



HISTORY OF LOCKS, DESIGNS, AND BYPASS

Locks, Safes, and Security
LSS+ Multimedia Supplement

www.security.org



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”



LEGAL ISSUES

- ◆ Liability
- ◆ Federal and state laws
- ◆ Personal safety
- ◆ Reputation
- ◆ Confidential records
- ◆ Negligence in design, defective product
- ◆ Locksmith liability



DISCLOSURE OF DEFECTS

- ◆ Legal liability
- ◆ Ethics
- ◆ Protection of public
- ◆ Education



LOCKS: THEIR HISTORY AND DESIGNS



PRIMER ON LOCKS

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



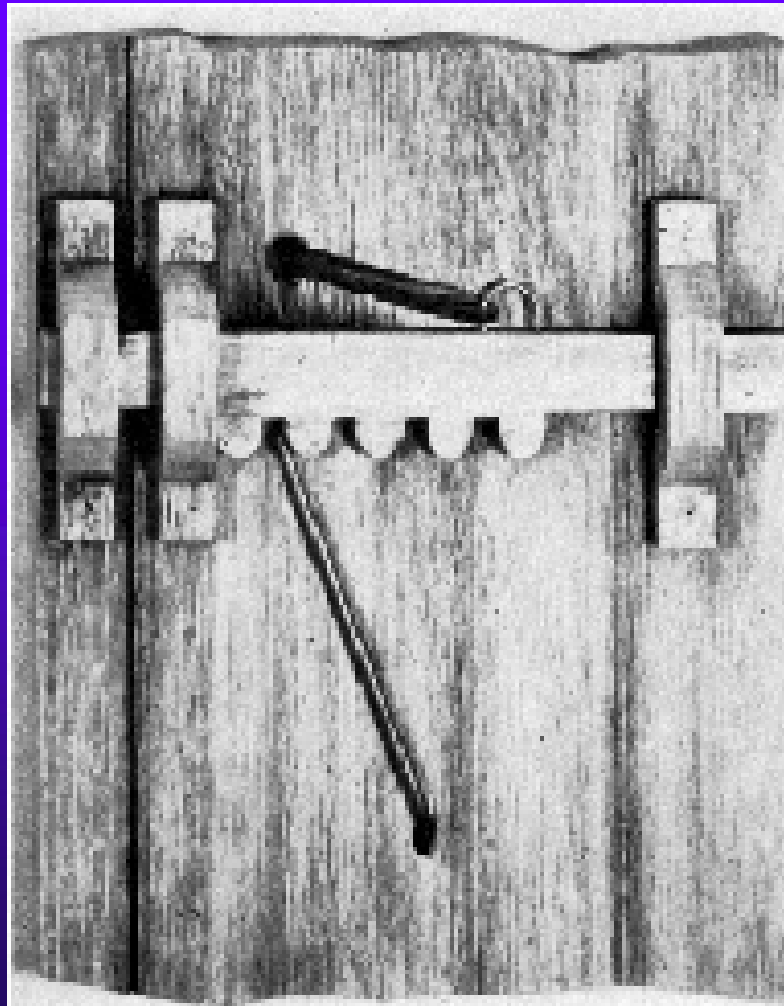
BASIC TYPES OF LOCKS

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

