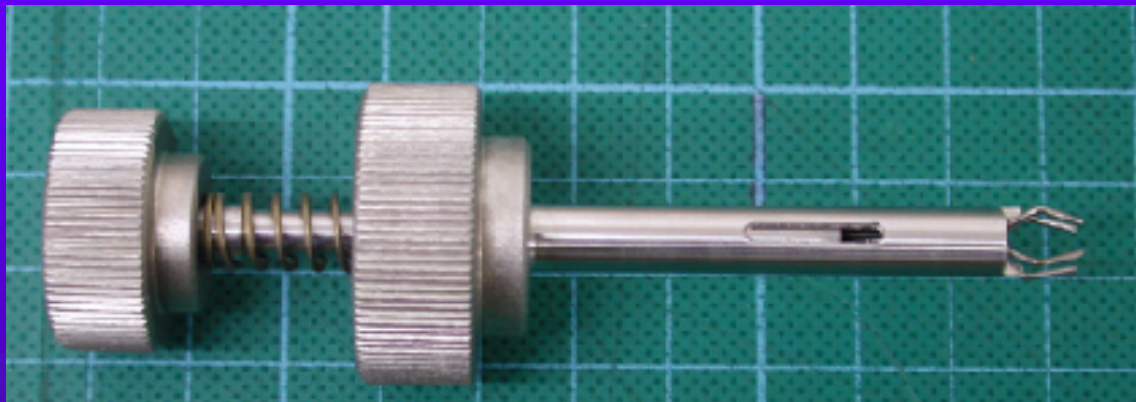


# Comb pick set: Falle

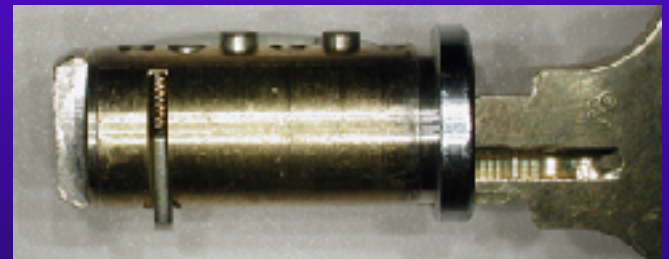
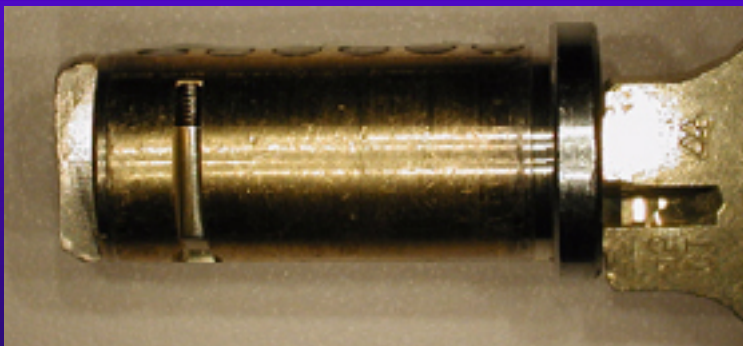




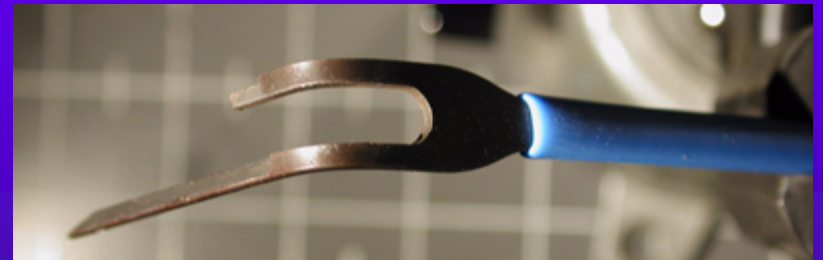
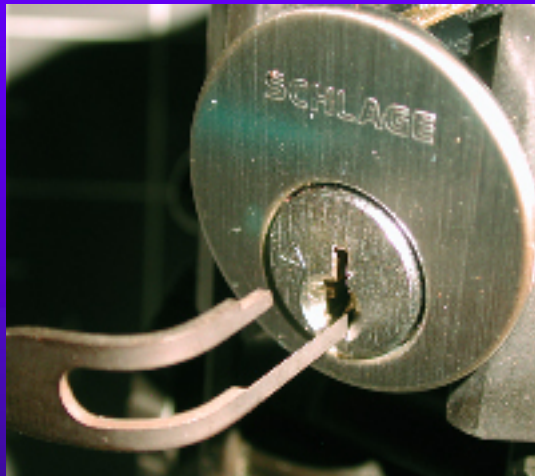
# Cross pick



# Schlage Everest



# Schlage Everest: Picking

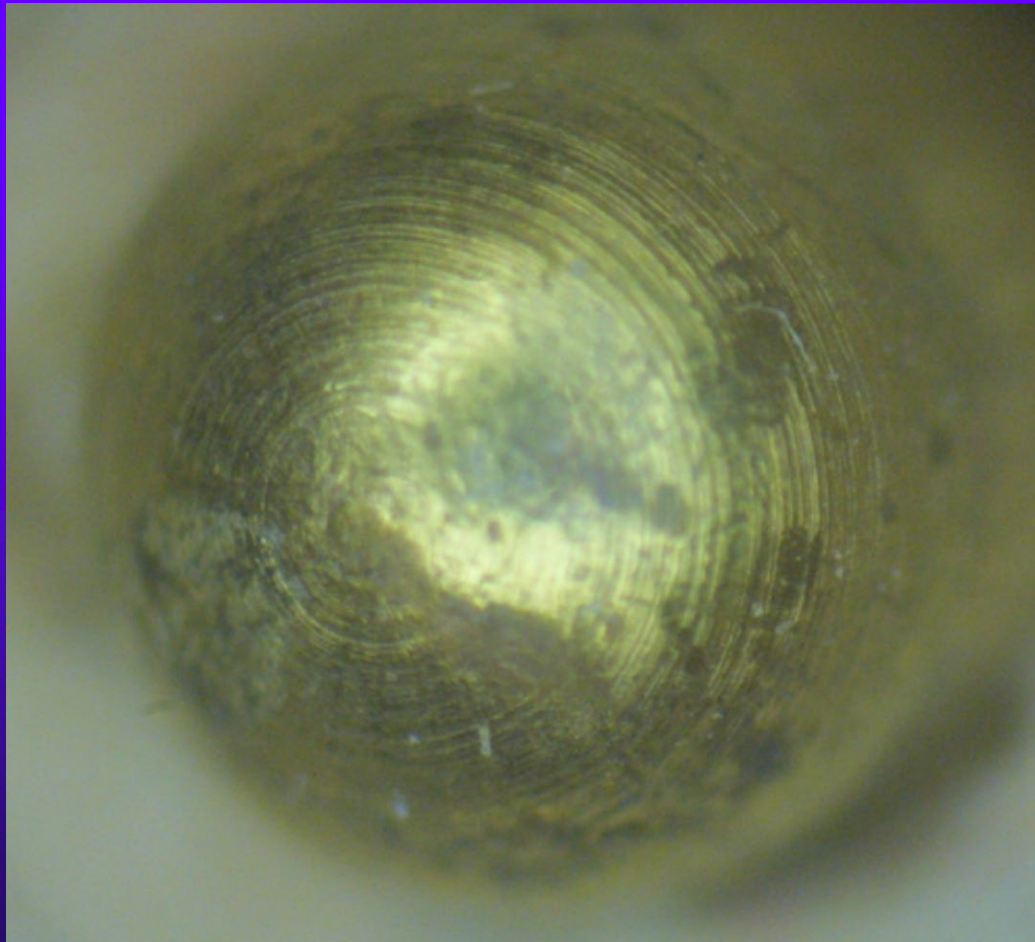




# FORENSICS OF PICKING

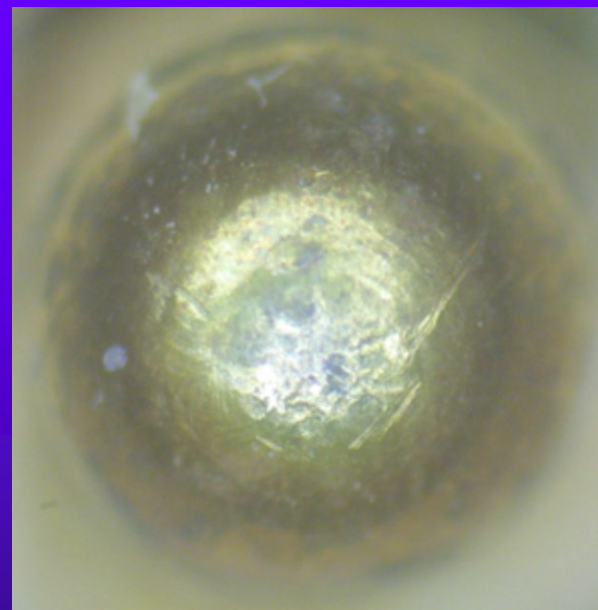
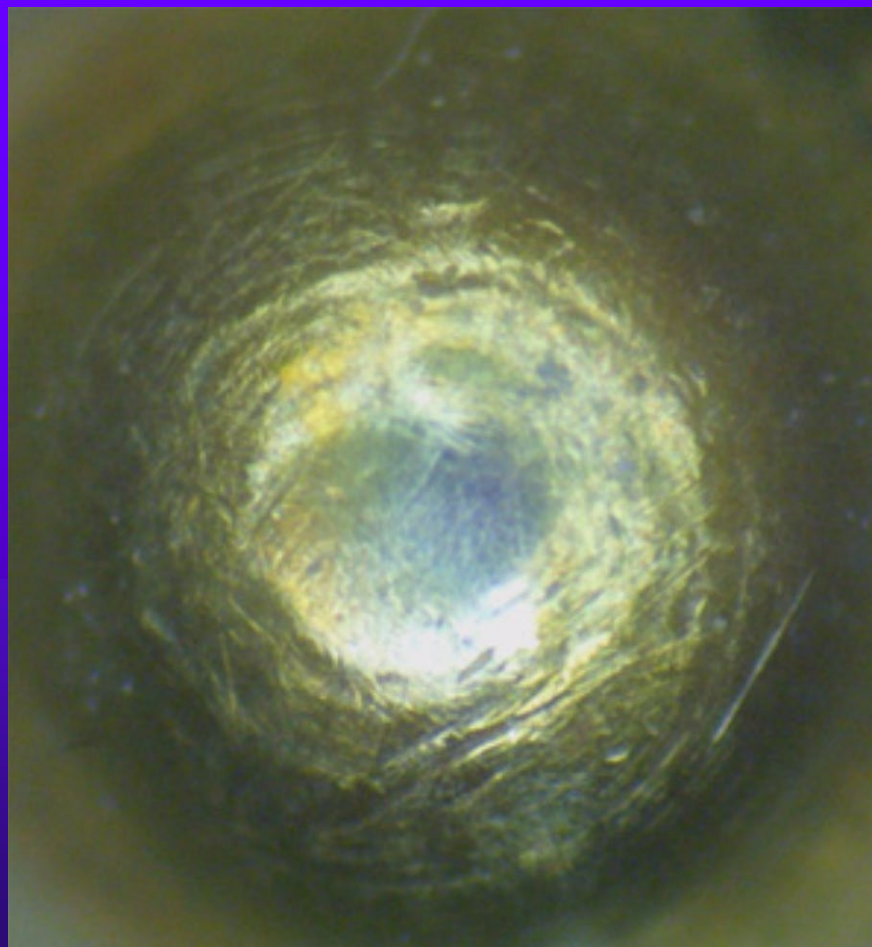


# FORENSIC INDICIA OF BYPASS

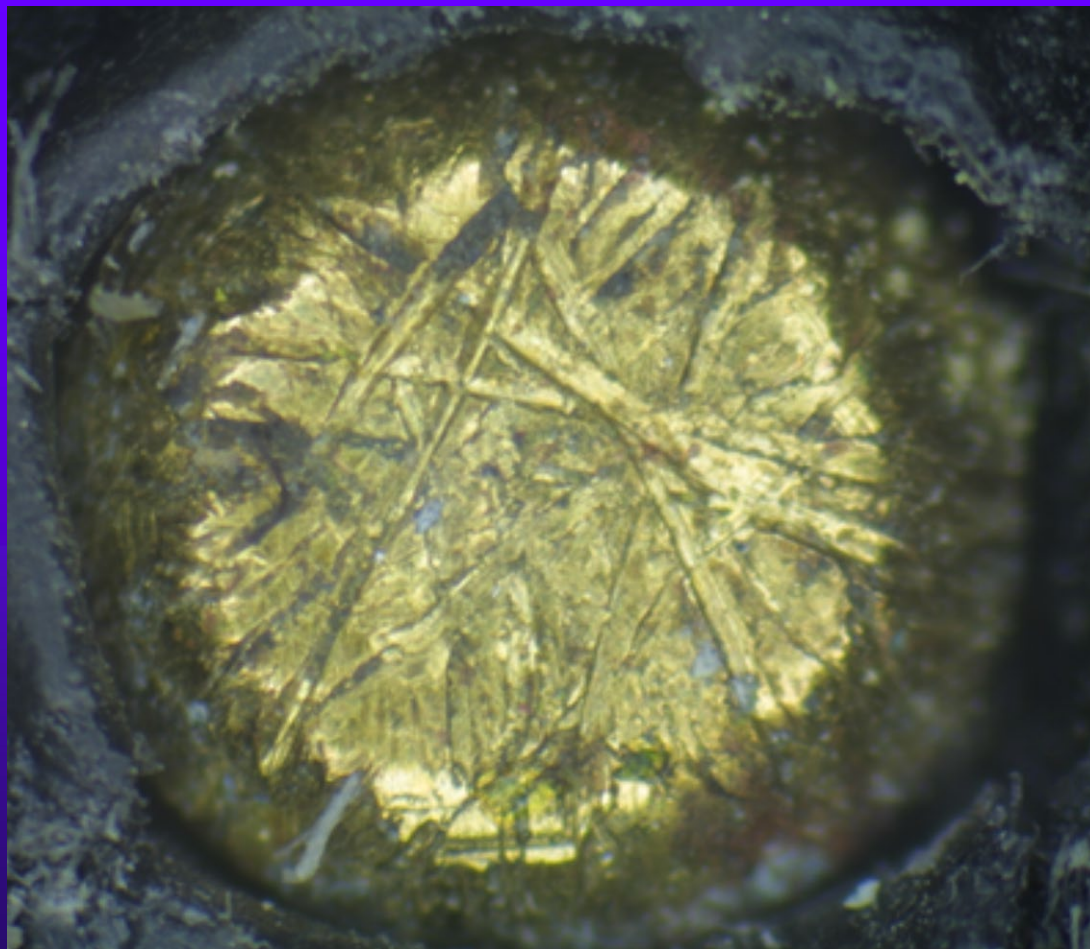




# Pick Marks on Pin

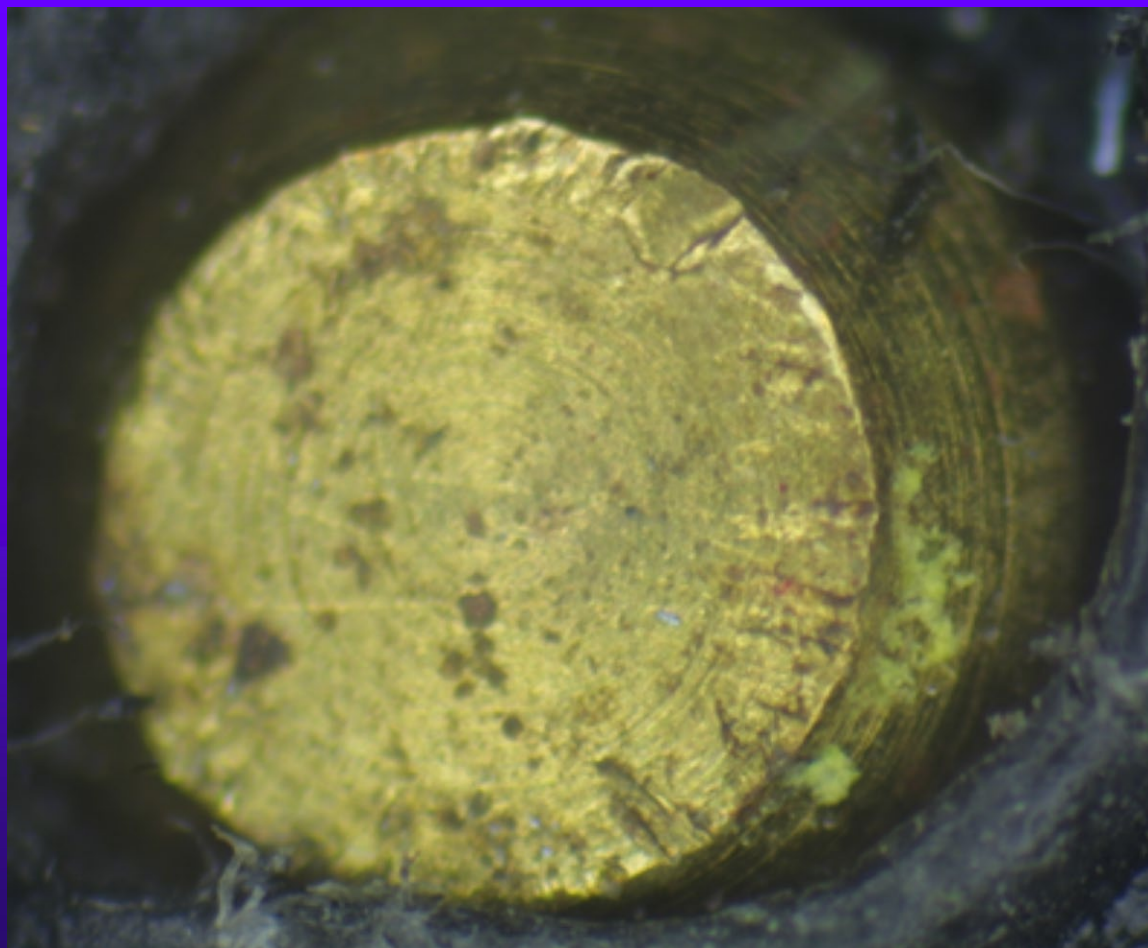


# Marks from Pick Gun

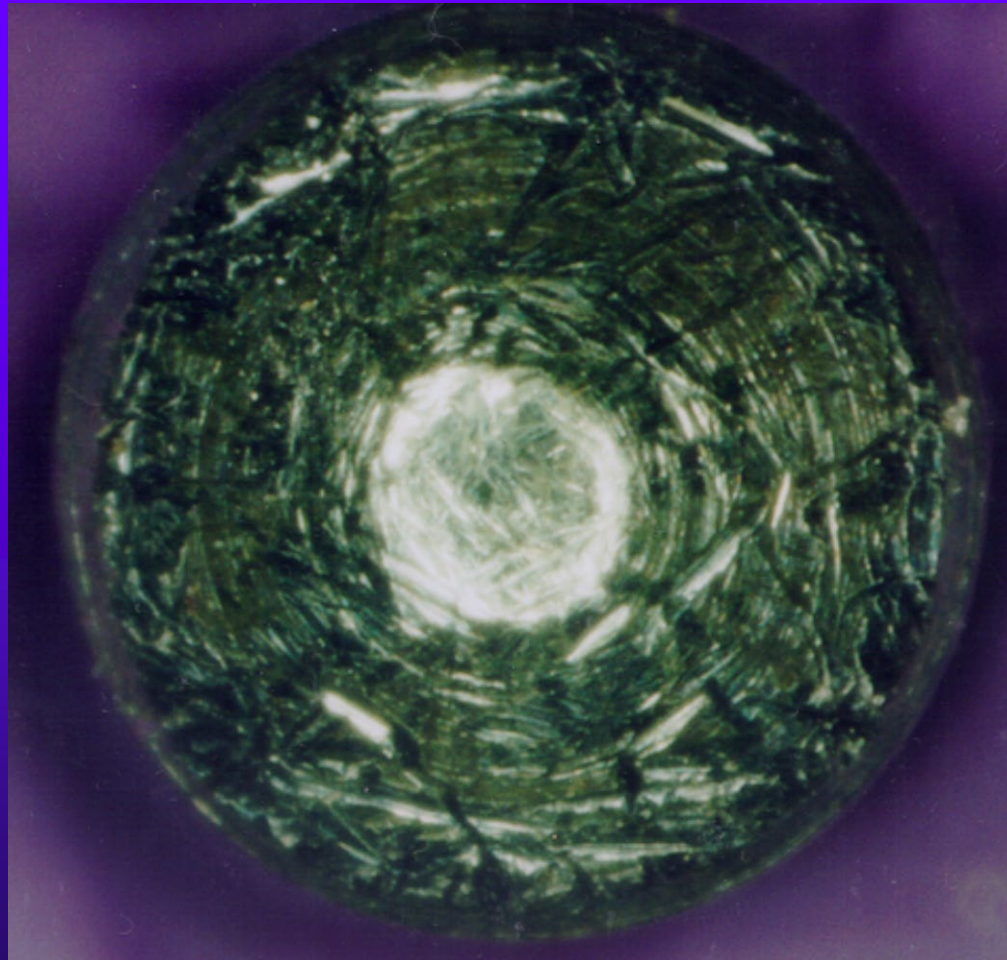




# Pick Gun Markings



# Impact Pick Marks