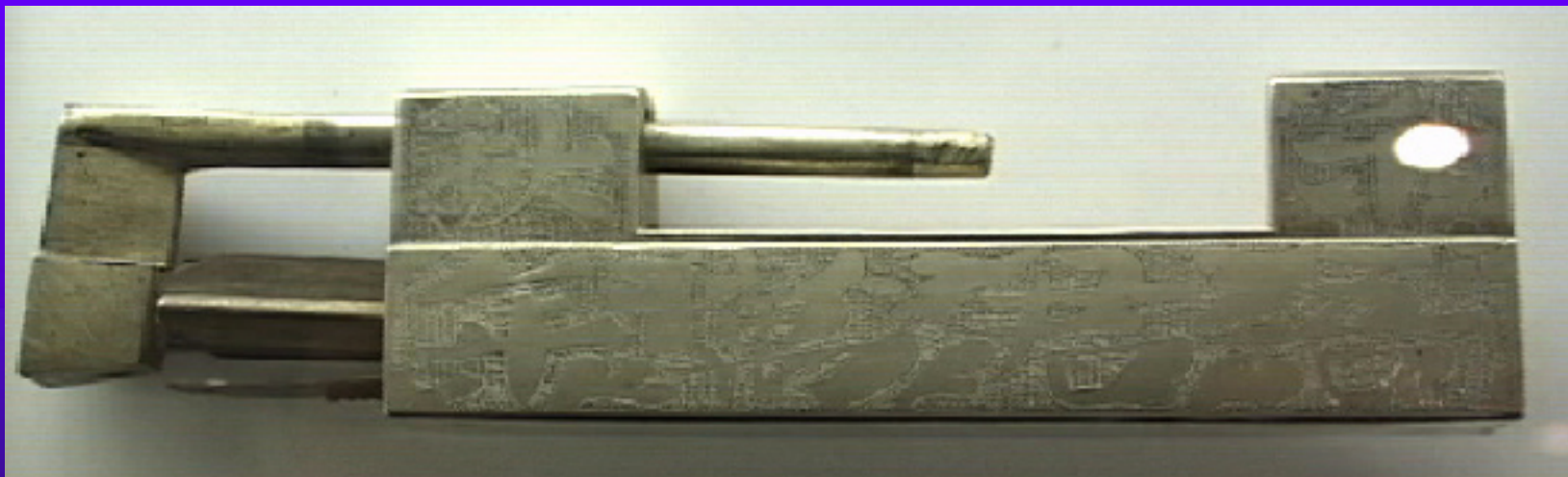


BEGINNING OF PHYSICAL SECURITY

GREEK LOCK



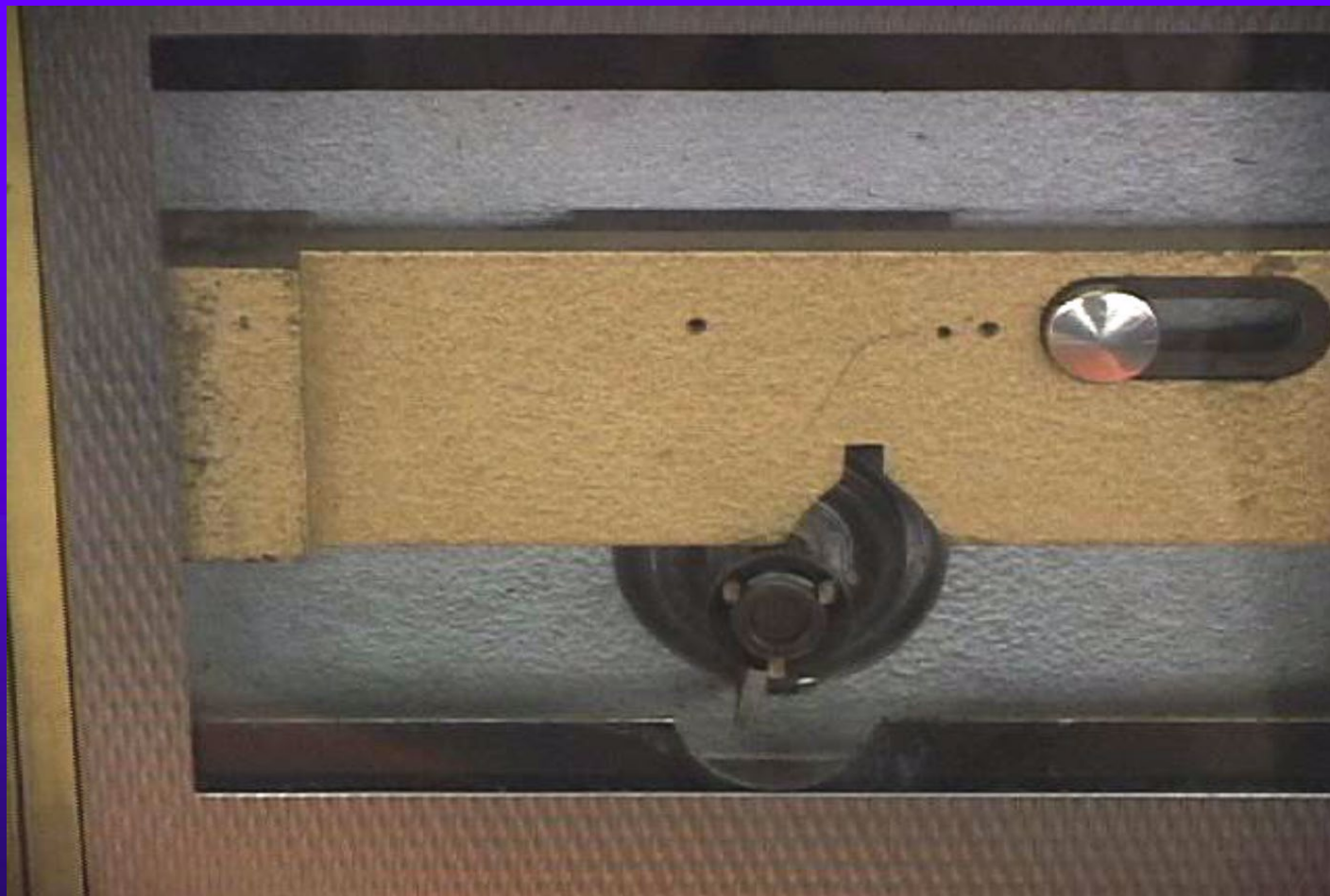
ROMAN PADLOCK



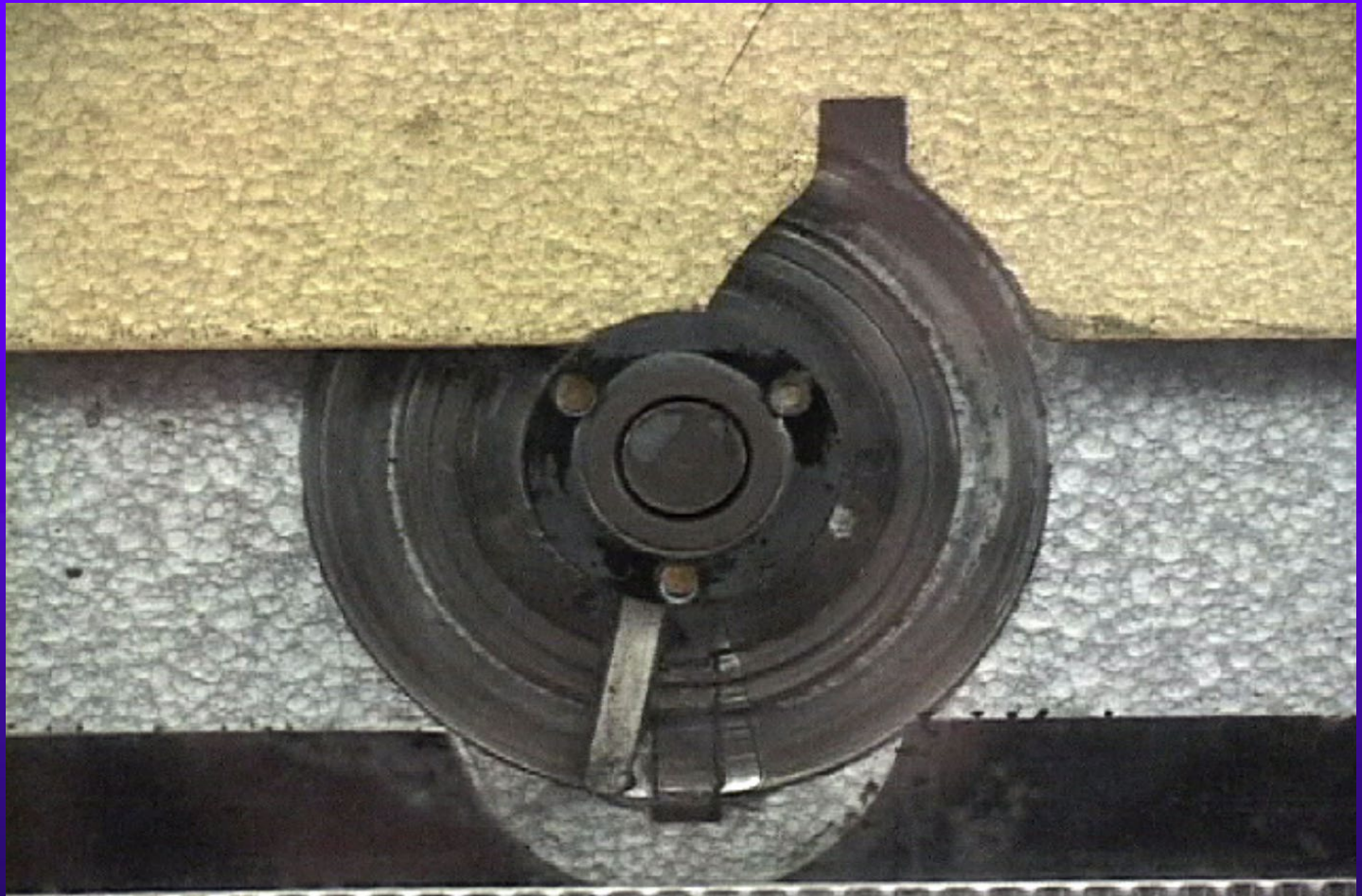


WARDED LOCK

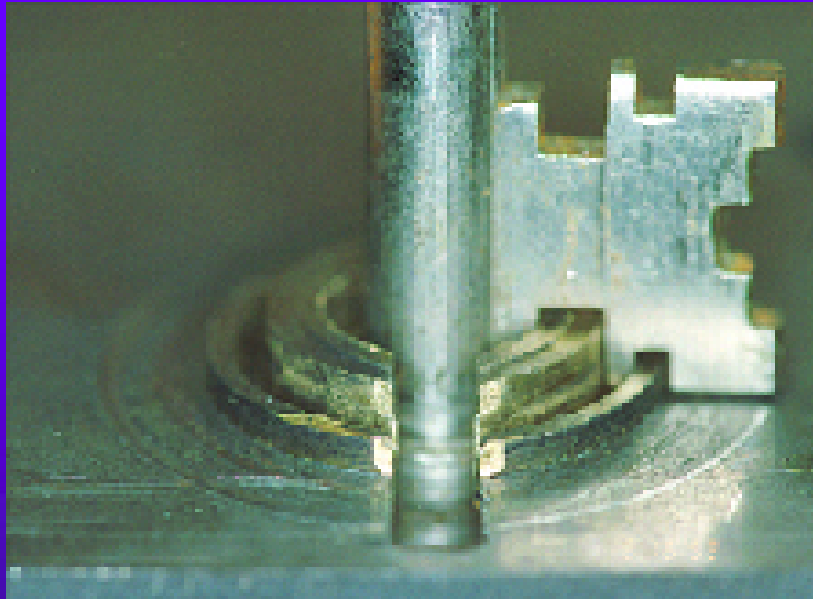
WARDDED LOCK



Warded lock detail



WARDDED LOCK AND KEY



EARLY WARDED LOCK



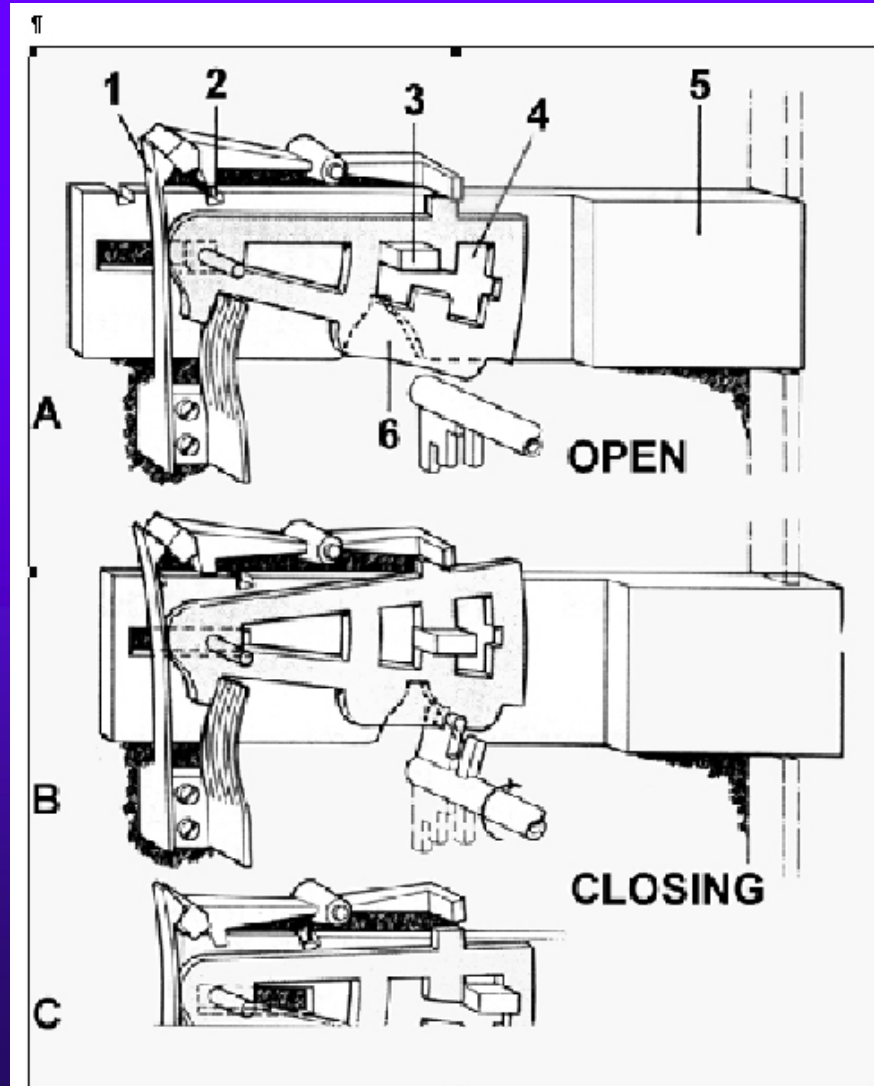
Warded lock for chest



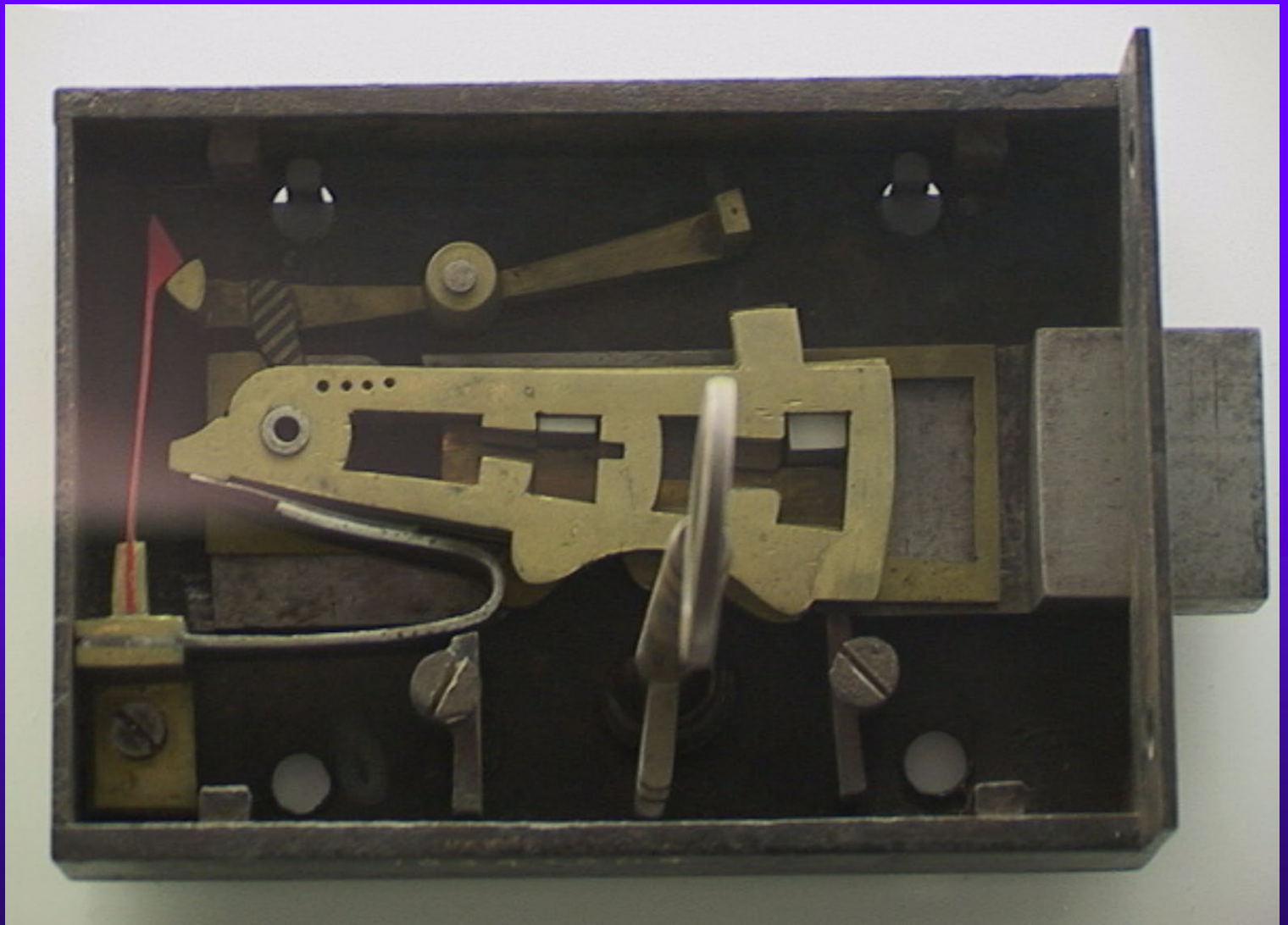


LEVER LOCK

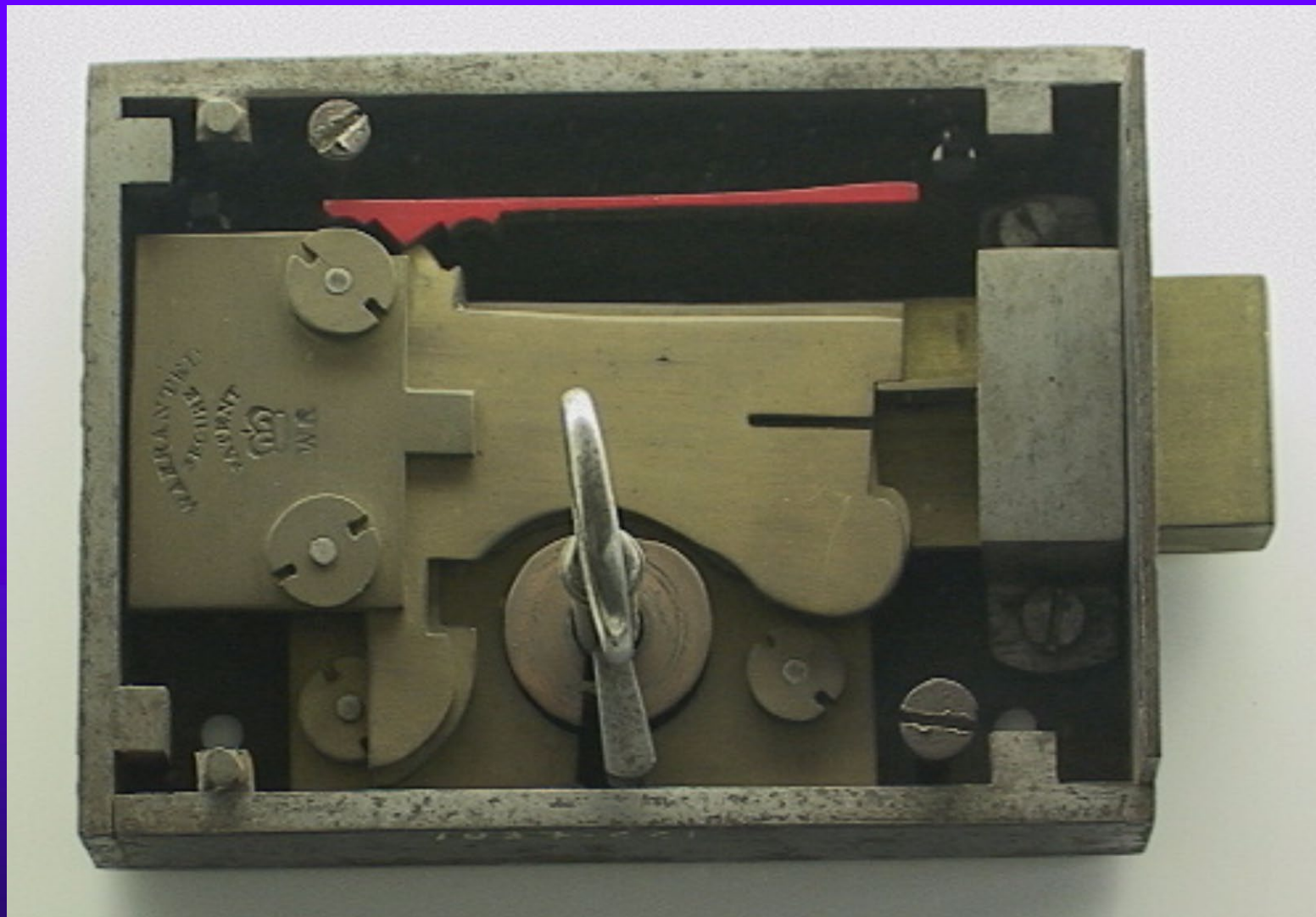
LEVER LOCK OPERATION



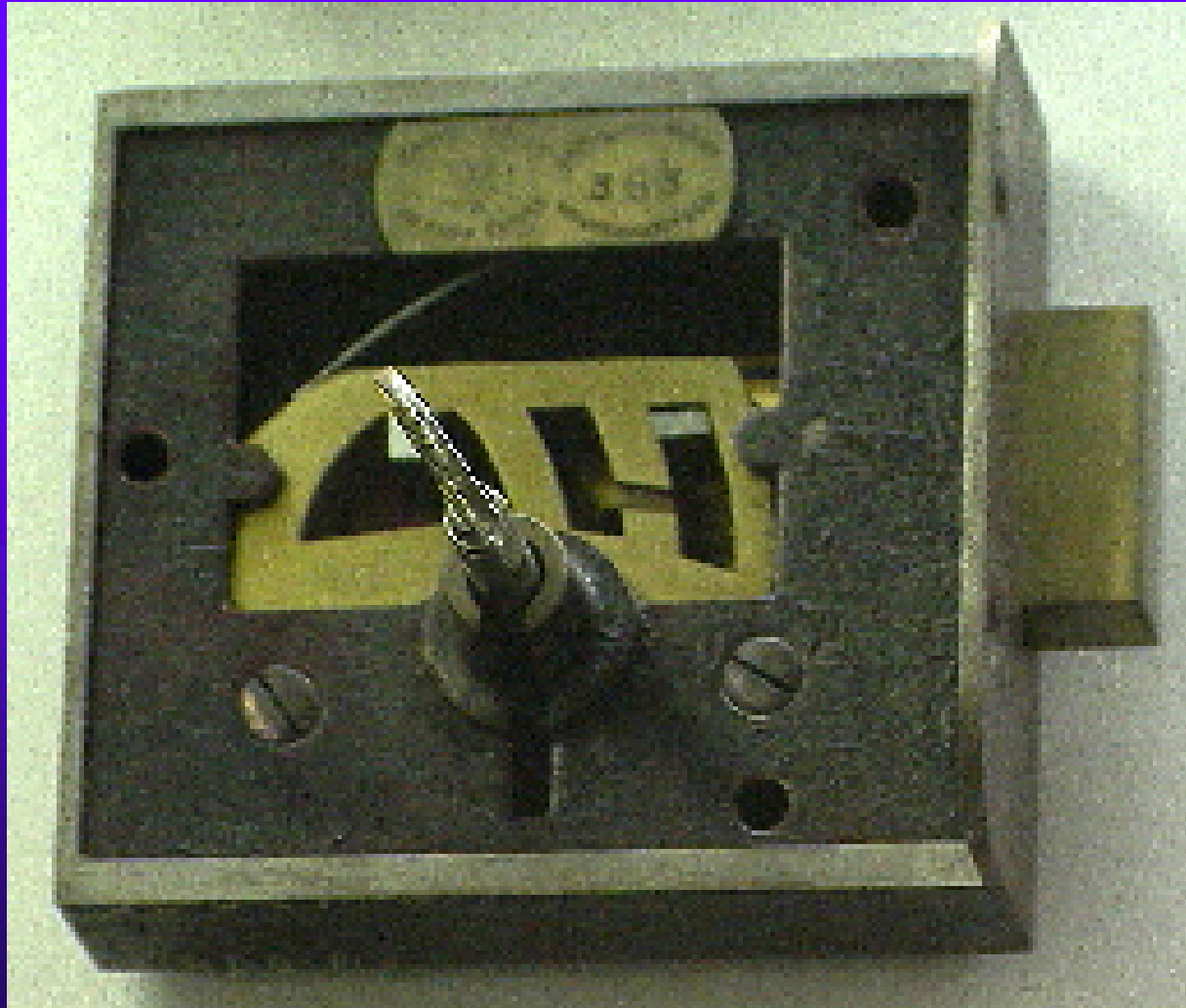
CHUBB Detector, 1827



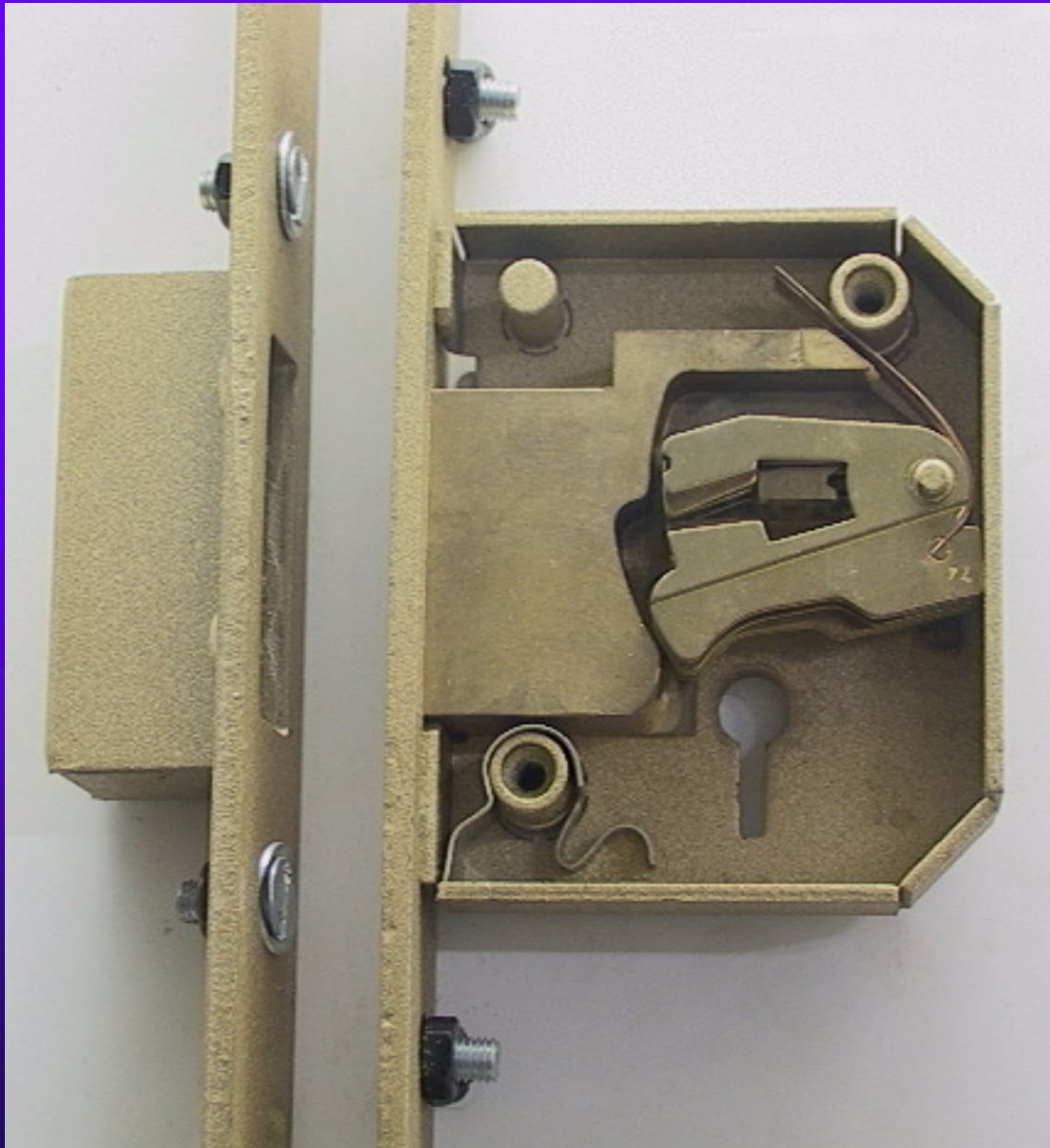
CHUBB Detector Lock