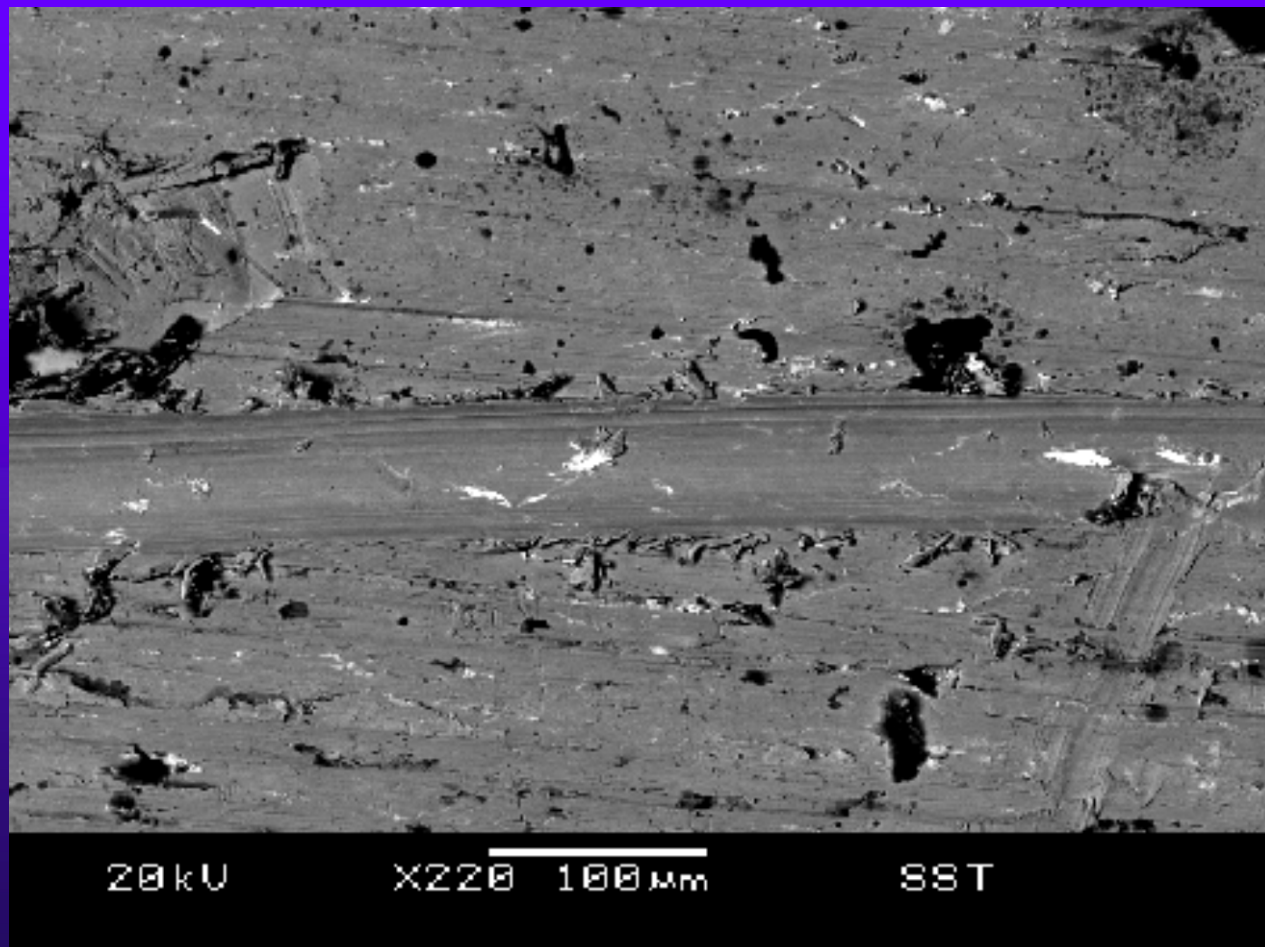


# USE OF SEM

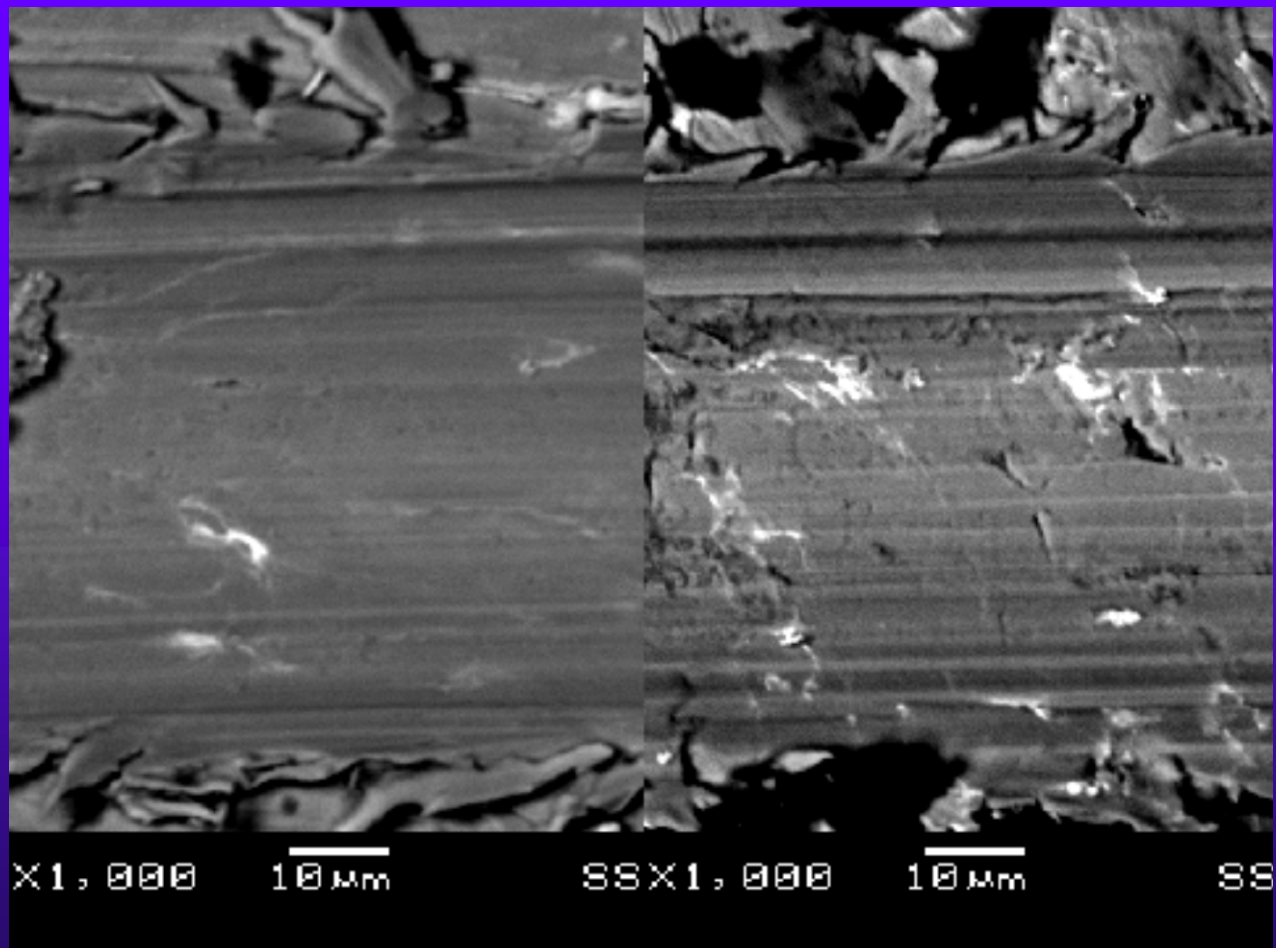




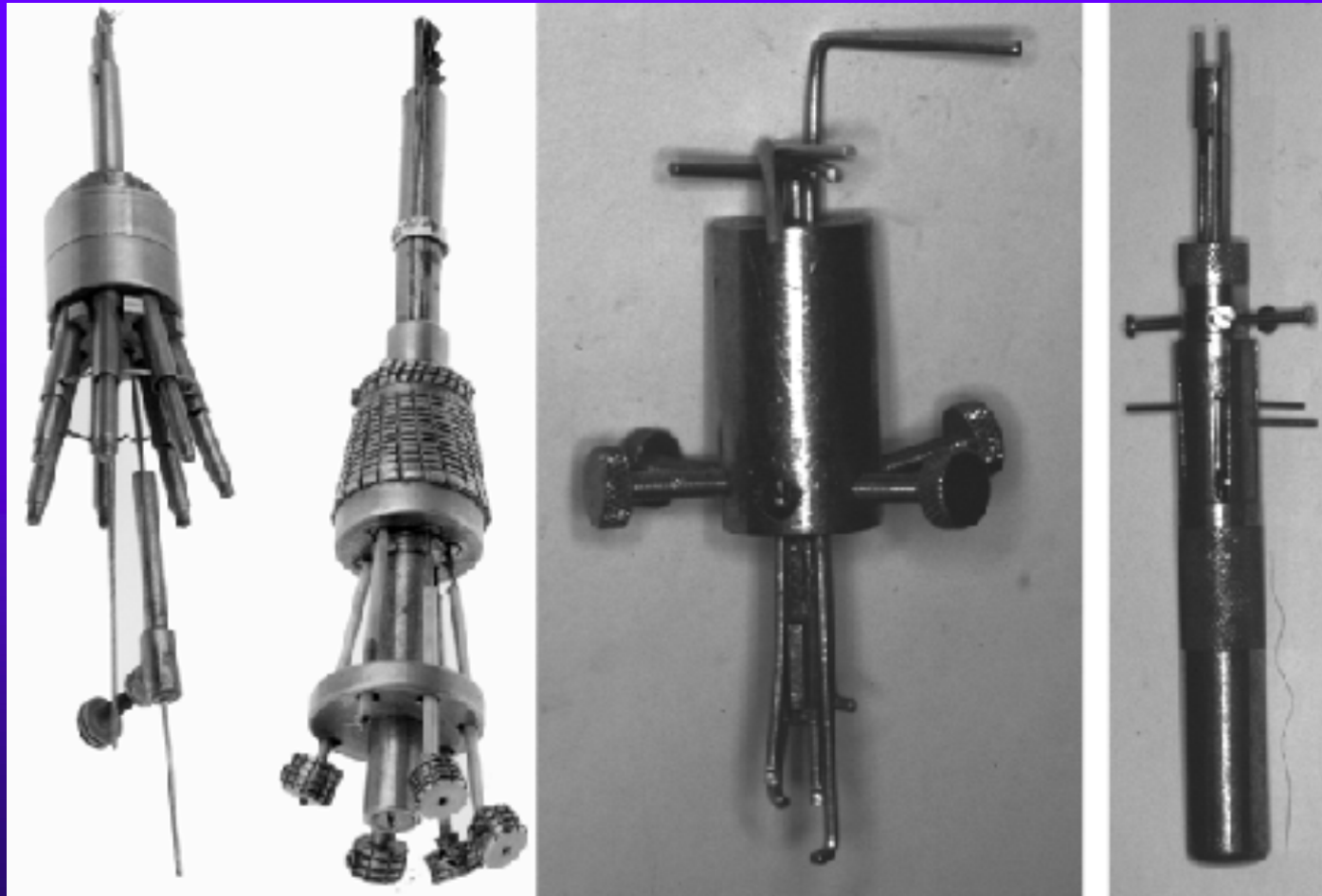
# Pick Tracks



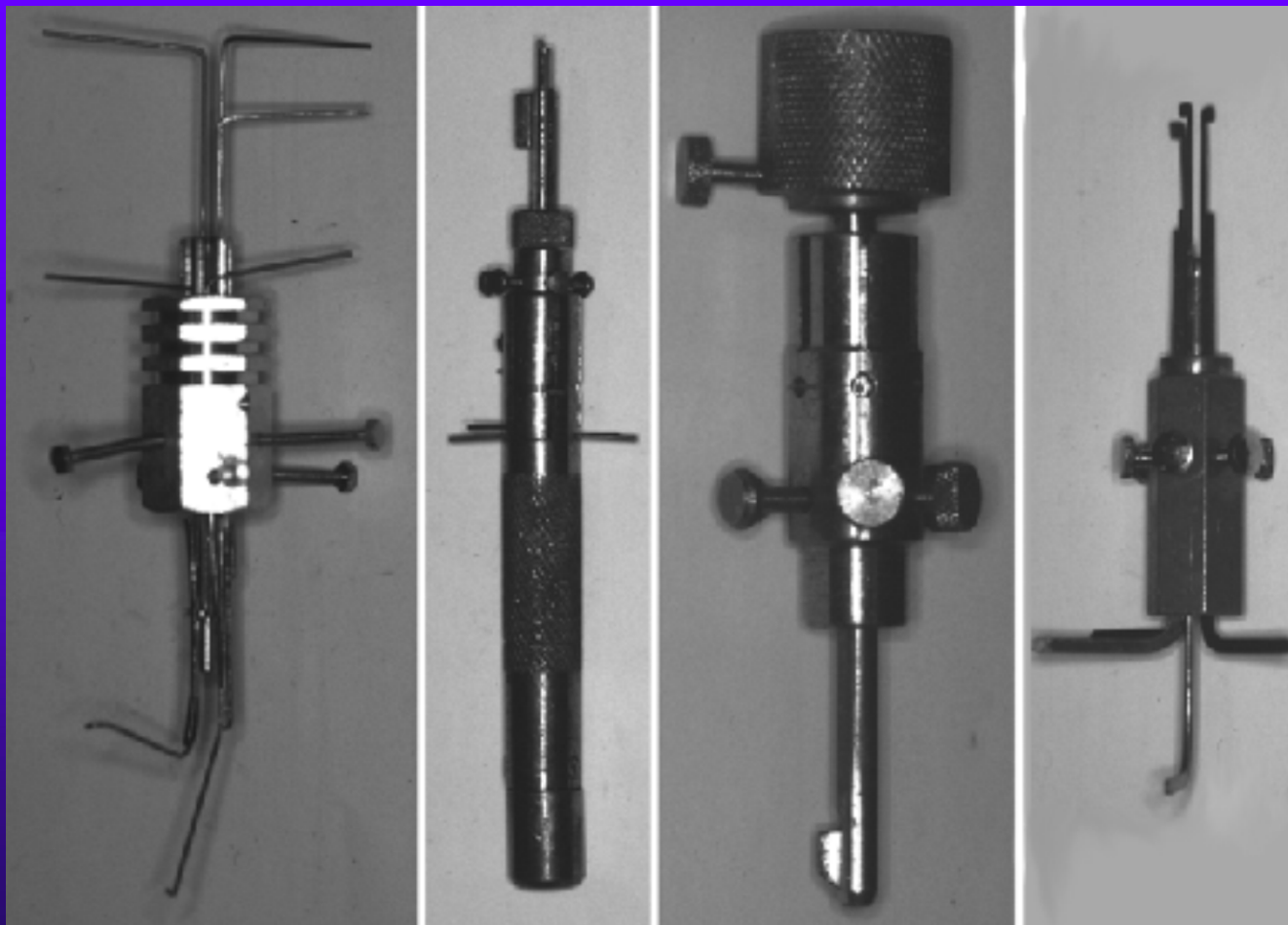
# SEM Pick Track Comparison



# More Special