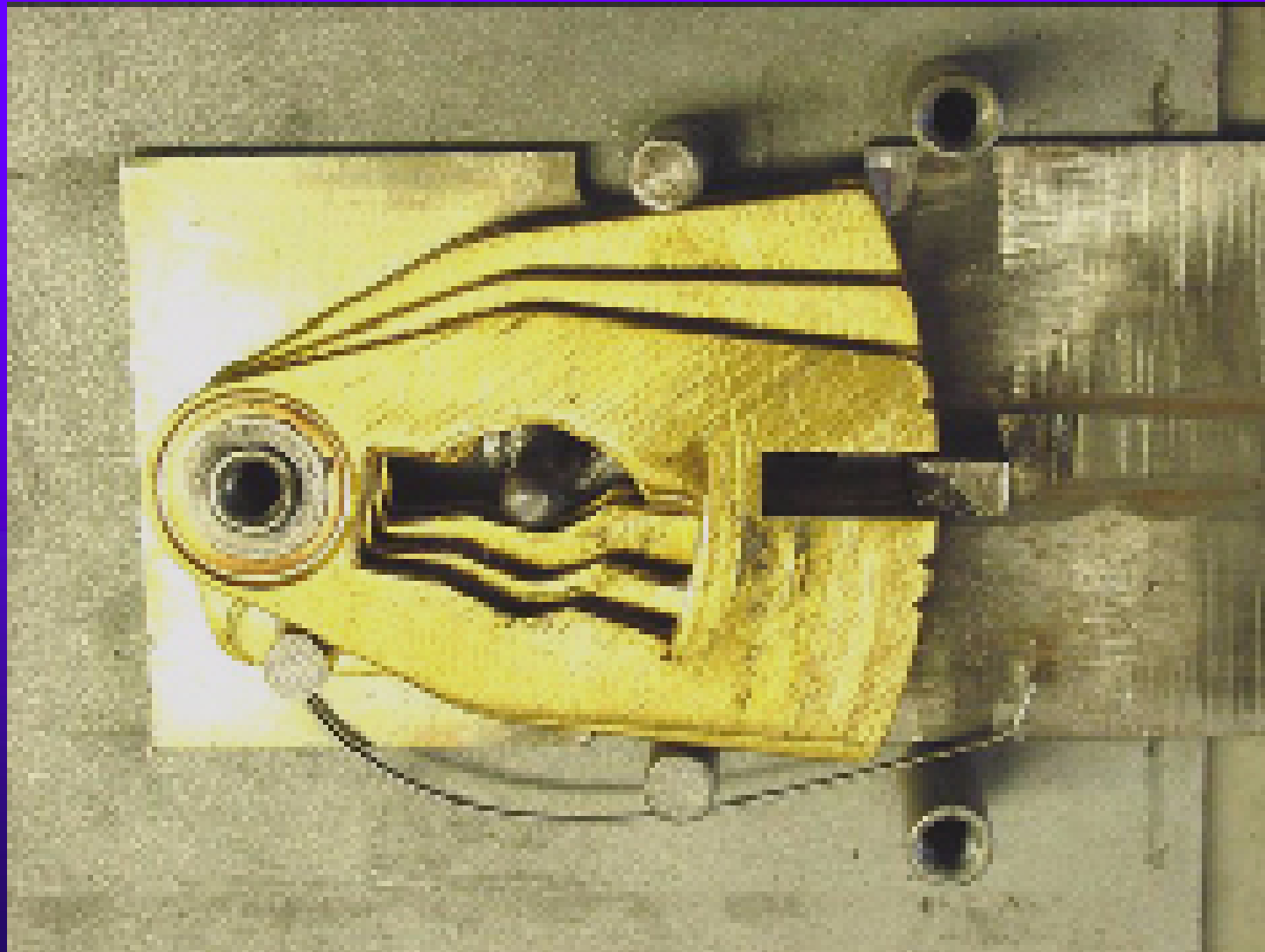
NePLUS LEVER



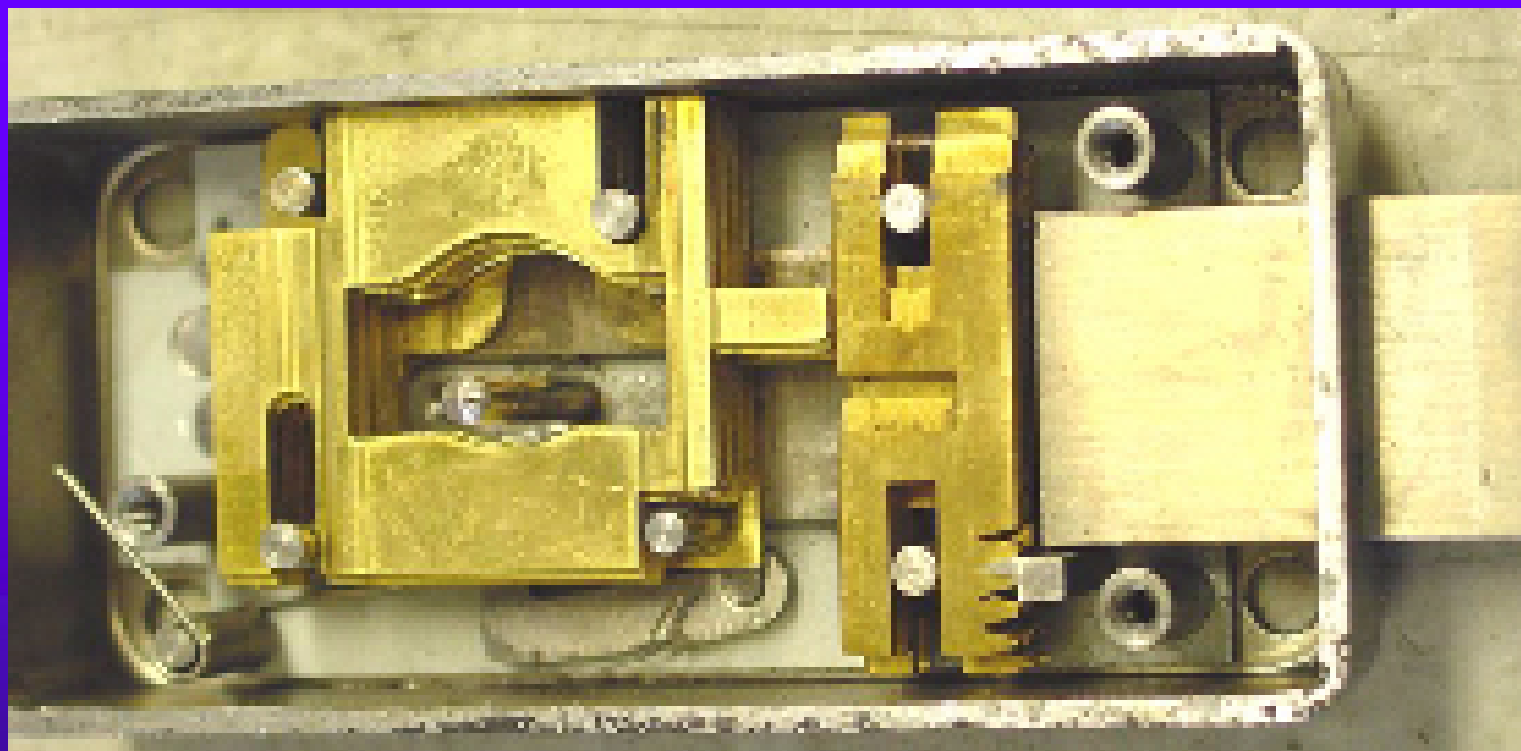
MODERN CHUBB LEVER



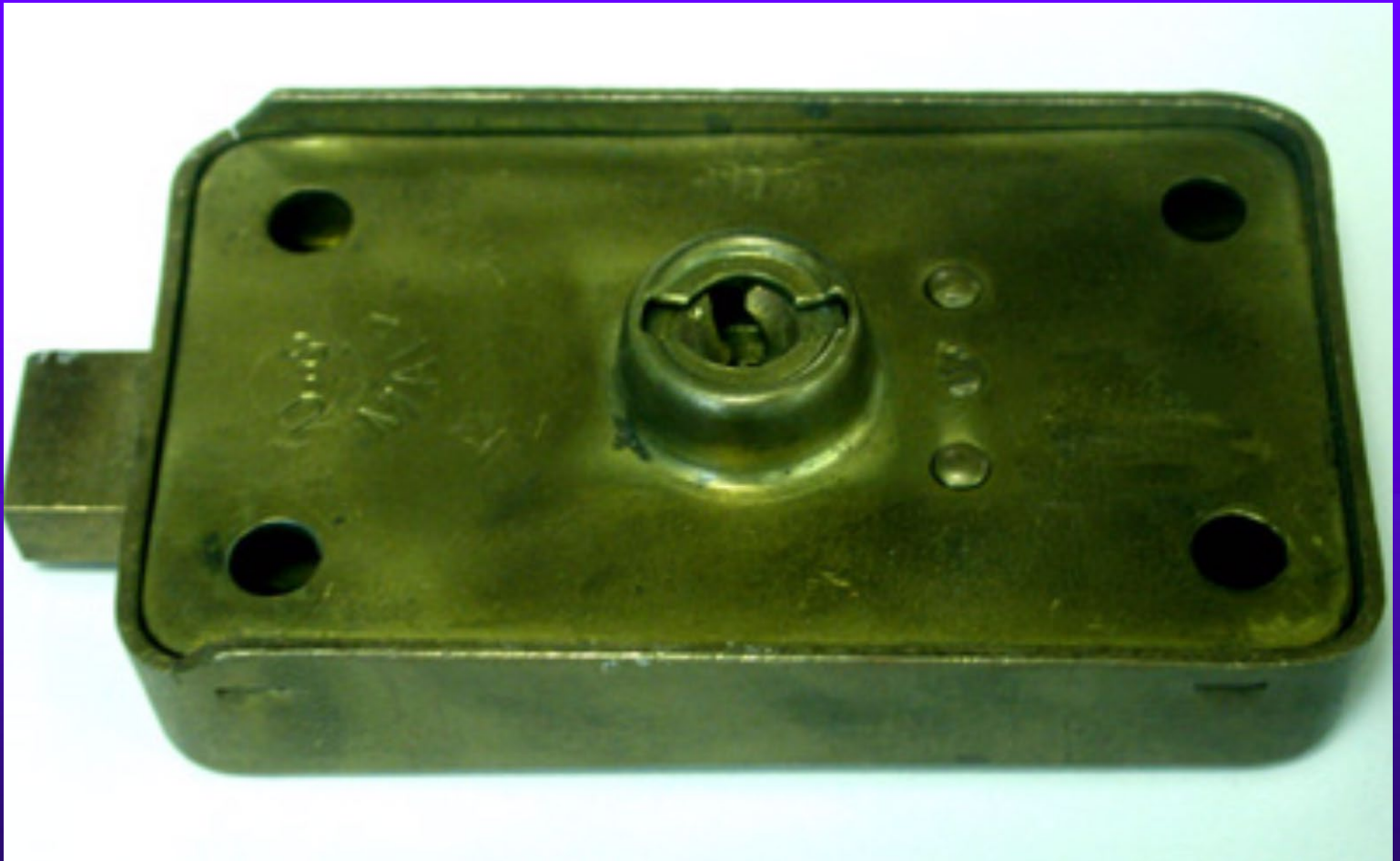
KROMER HIGH SECURITY



STUV LEVER LOCK



POST OFFICE LEVER LOCK



Lever Key Detail – Postal



Lever Detail – Postal



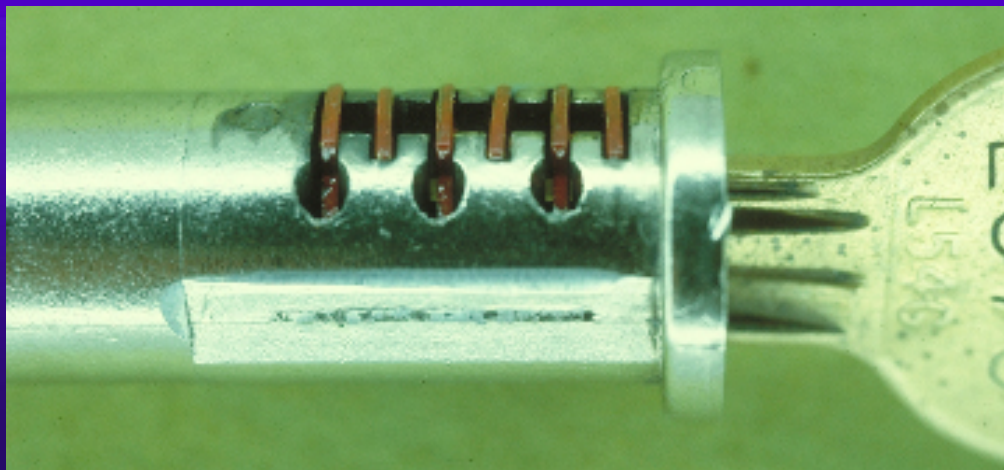
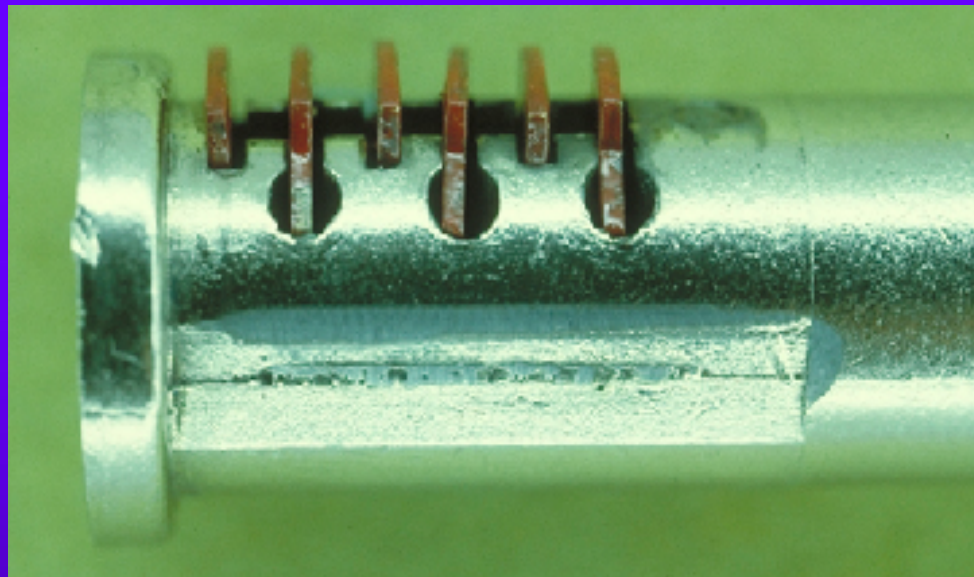
NAZI SUBMARINE LEVER LOCK





WAFER LOCK

WAFFER TUMBLER LOCK



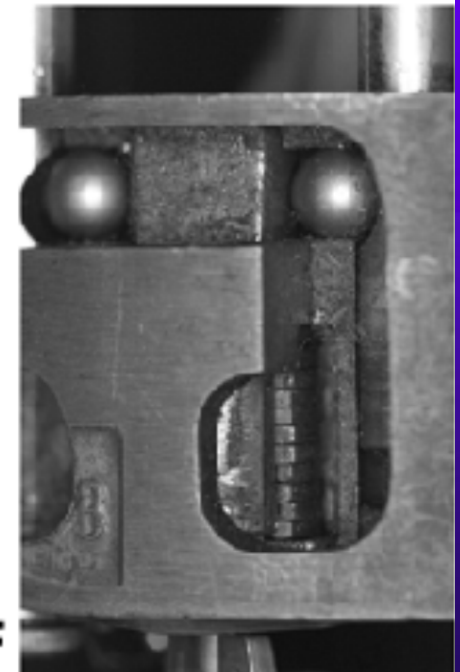
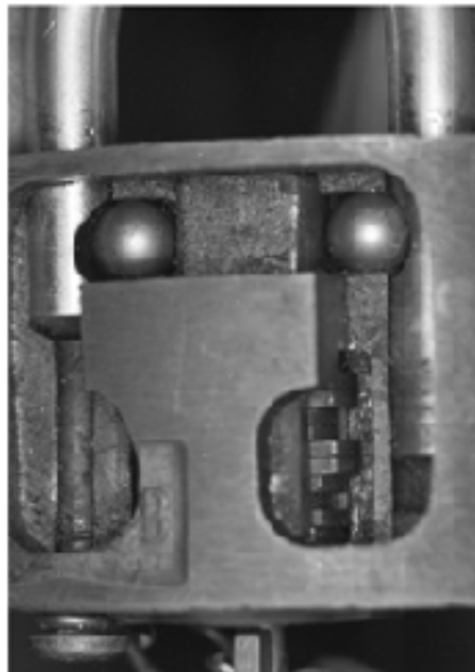
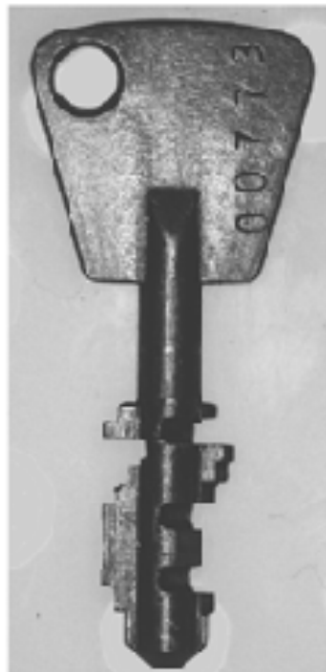
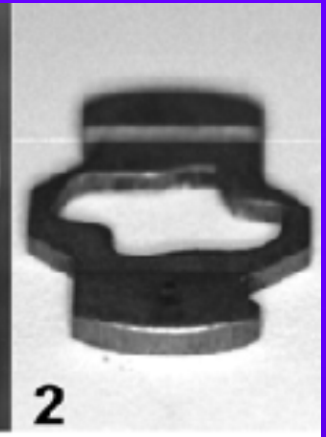
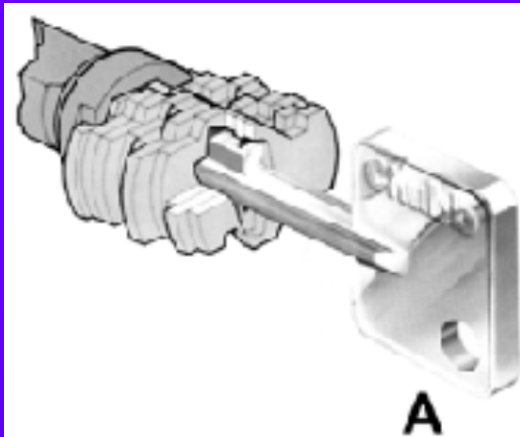
WAFER LOCK – LOCKED



WAFER LOCK – OPEN



CHUBB AVA WAFER





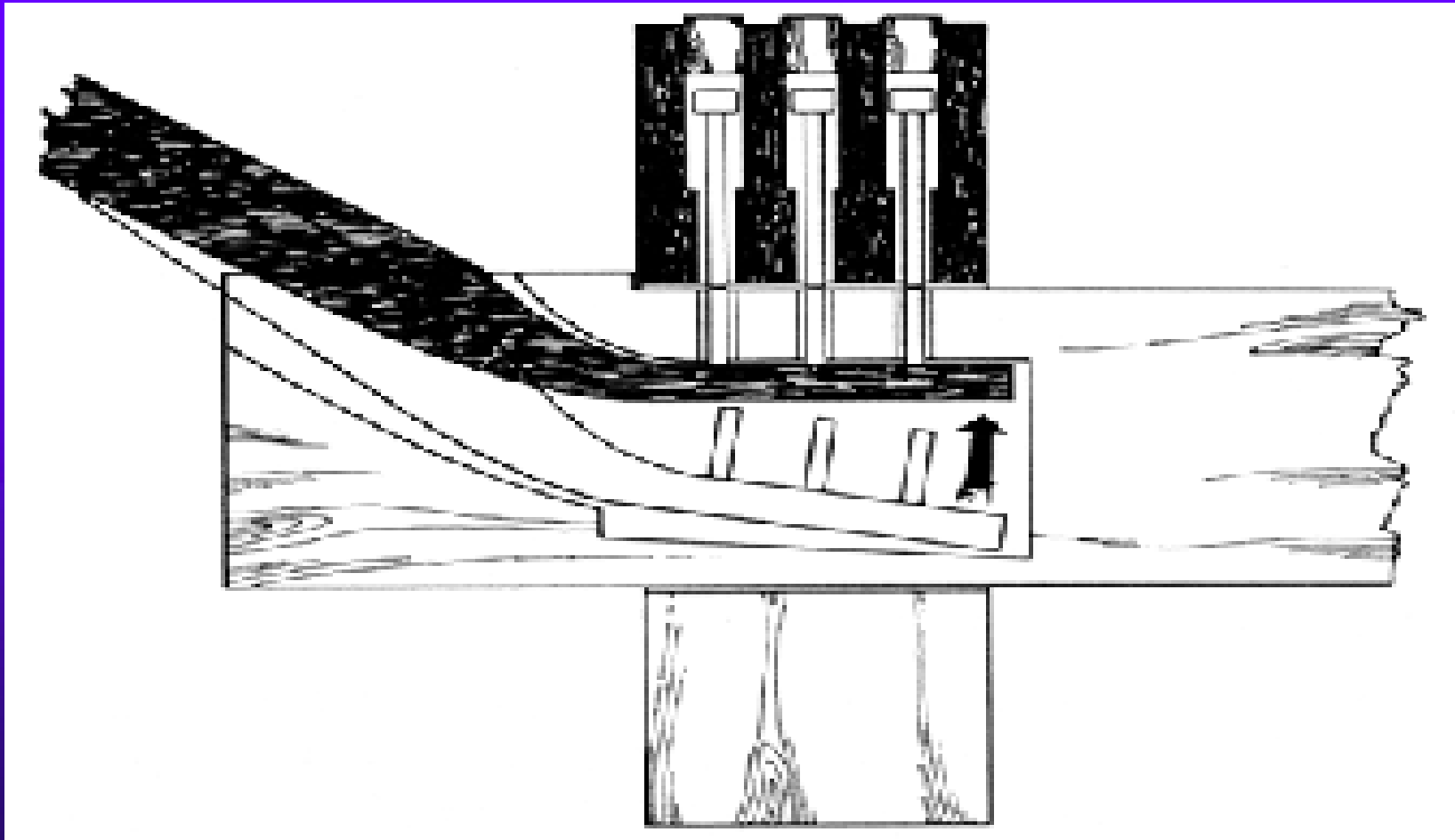
PIN TUMBLER LOCK



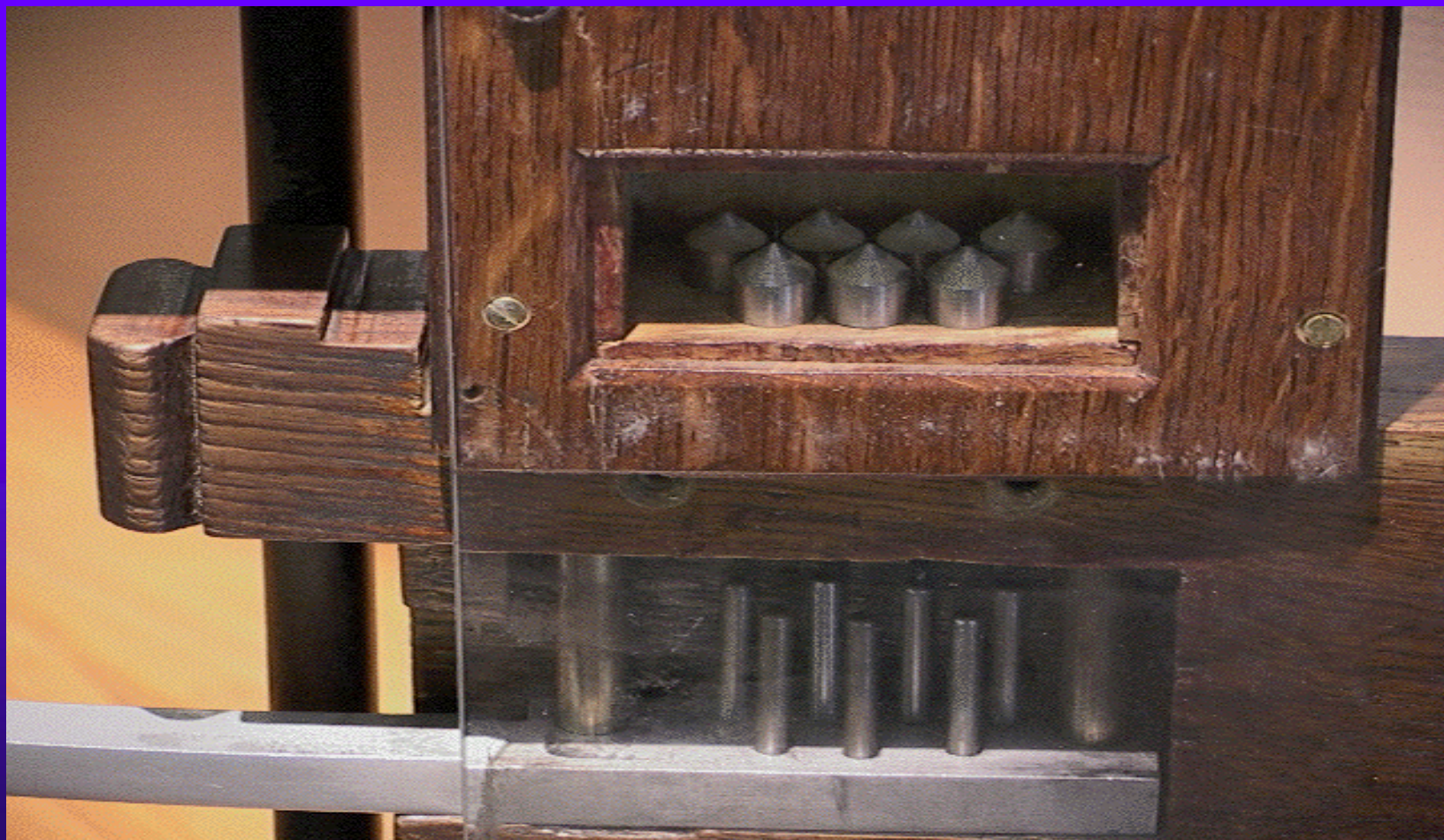
PIN TUMBLER LOCKS

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

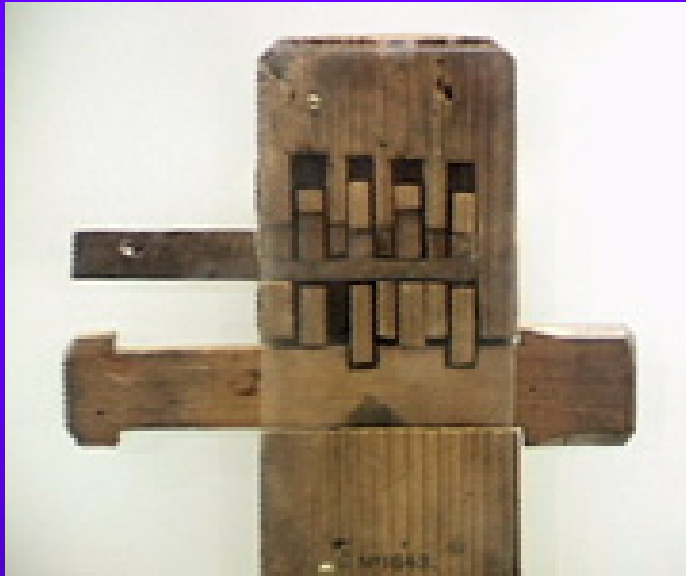
PIN TUMBLER – EGYPTIAN



EGYPTIAN DETAIL



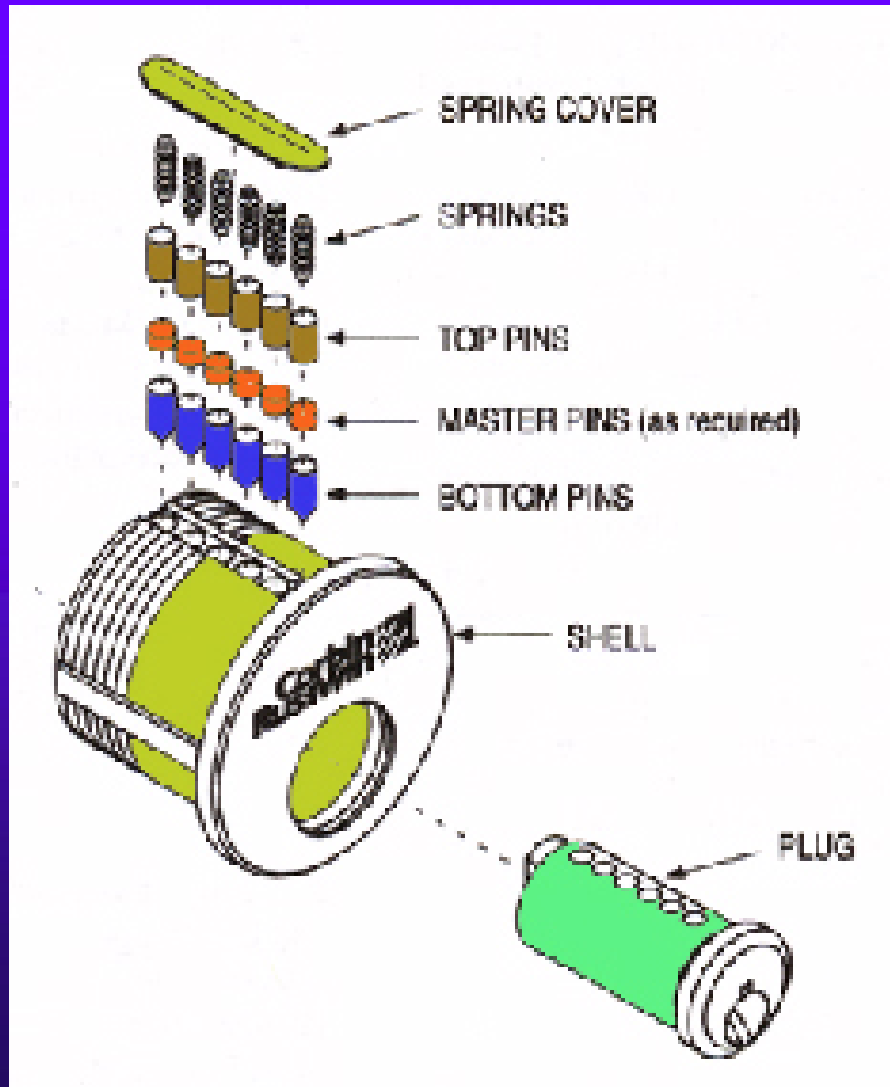
EGYPTIAN PIN TUMBLER



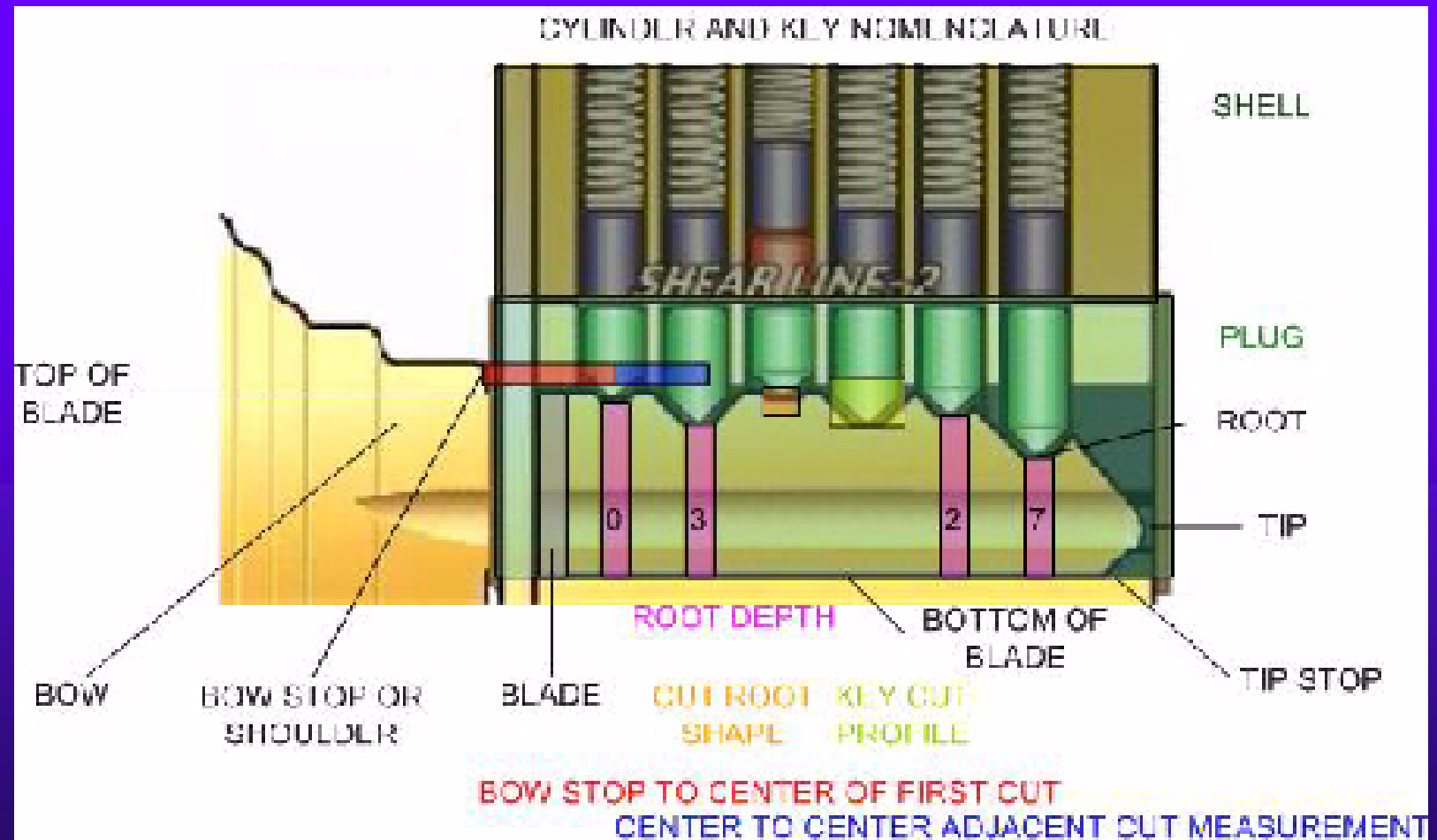


MODERN DESIGN

PIN TUMBLER DETAIL



PIN TUMBLER NOMENCLATURE



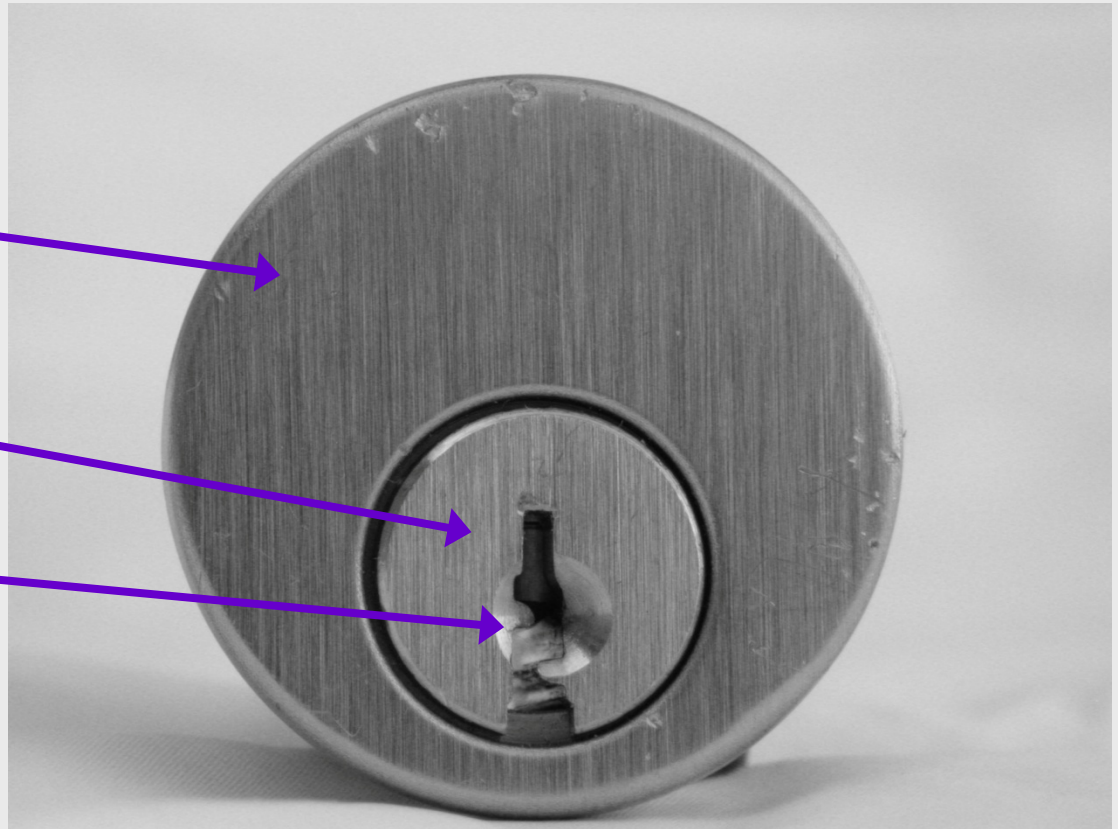
Pin Tumbler Lock



Shell

Plug

Keyway slot



Inside the Pin Tumbler Lock



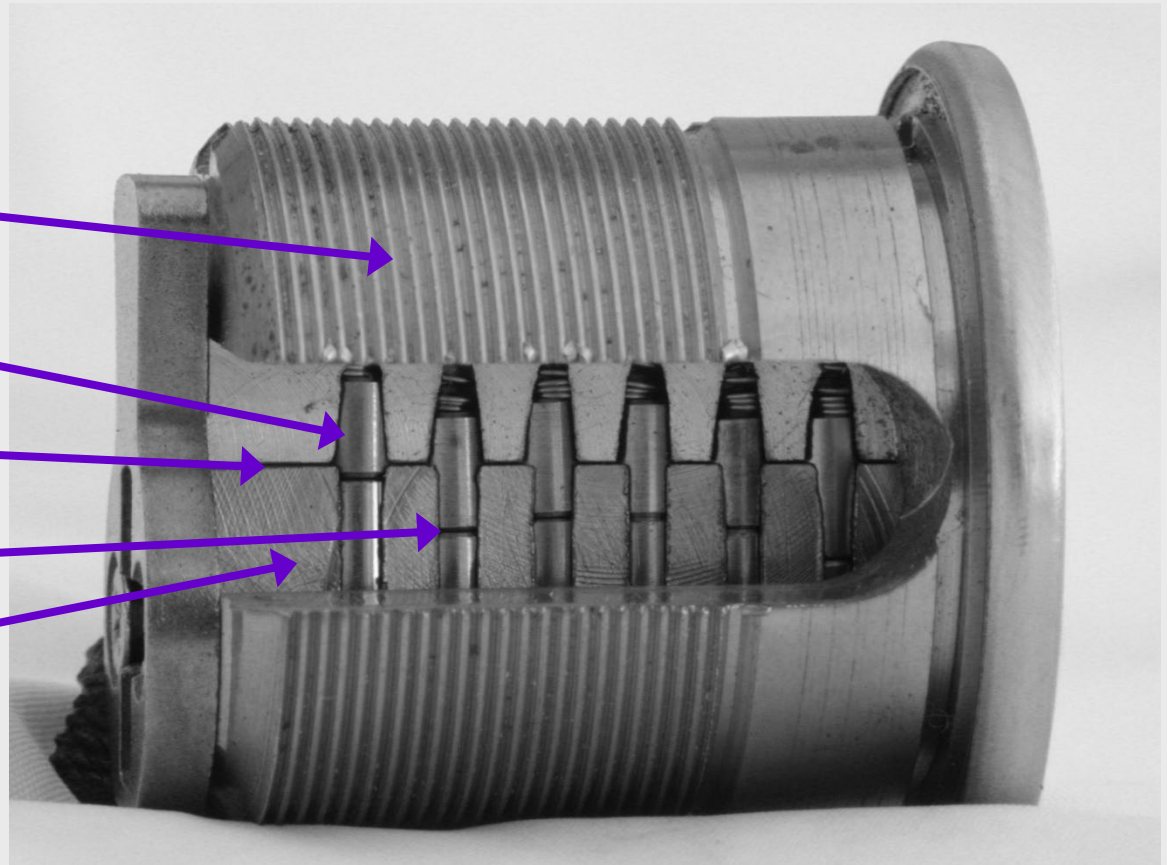
Shell

Pin stack

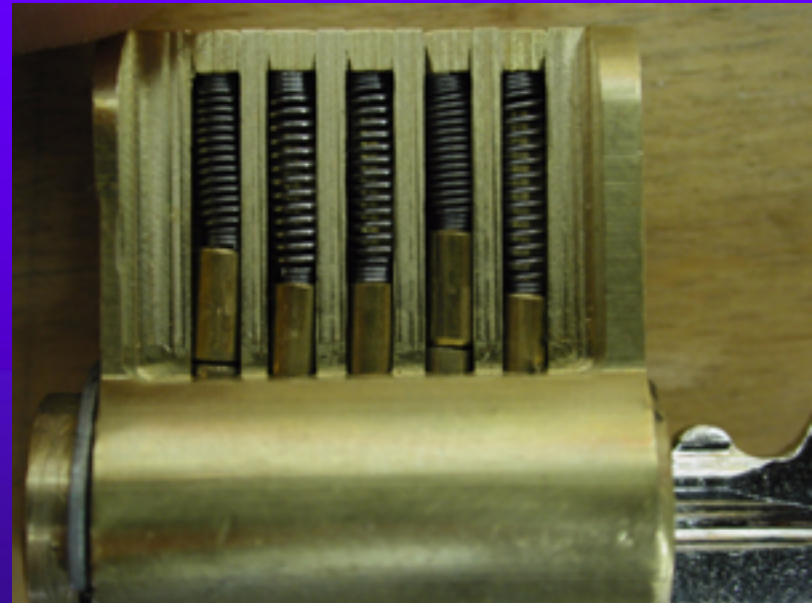
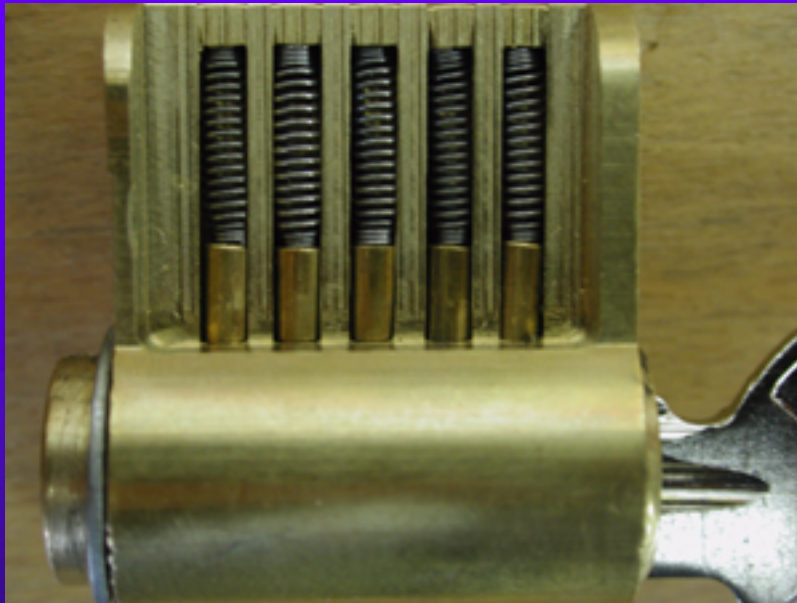
Shear line