Picks – Europe

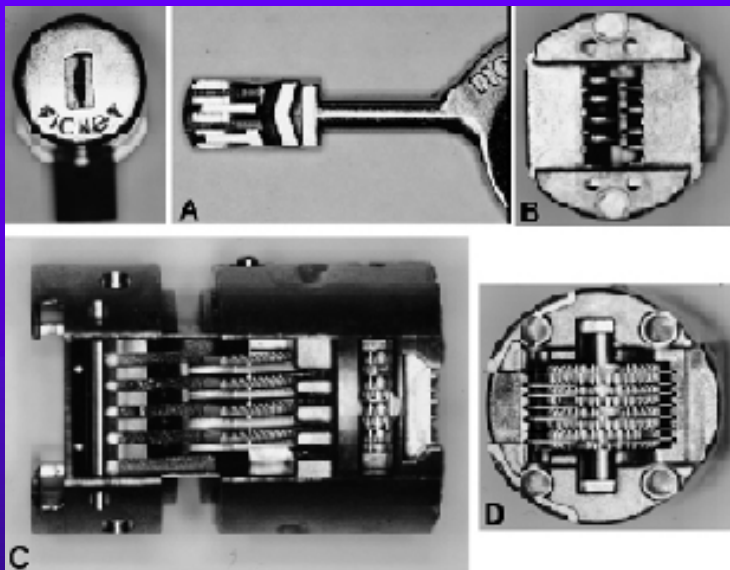


# SPECIAL PICKS



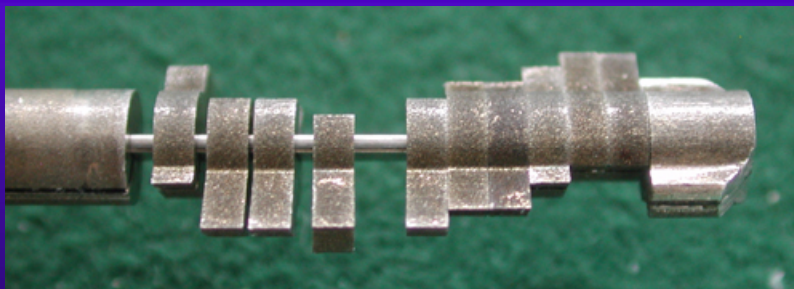


# Fichet Decoder





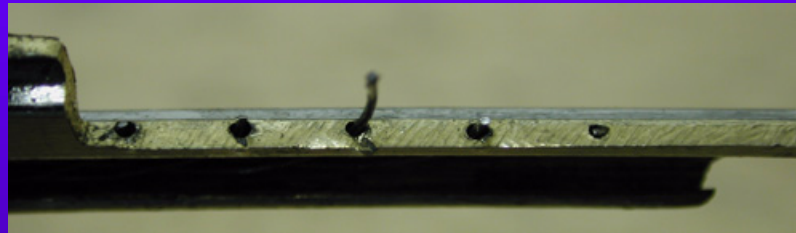
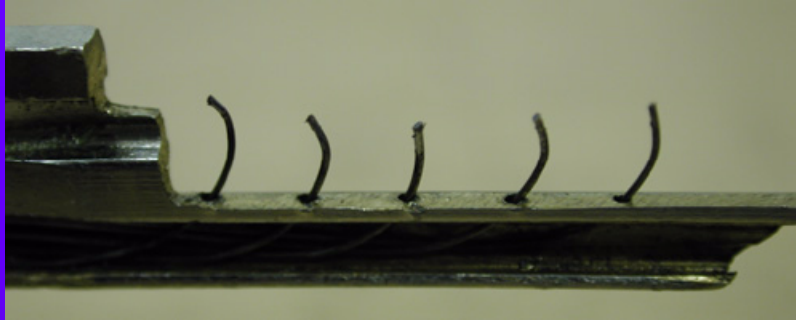
# Chubb Ava decoder



# Rake pick for dimple locks

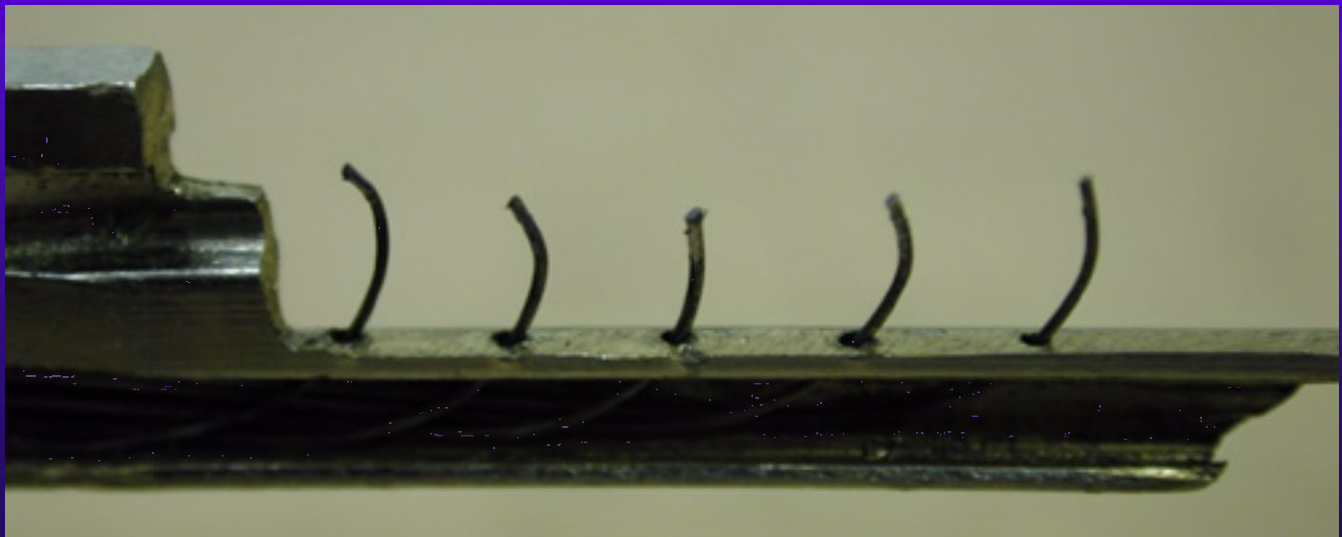
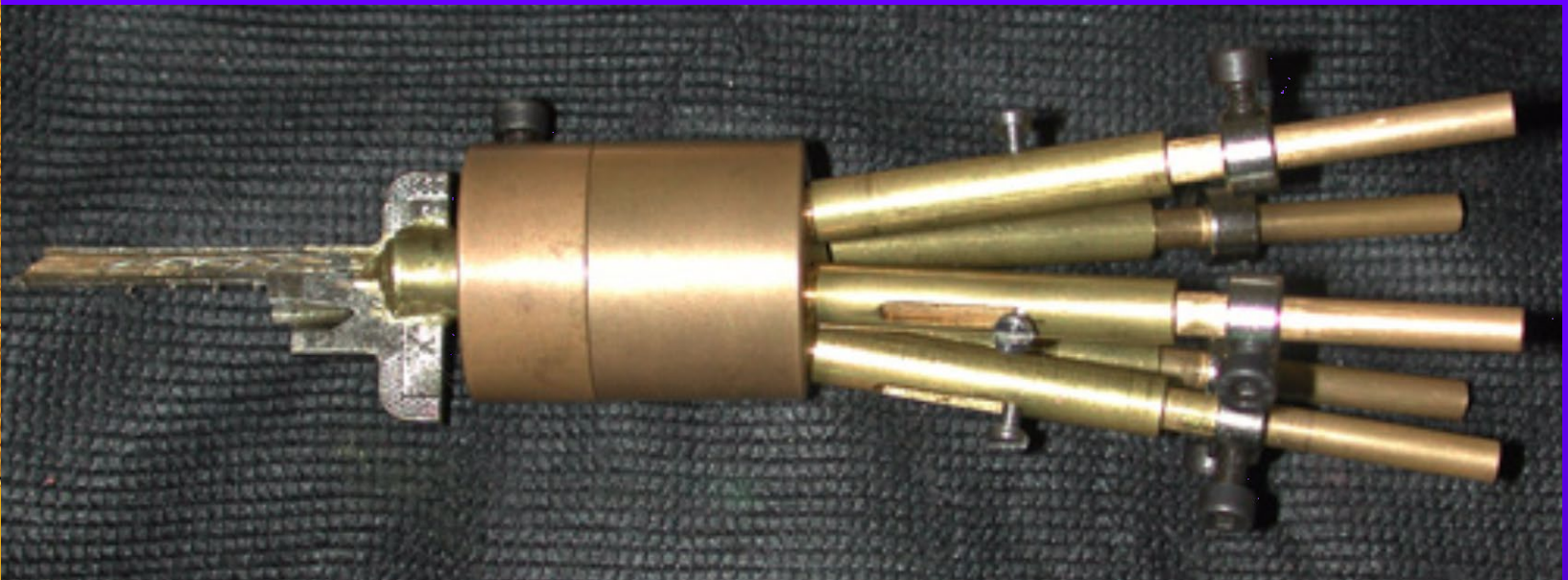