Cut

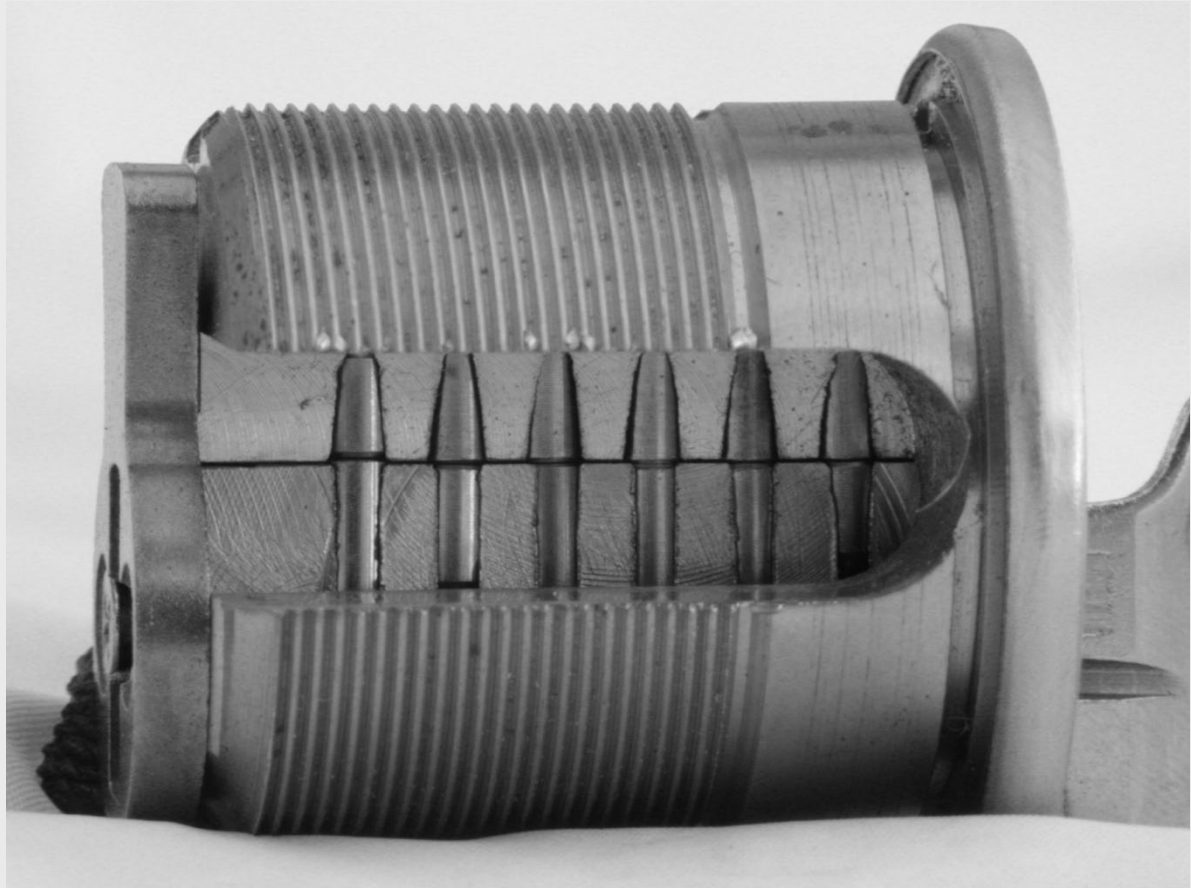
Plug



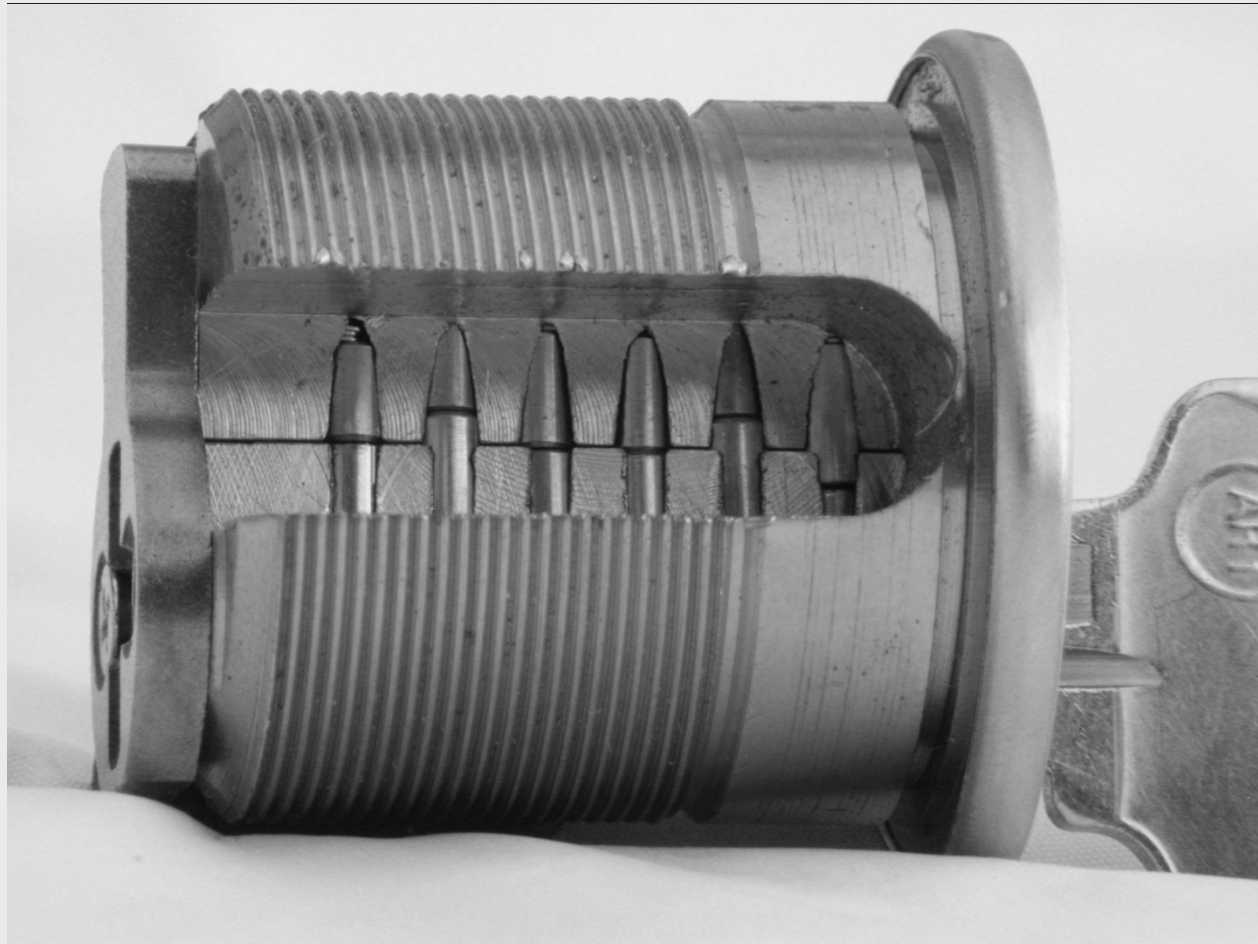
SHEAR LINE



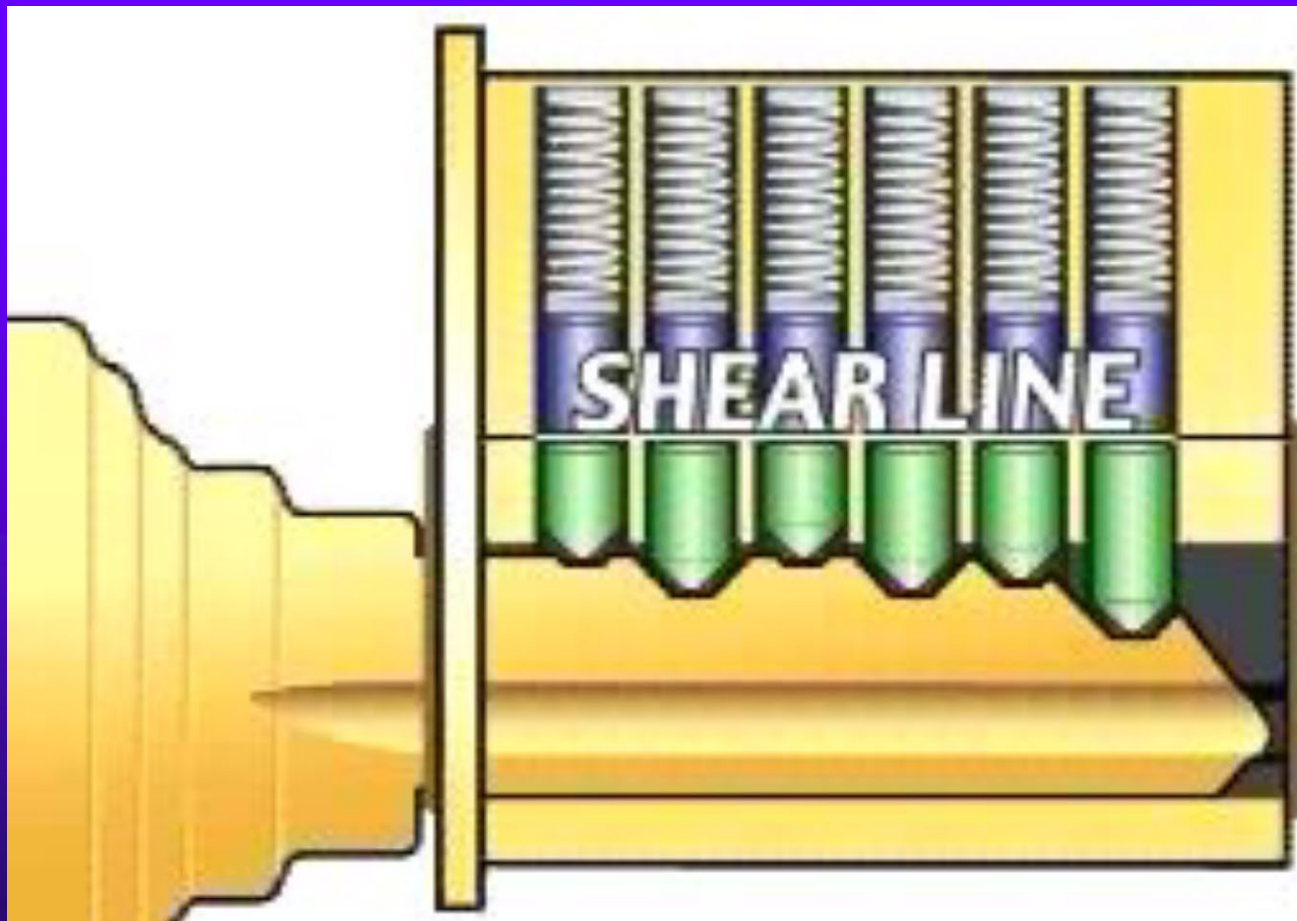
Correct Key Inserted



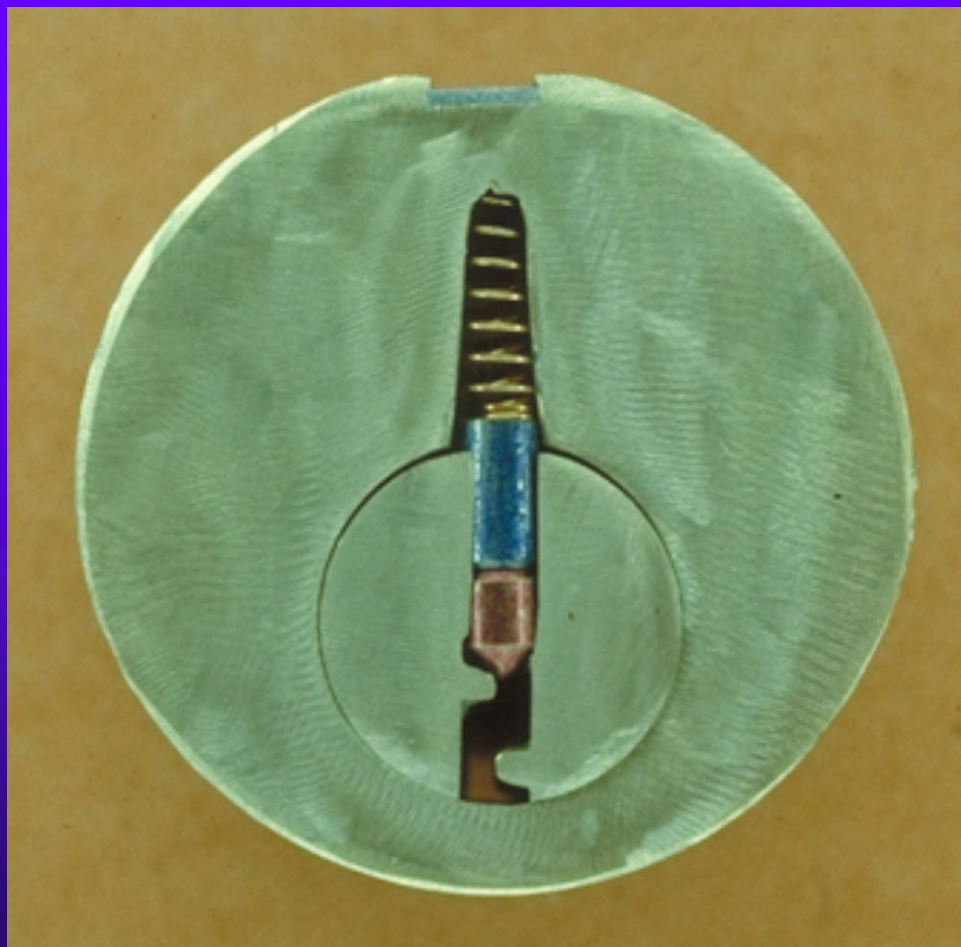
Incorrect Key Inserted



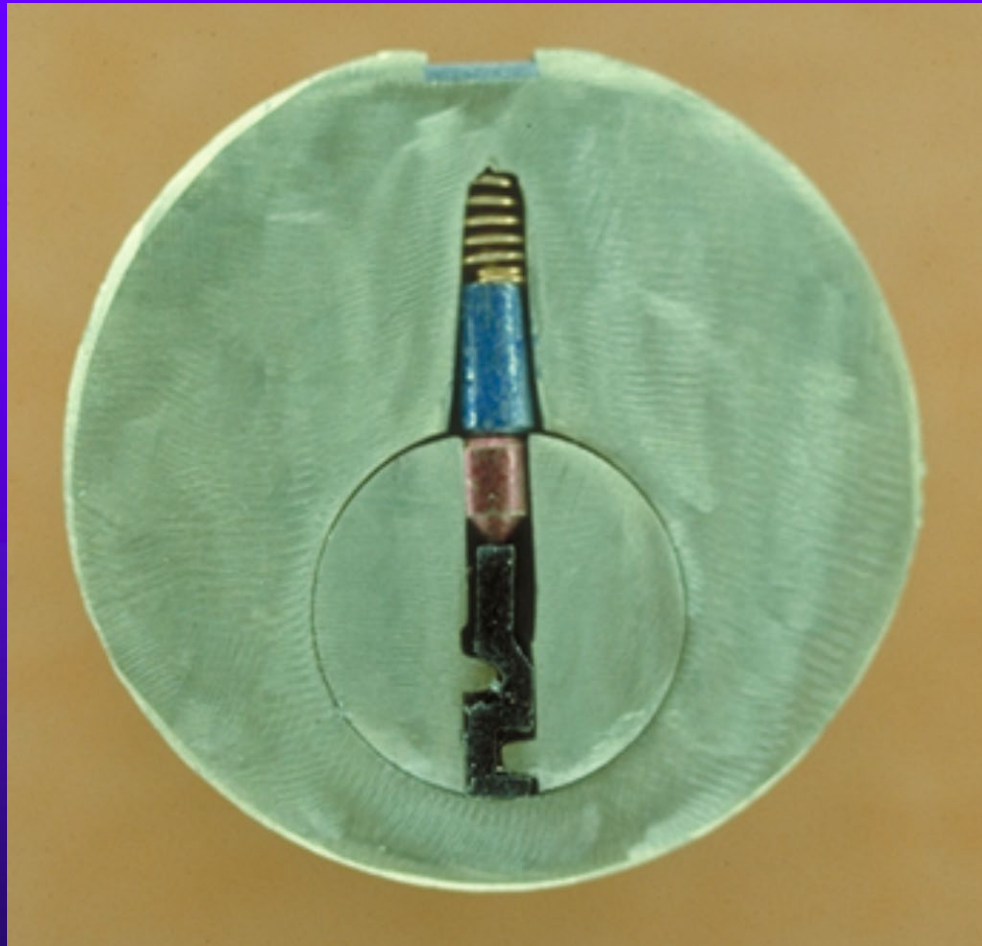
Shear Line



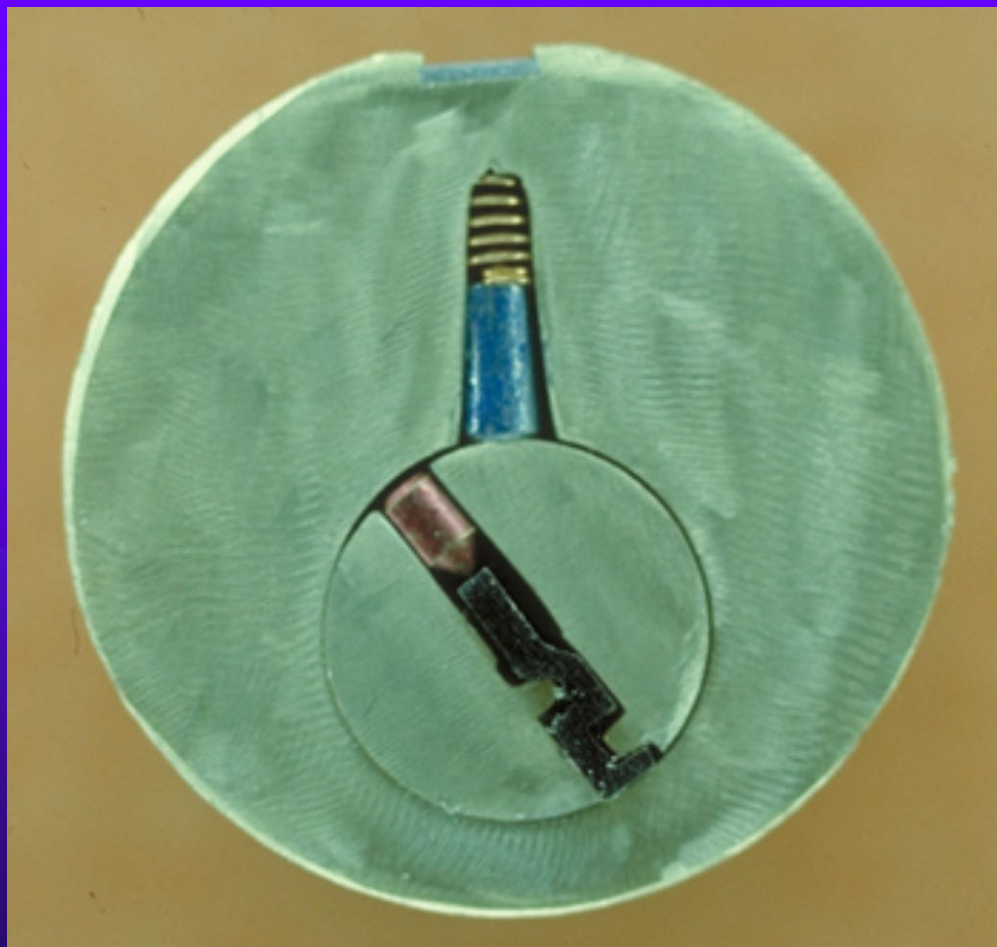
Locked



Pins at Shear Line



Plug Rotated





SECURITY TUMBLERS AND PICK RESISTANCE