# Feeler Wires for Picking





# SPUTNIK PICK

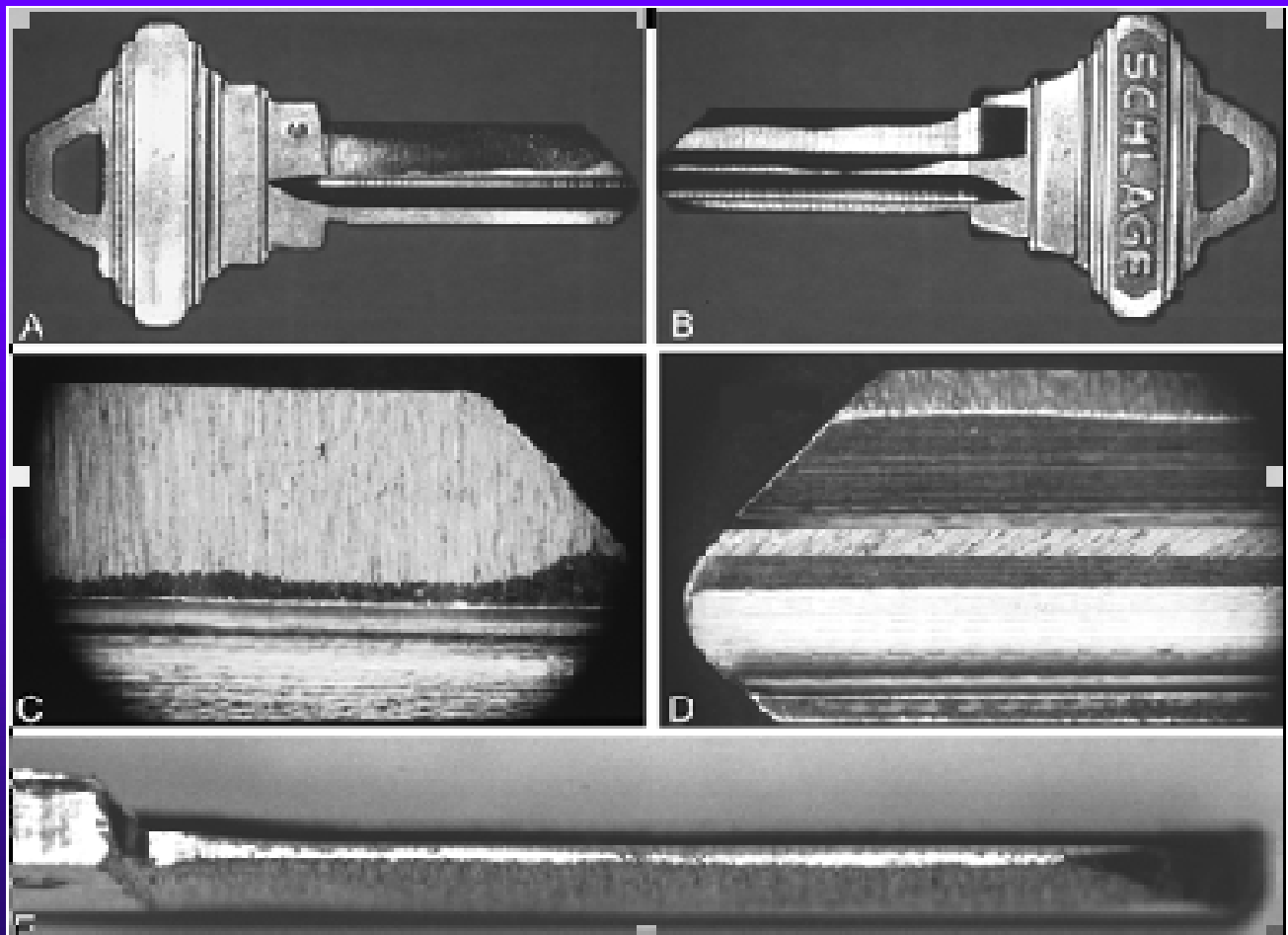




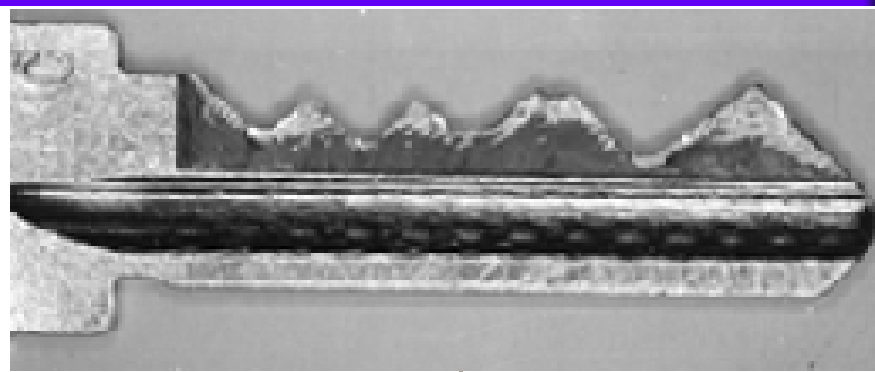
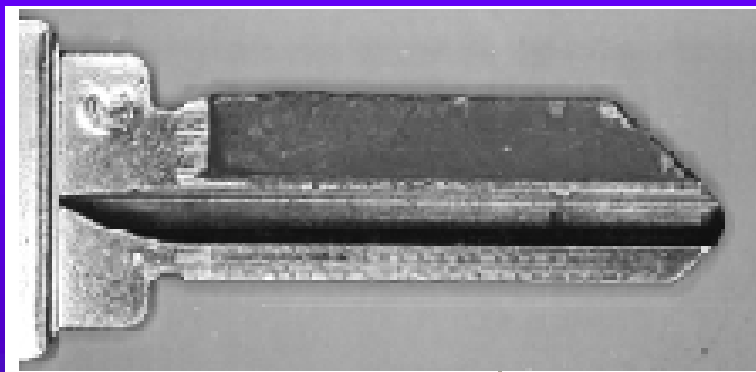


# IMPRESSIONING TOOLS

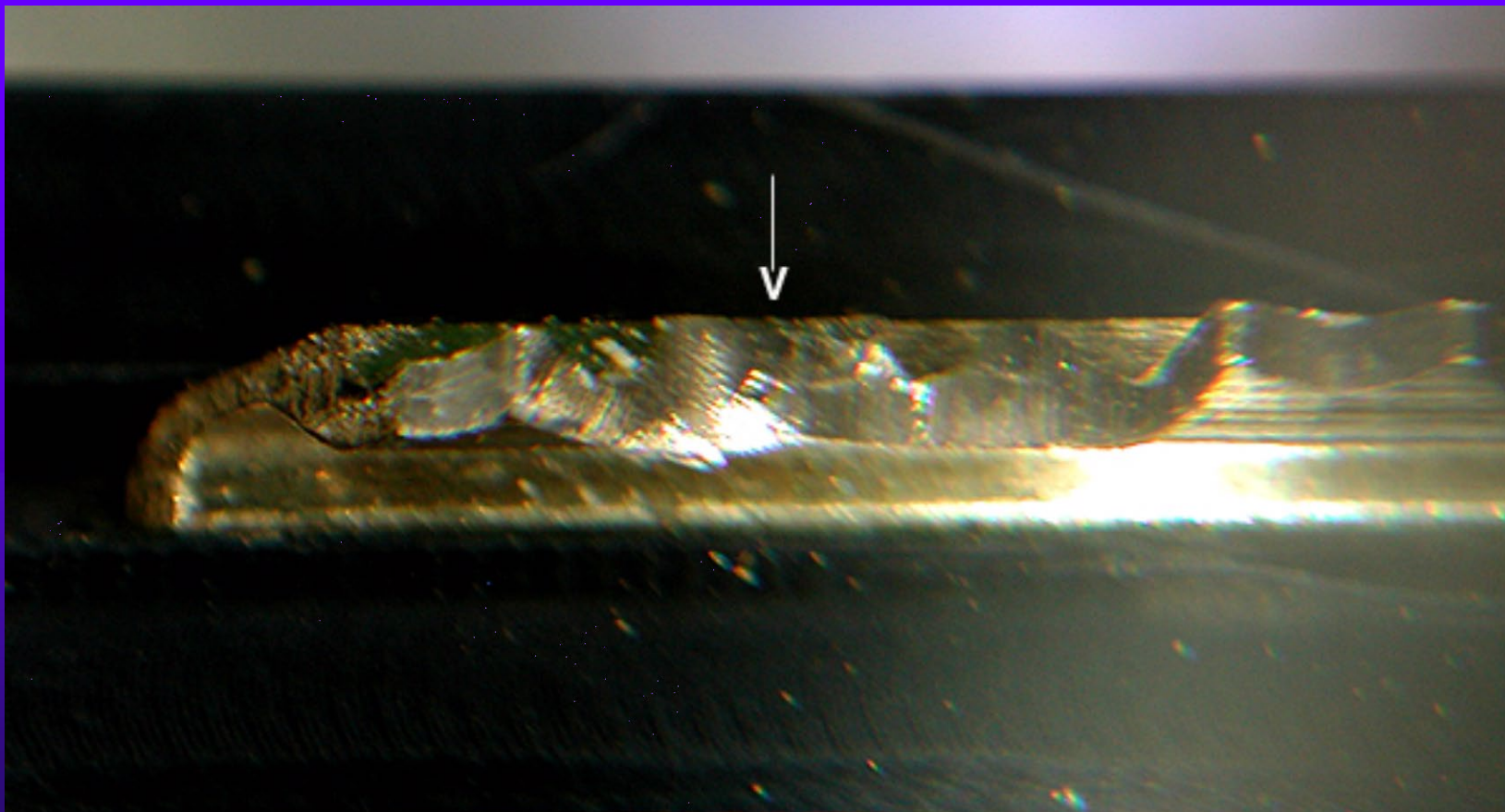
# IMPRESSIONING



# LEAD COMPOSITE IMPRESSIONING

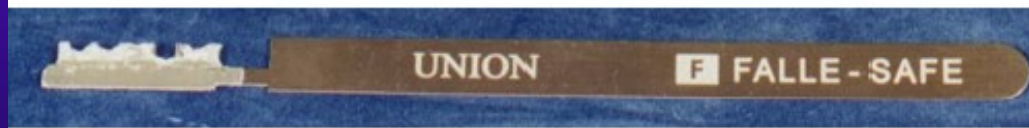
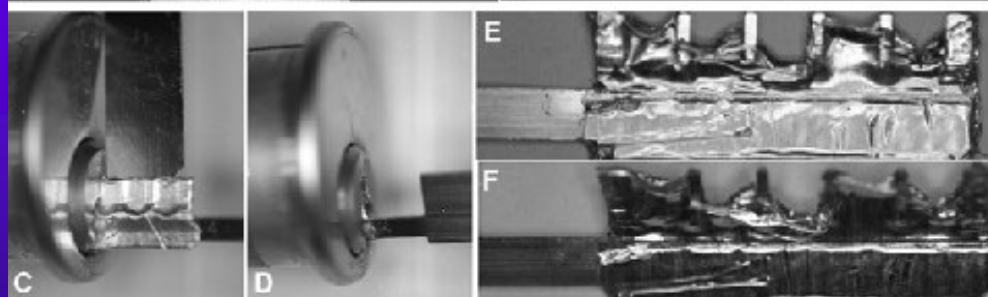
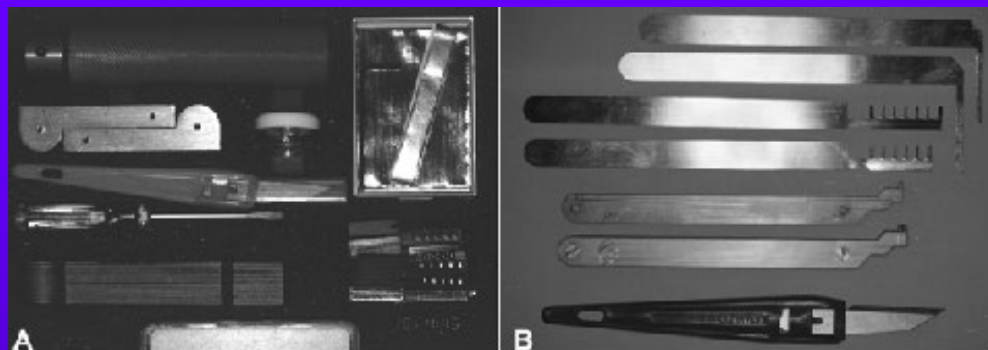


# Marks are Produced

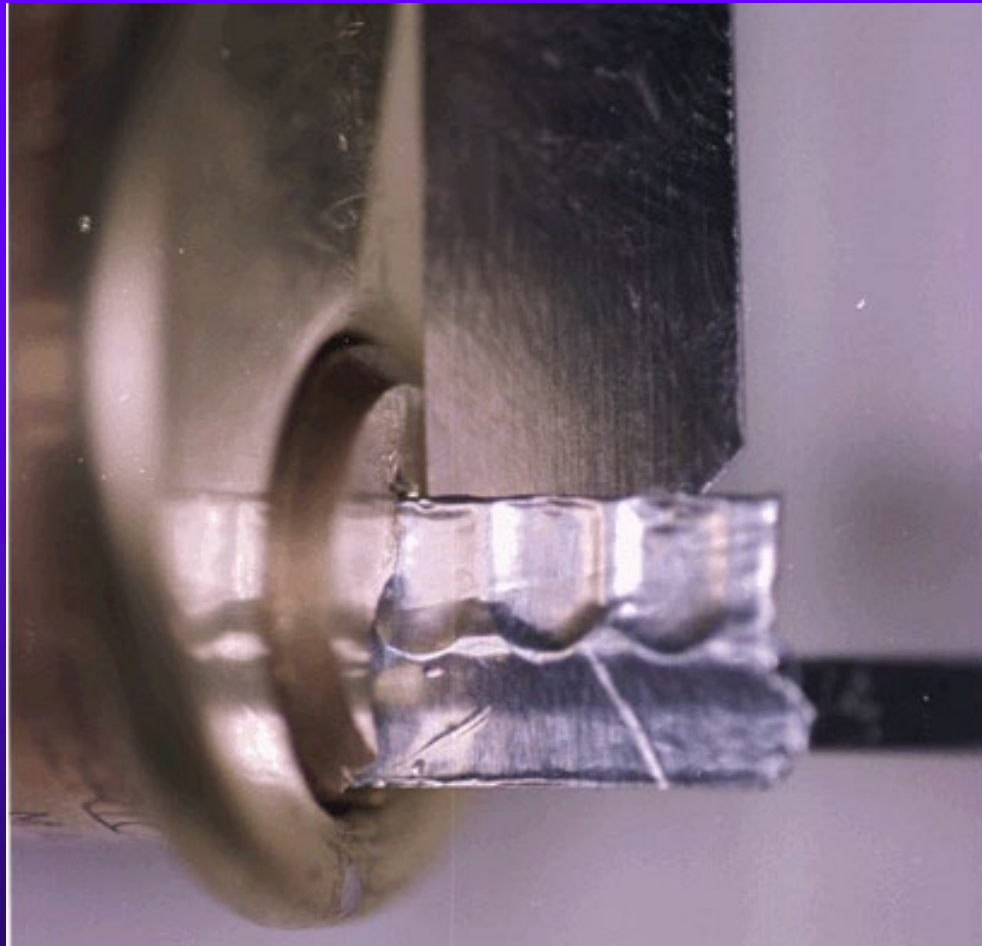




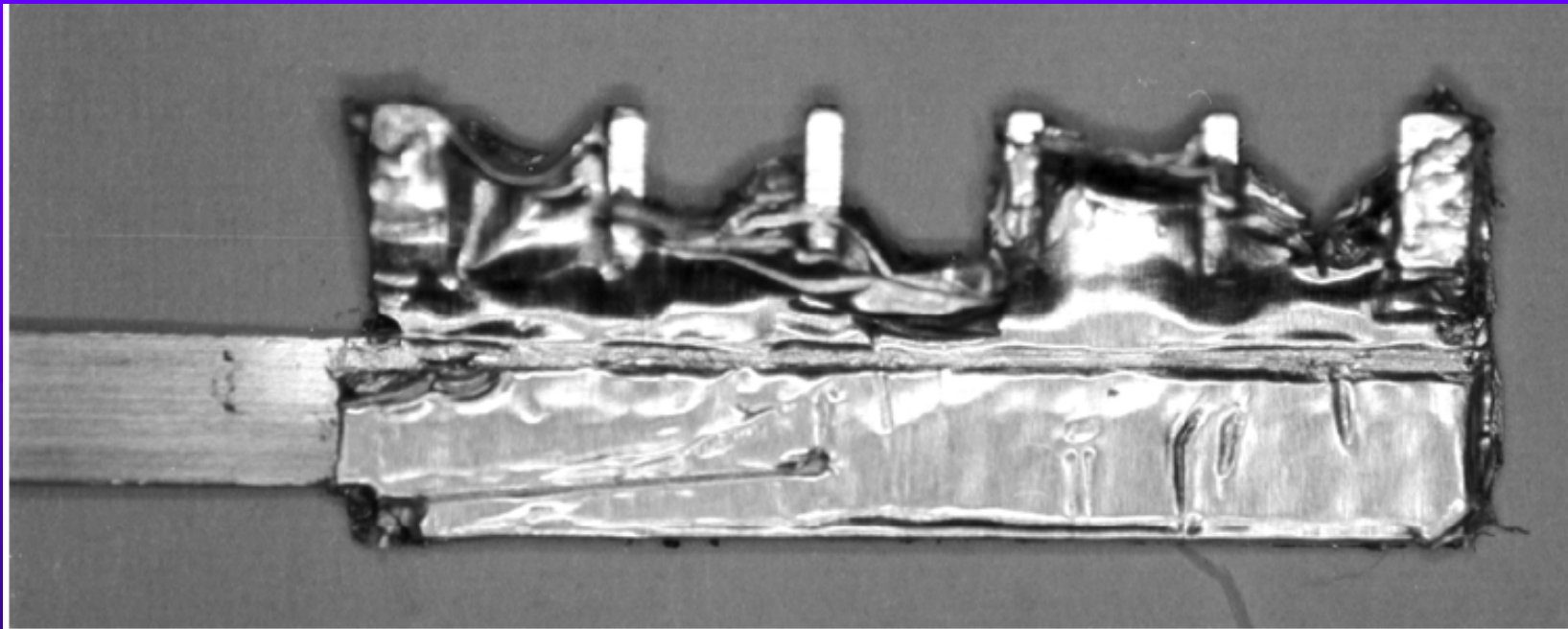
# FOIL IMPRESSIONING TOOLS



# Foil Blank Key is Inserted

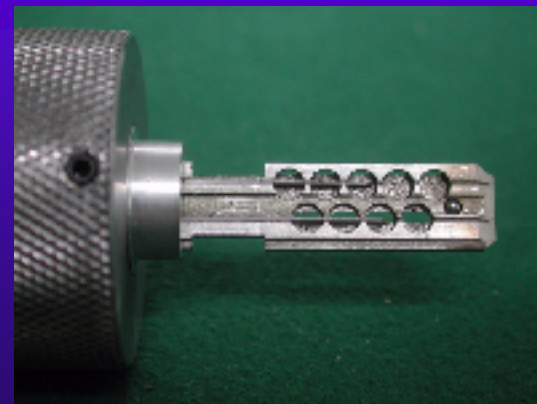
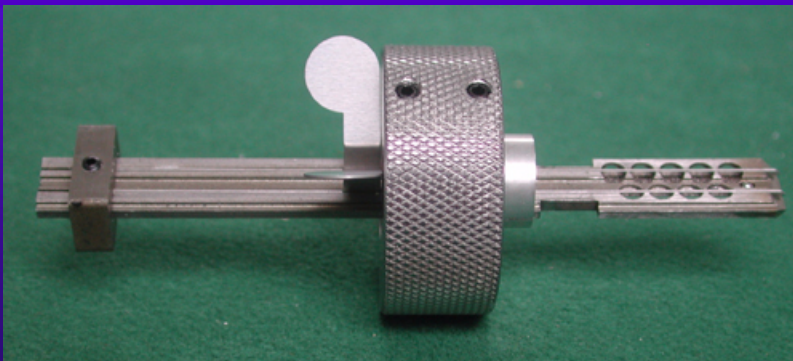
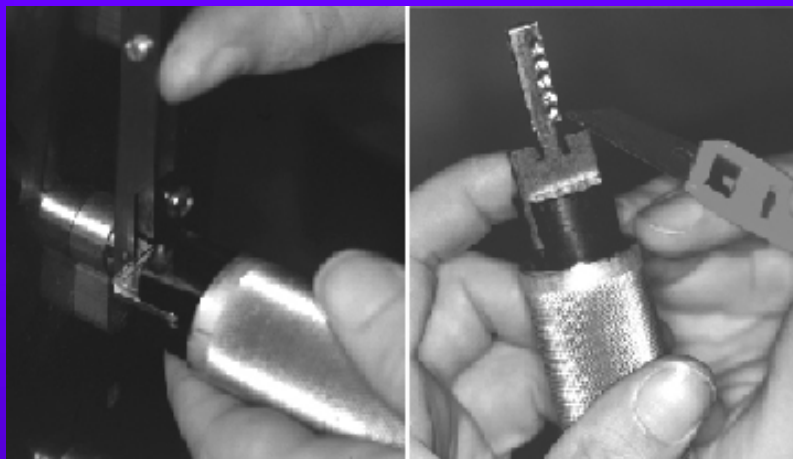


# Foil Key is Produced





# Falle Foil impressioning







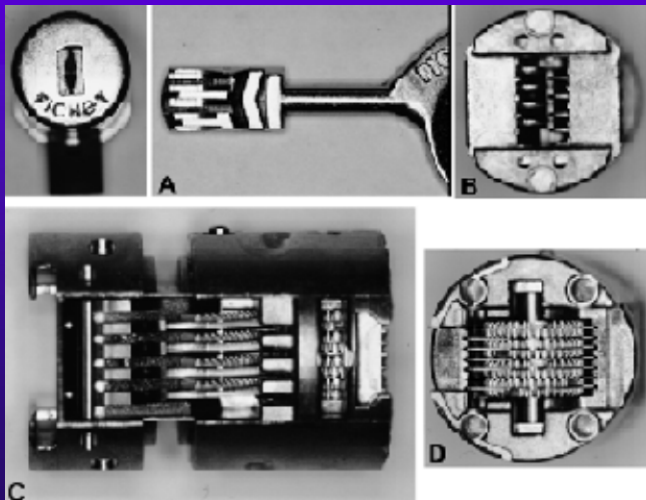
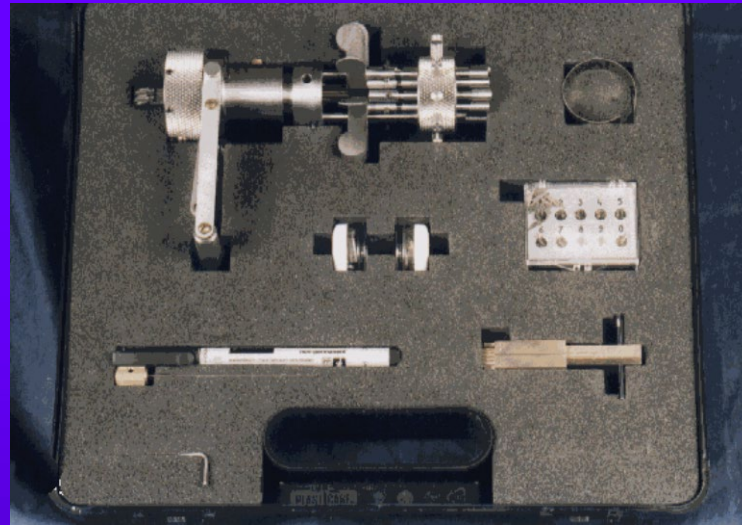
# DECODING OF LOCKS