PARACENTRIC KEYWAY



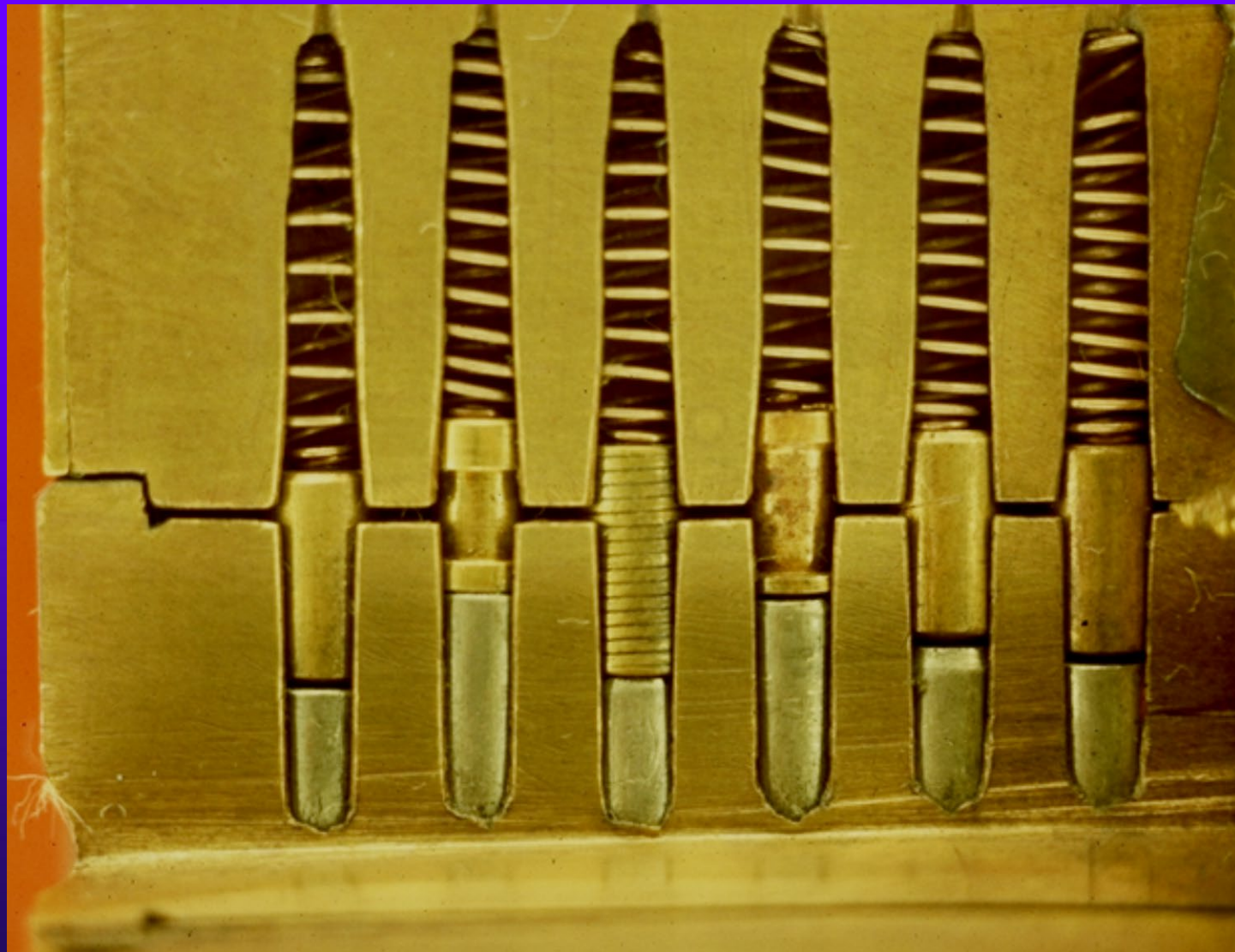
SECURITY TUMBLERS and PICK RESISTANCE



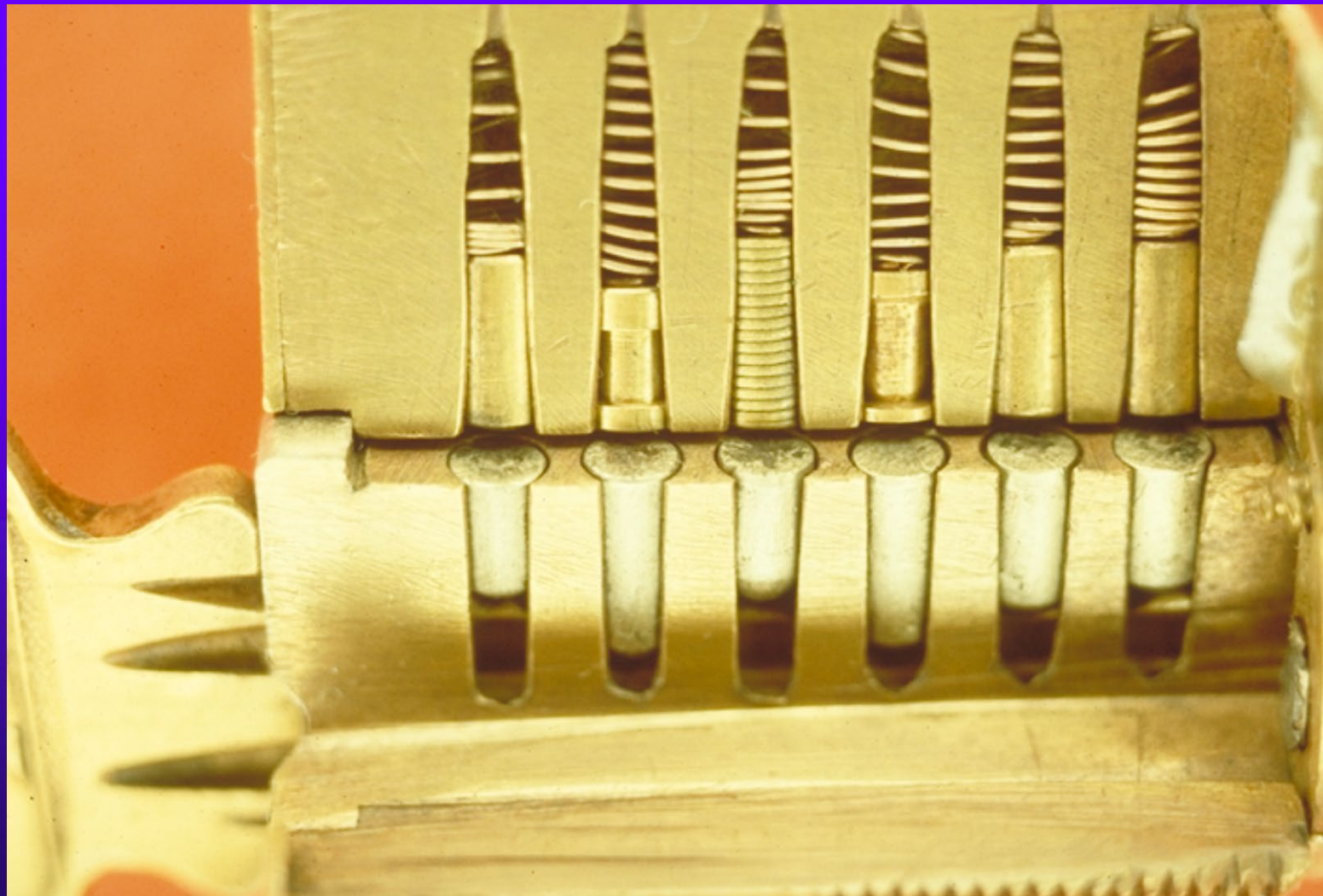
PLUG BLOCKED



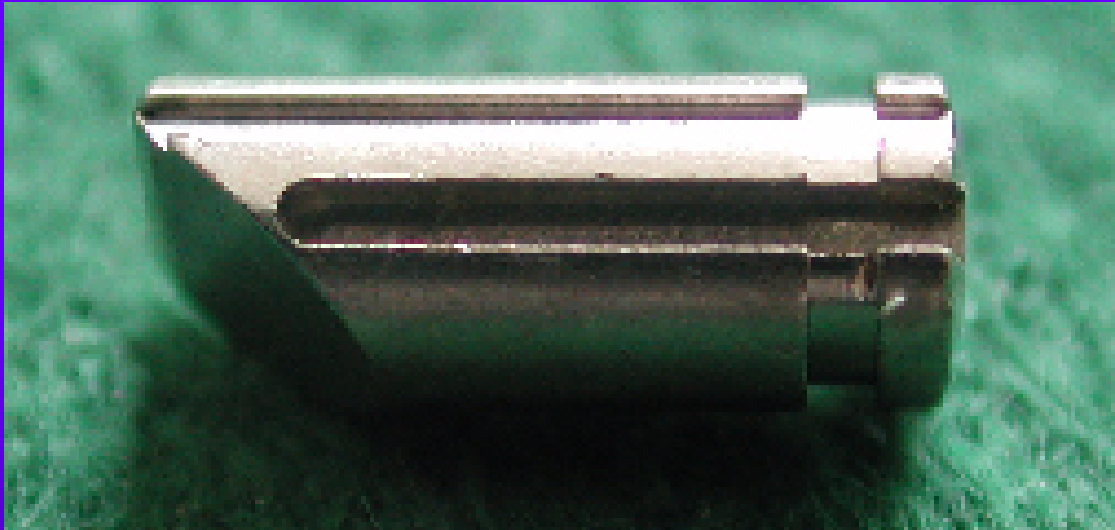
SECURITY PINS



SECURITY PIN DETAIL



MEDECO PINS

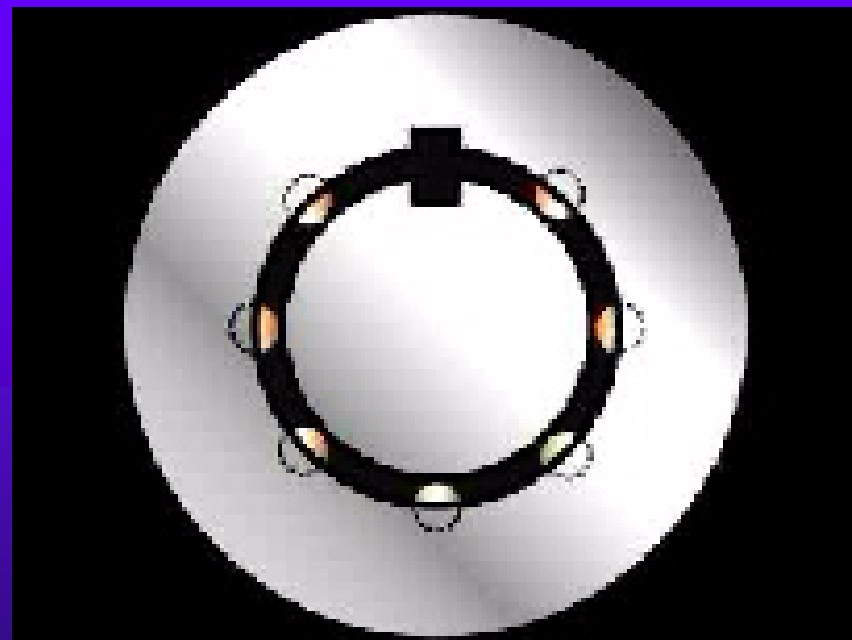




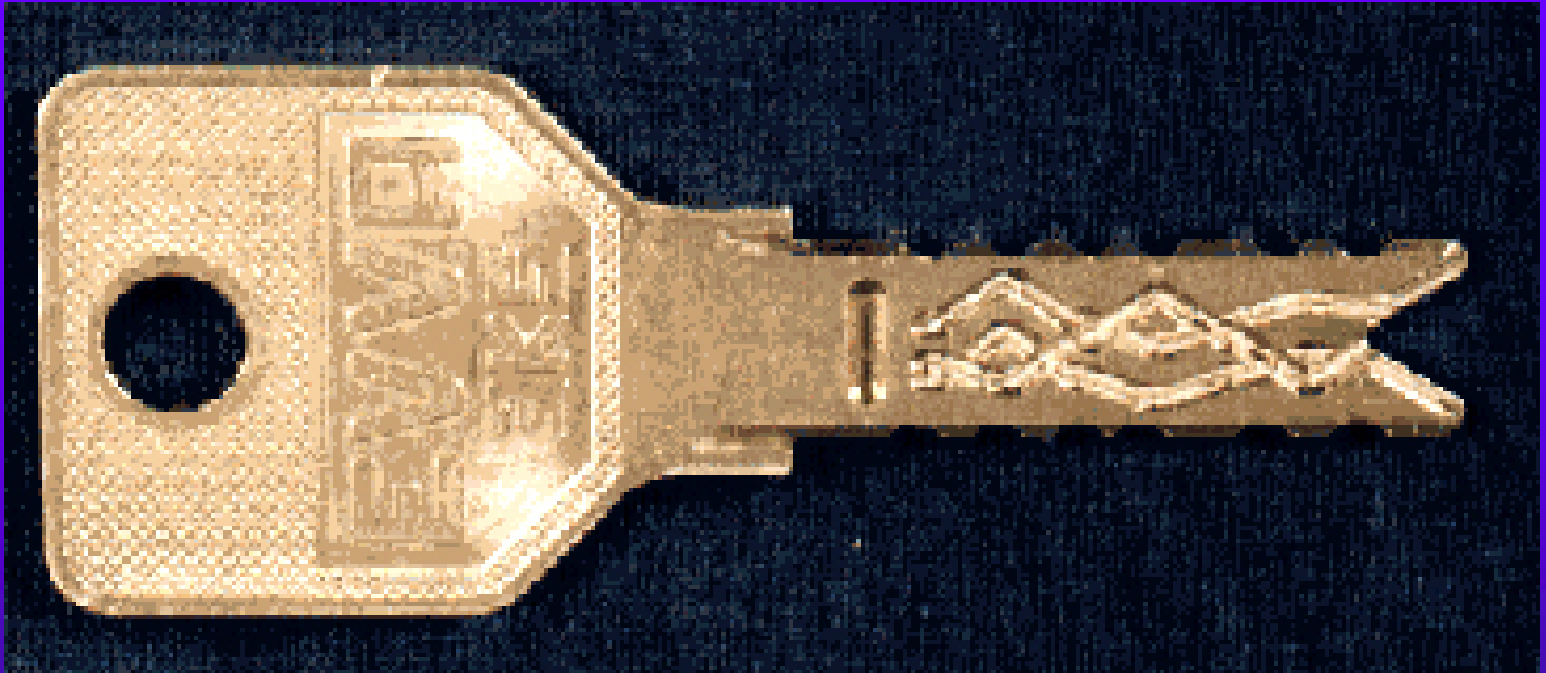
HYBRID LOCKS

- ◆ 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



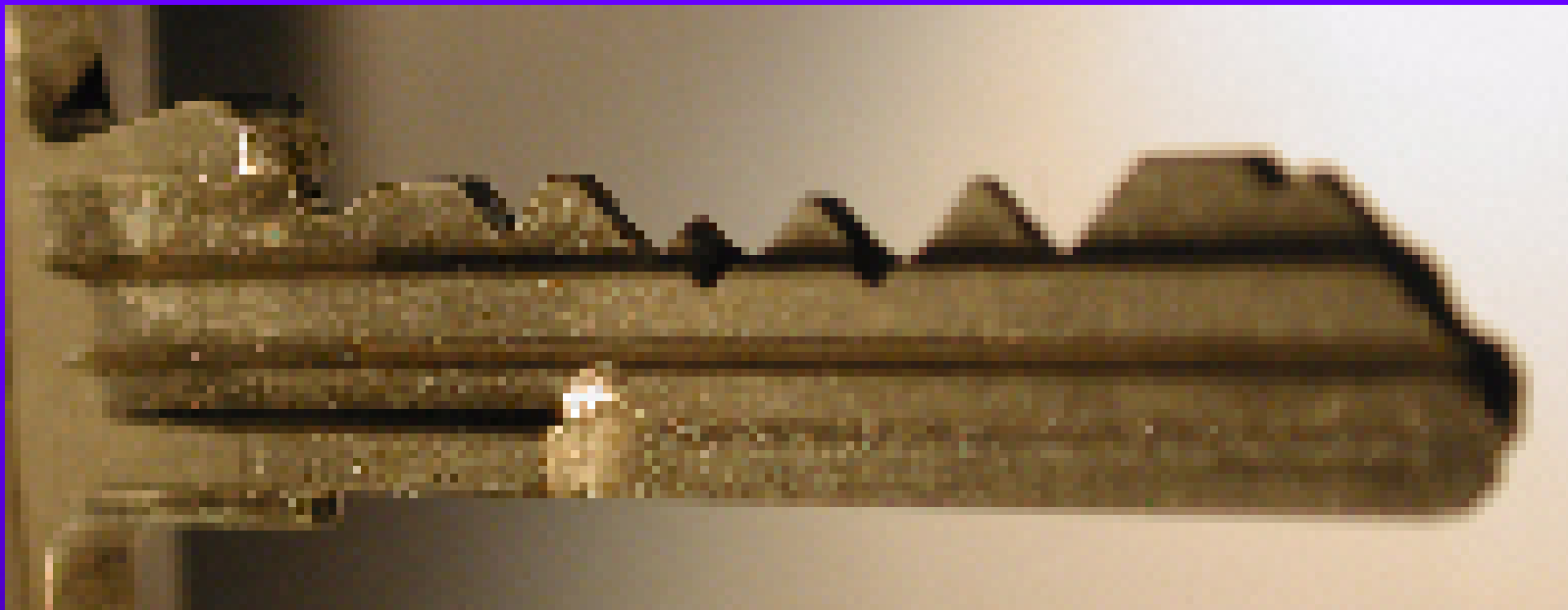
MEDECO Biaxial and Original

COMPARISON OF MEDECO ORIGINAL AND BIAxIAL DESIGNS

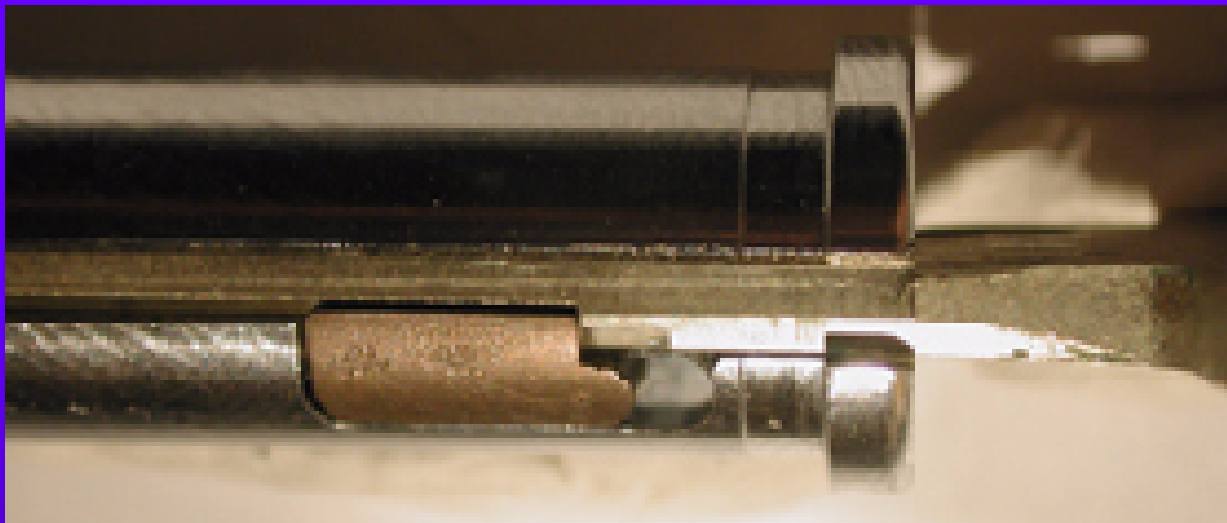
BIAXIAL
ORIGINAL



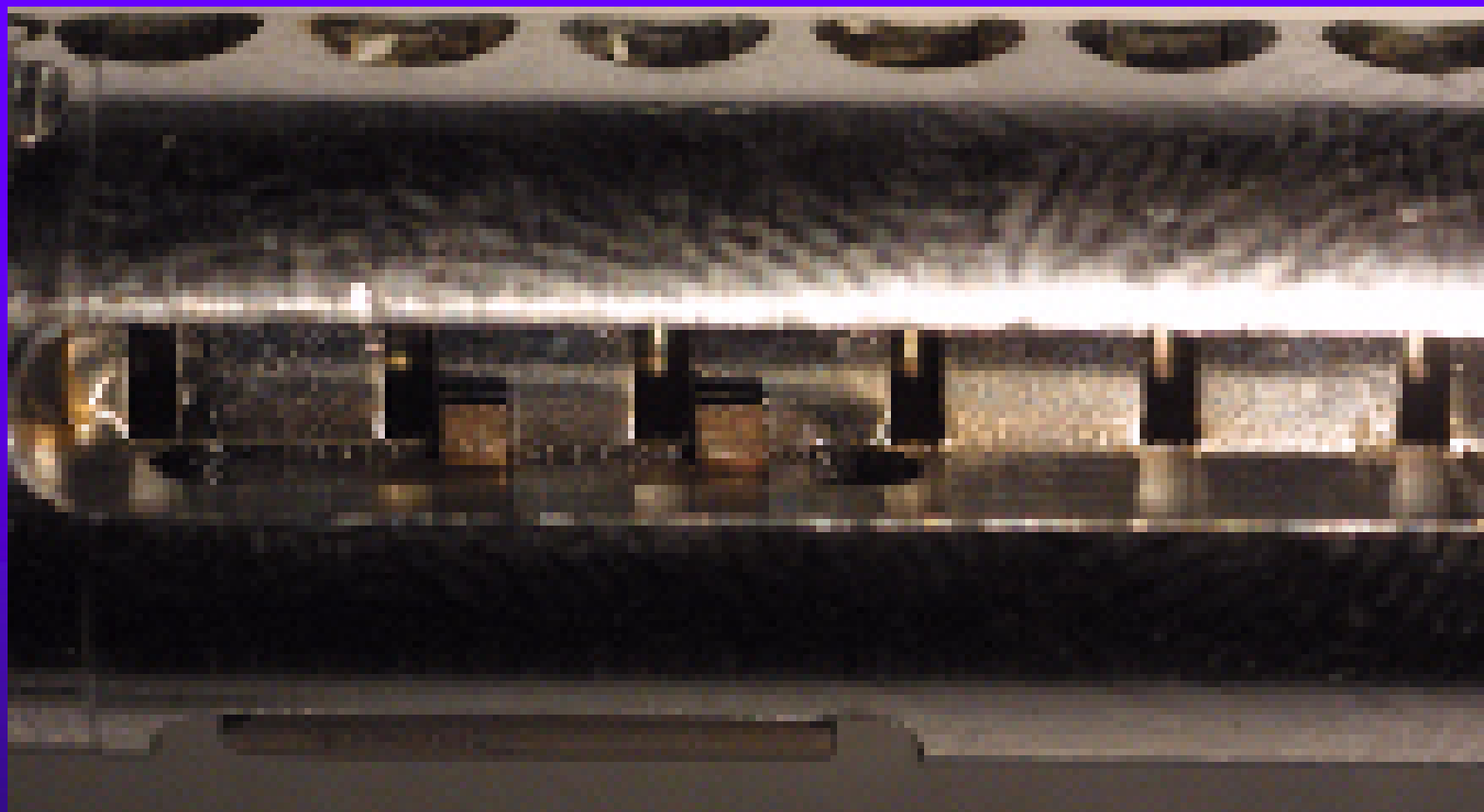
MEDECO M3



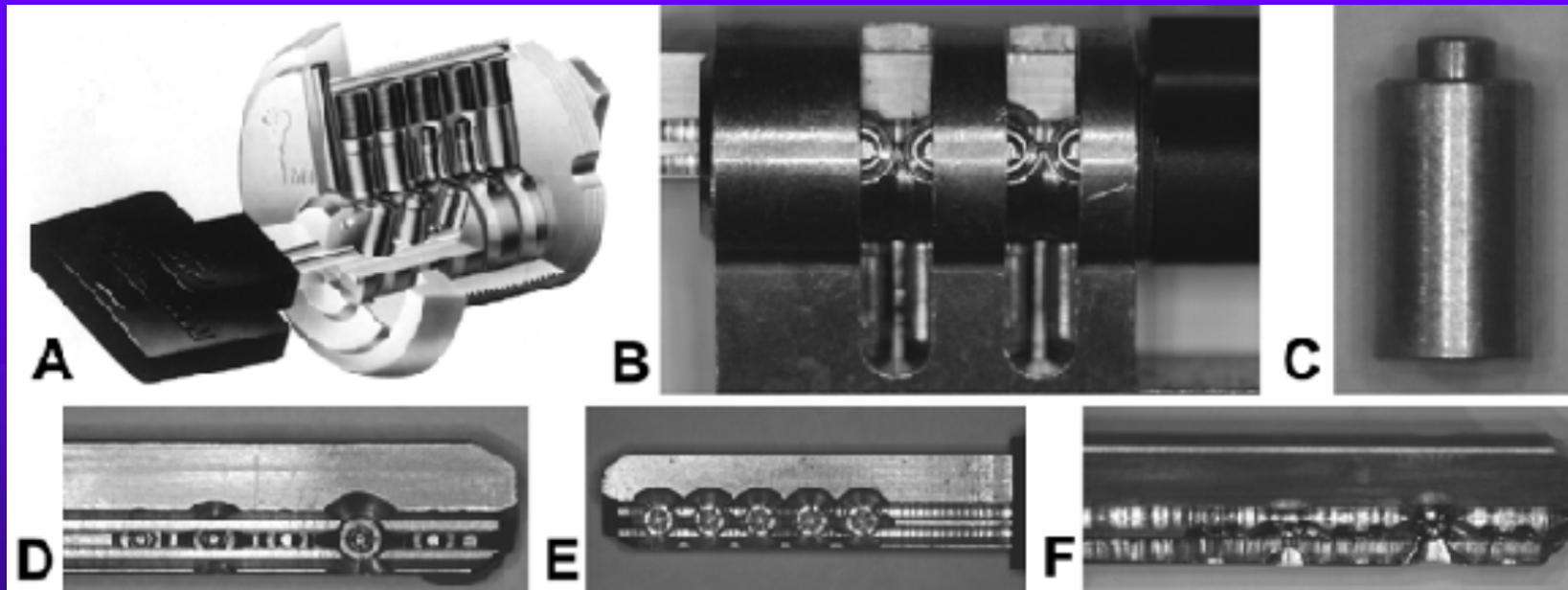
M3 SLIDER POSITIONS



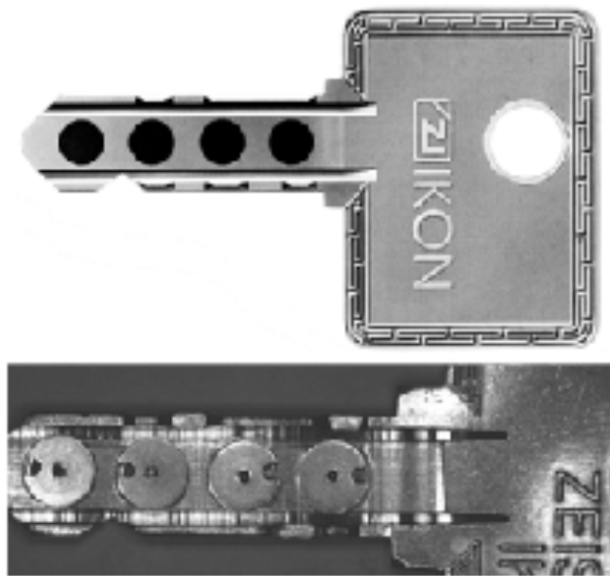
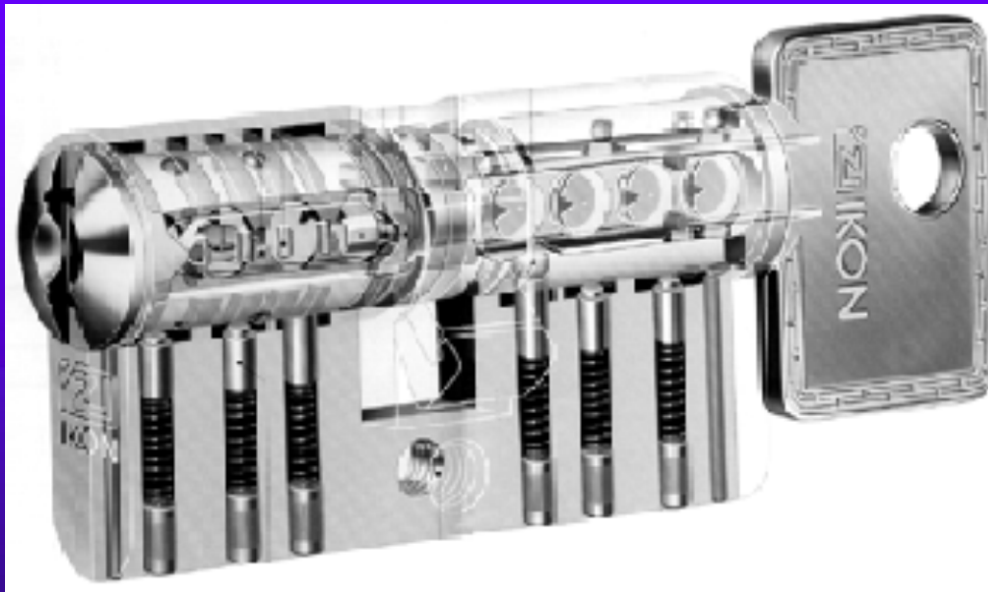
M3 SLIDER GATES