Many techniques

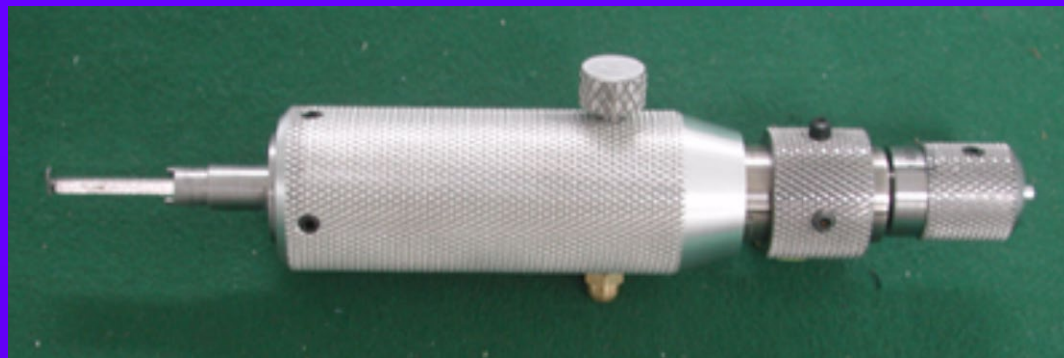
Many specialized tools

Derive key codes to simulate or generate a key

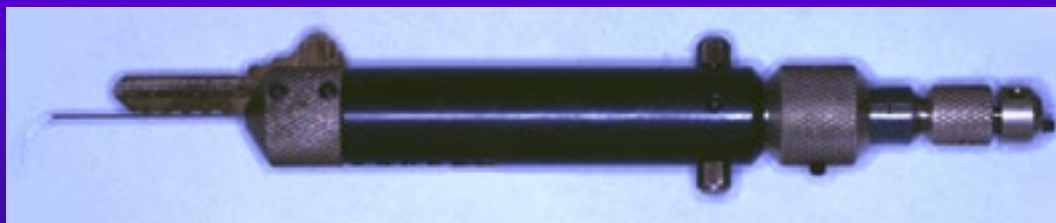
# DECODING OF LOCKS



# DECODING OF LOCKS

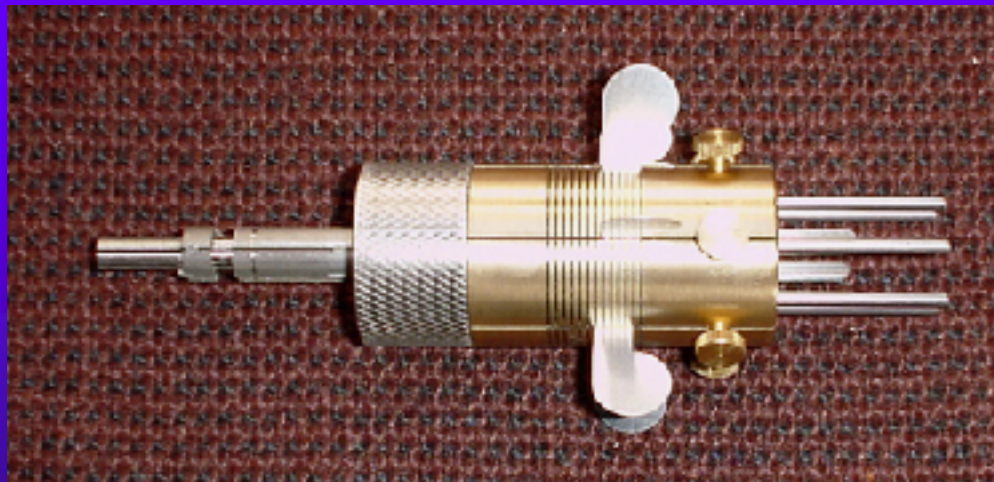


# DECODING OF LOCKS

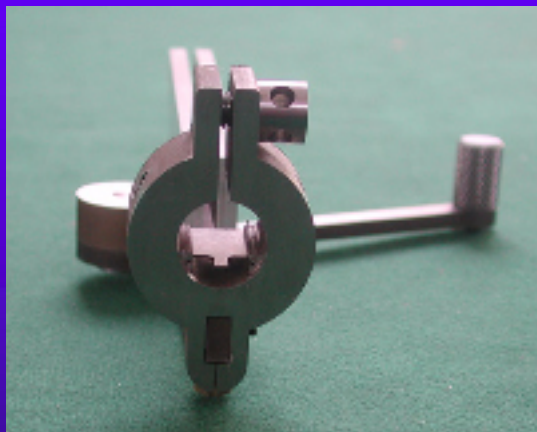




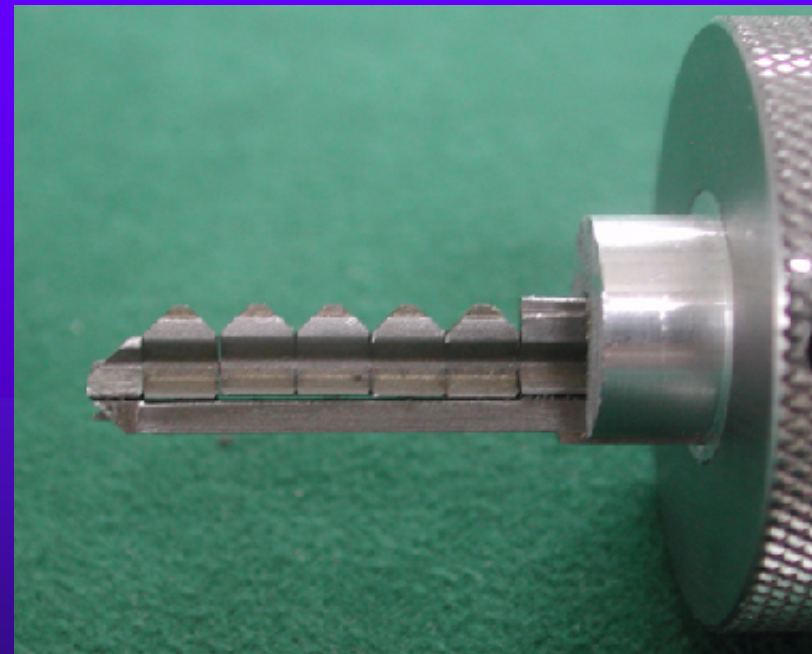
# PICARD Pick



# Evva 3KS Decoder



# FALLE Pin Lock Decoder v.2



# FALLE Pin lock decoder





# Variable Key Generation



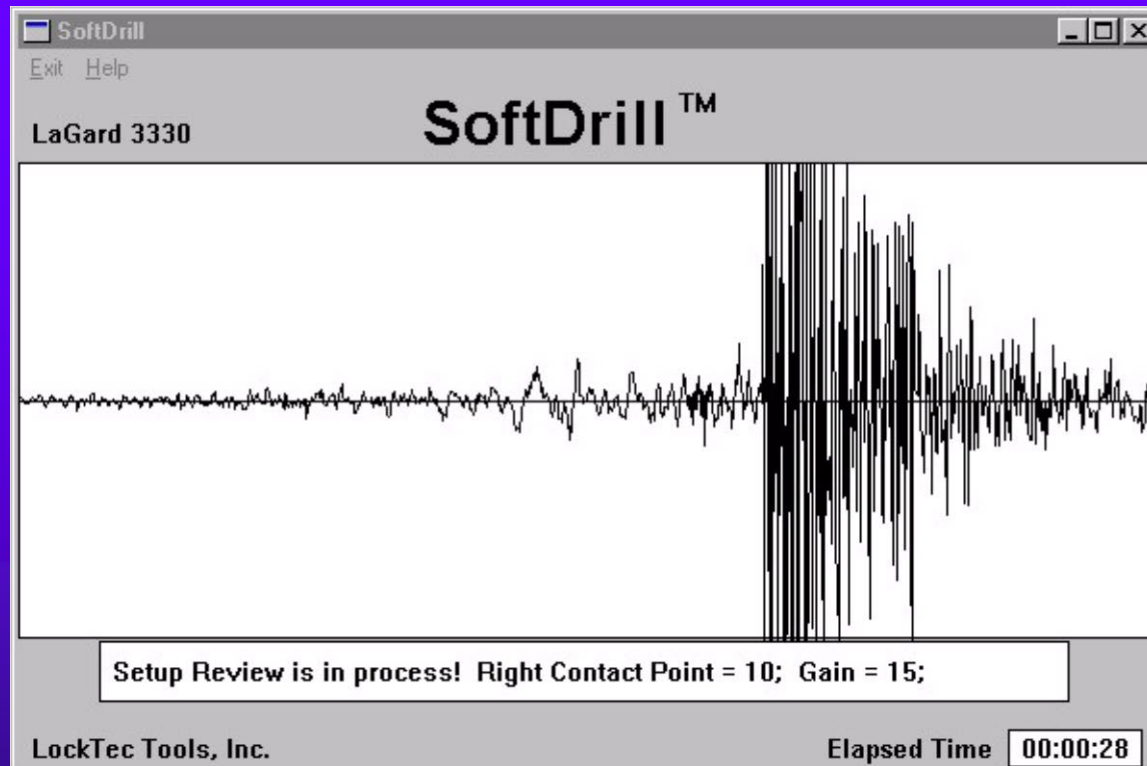


# COMBINATION LOCK BYPASS

# MANIPULATION OF COMBINATION LOCKS



# Soft Drill Output Data



- ☐ Increase cam park position
- ☐ Decrease cam park position
- ☐ Increase Gain and Click
- ☐ Decrease Gain and Click
- ☐ Click
- ☐ MultiClick
- ☐ Continue Test

Cancel





# Summary of Bypass Techniques

- ◆ Never certain
- ◆ Skill required
- ◆ Time required
- ◆ Specialized tools required
- ◆ Potential for discovery
- ◆ May require several locks
- ◆ Problems may develop which will leave evidence



# Conventional Bypass

- ◆ Picking
- ◆ Impressioning
- ◆ Decoding
- ◆ Alternative methods



# Bypass Alternative

- ◆ Obtain the Top Level Master Key
  - Open all locks
  - No forensic trace
  - Totally covert
  - Access assured
  - Can accomplish over time



# LOCKS, SAFES, AND SECURITY

© 2018 Marc Weber Tobias and Tobias Bluzmanis

[mwtobias@securitylaboratories.org](mailto:mwtobias@securitylaboratories.org)