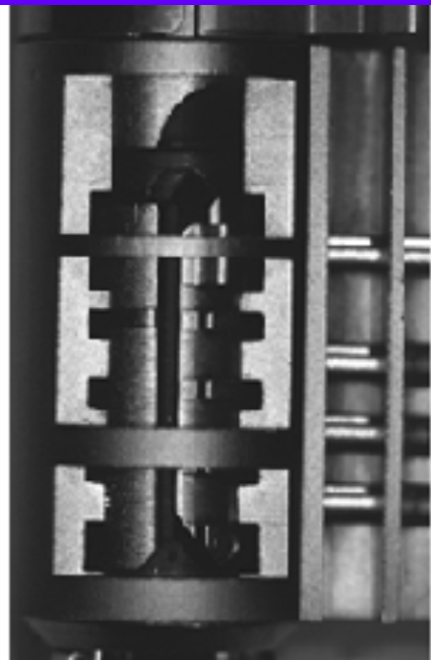
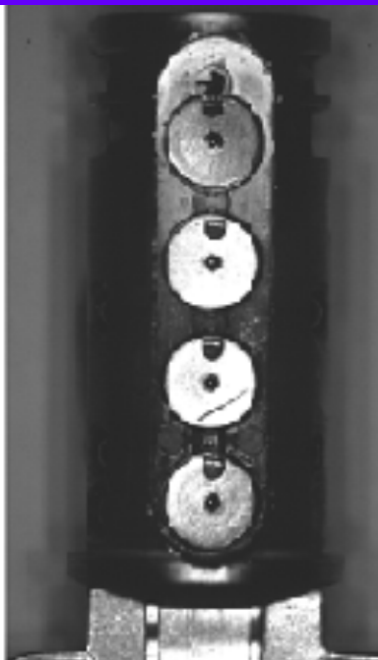
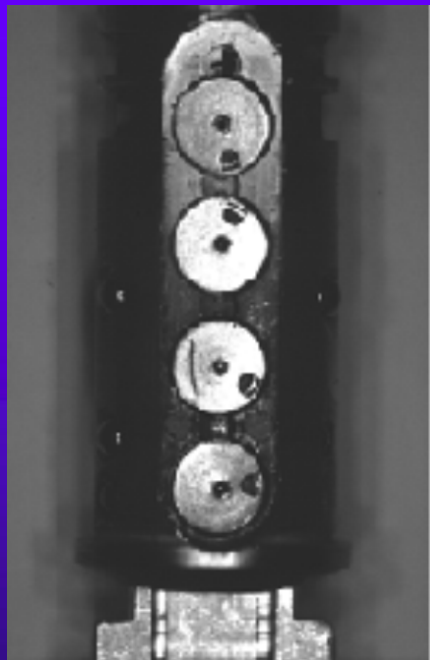
MUL-T-LOCK DIMPLE



MAGNETIC SIDEBAR



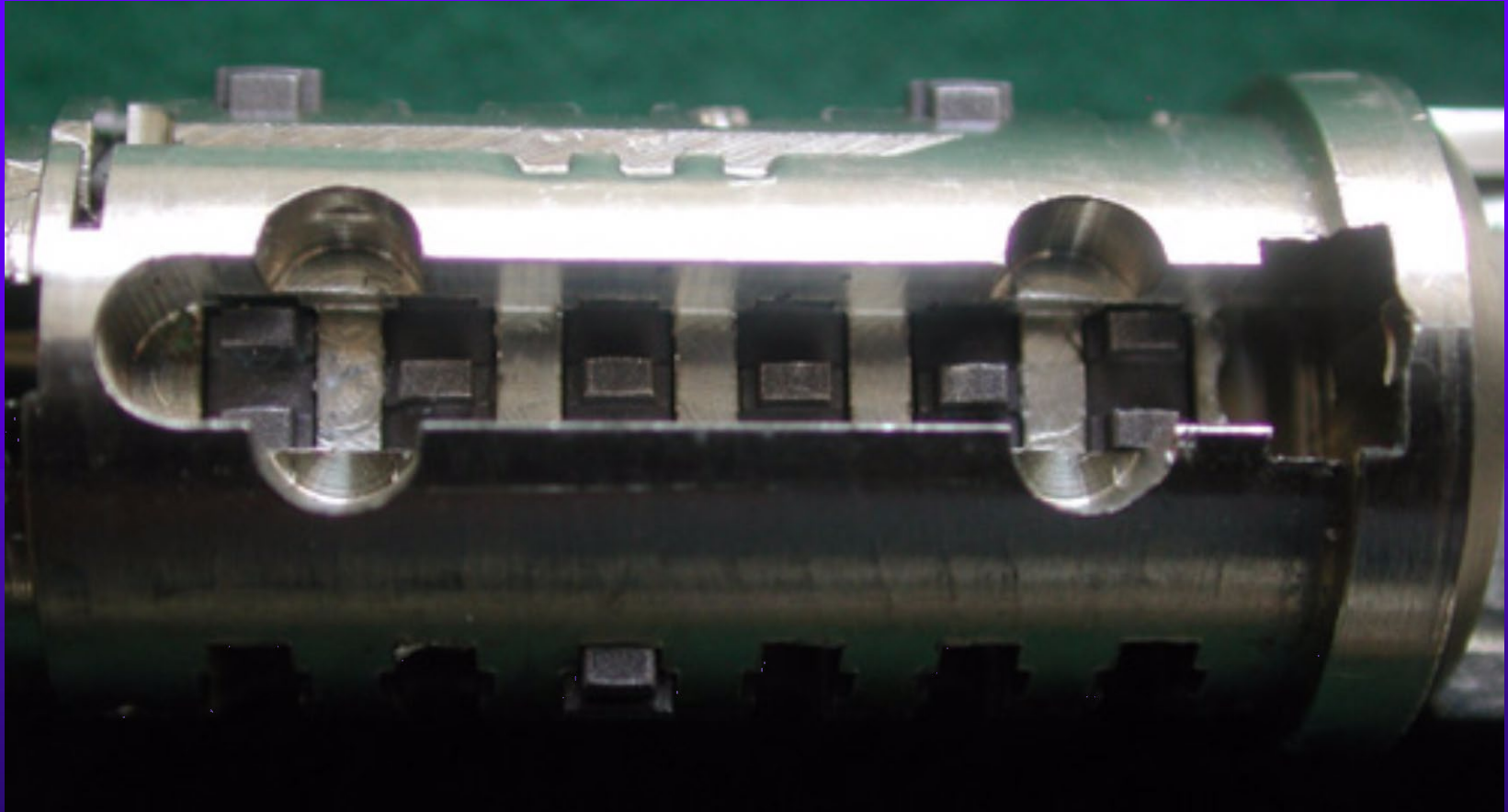
IKON Magnetic Detail



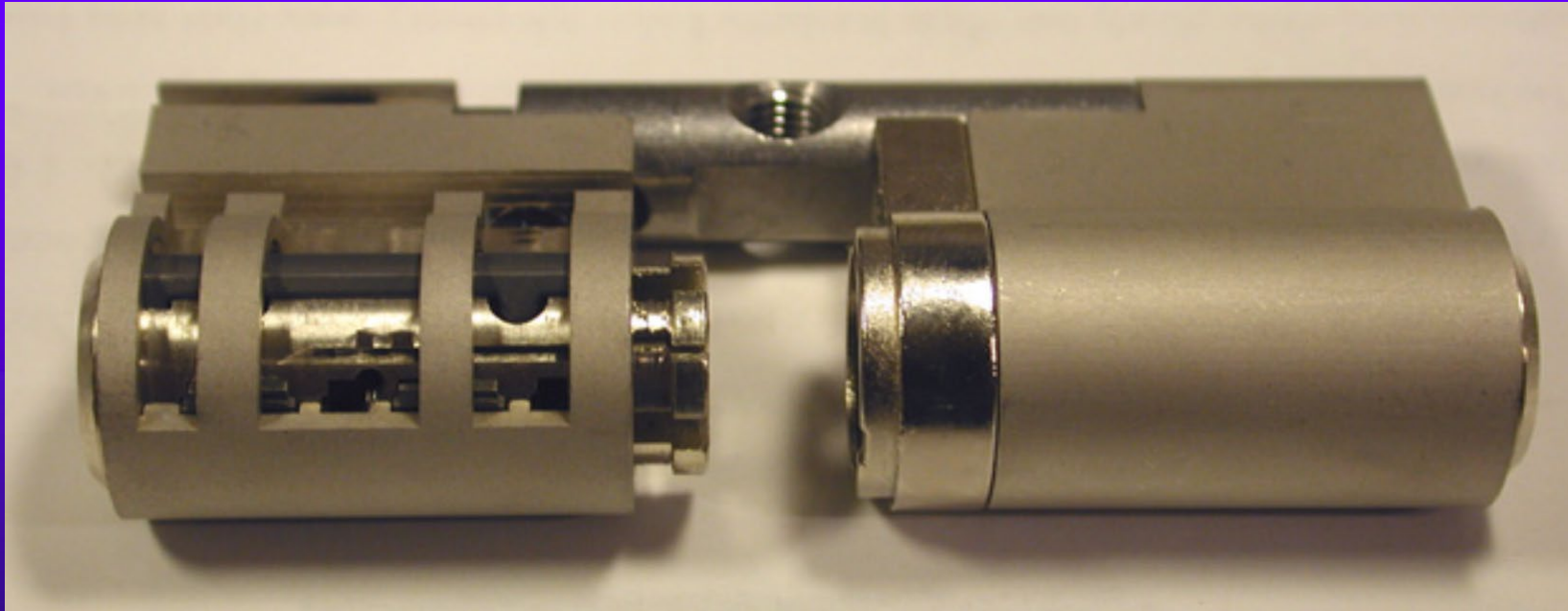
LASER TRACK – EVVA 3KS



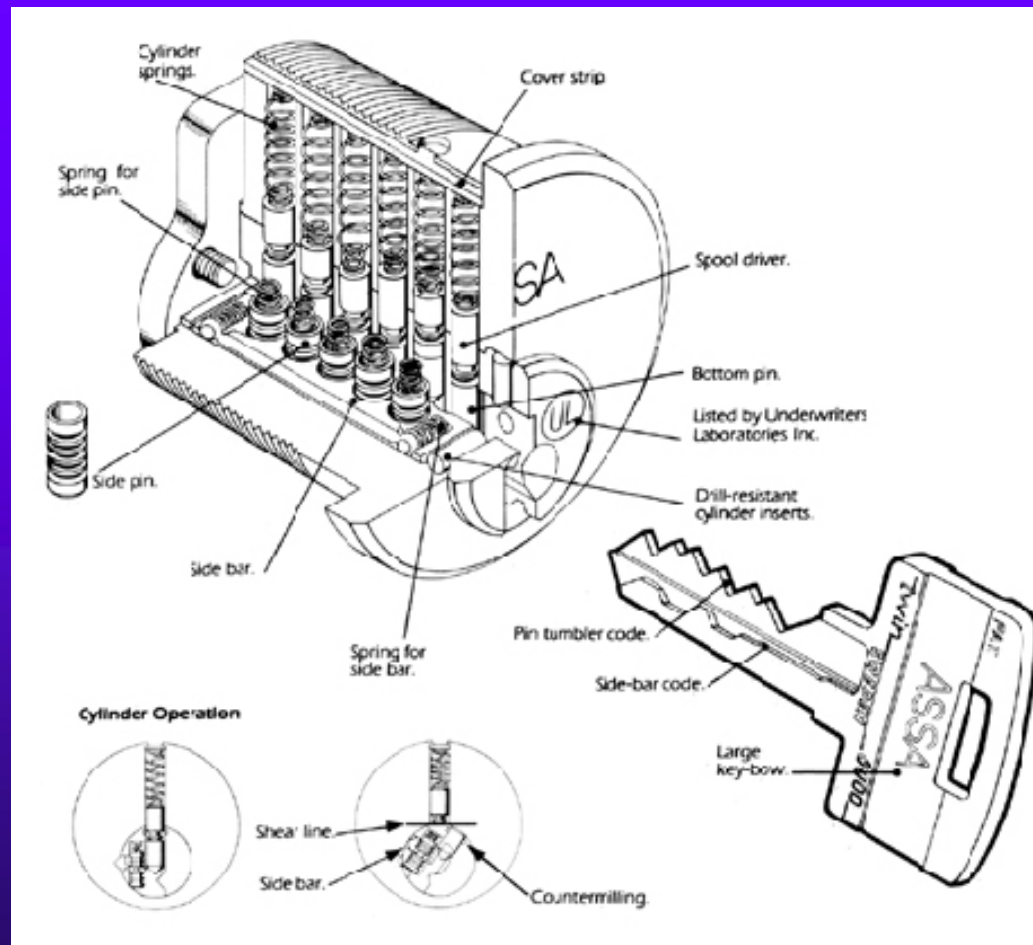
3KS Sidebar Locking Principle



3KS Locked Cylinder



ASSA SIDEBAR





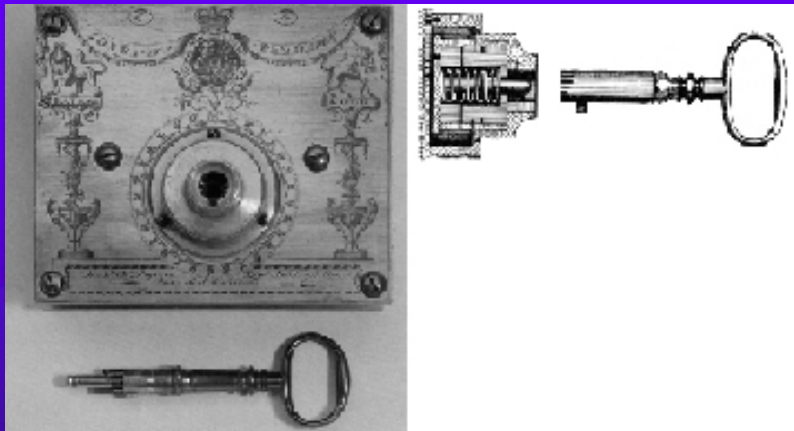
BYPASS OF LOCKS

BRAMAH: 124 PICADILLY, LONDON

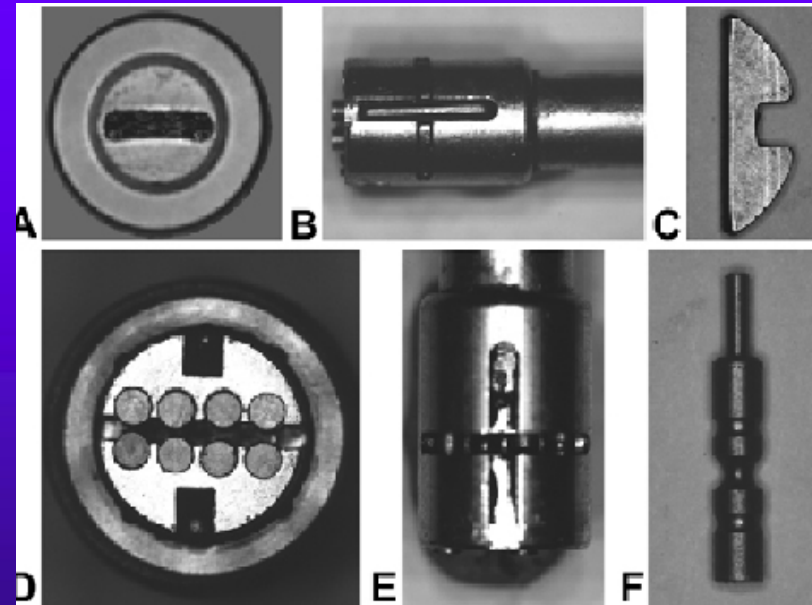
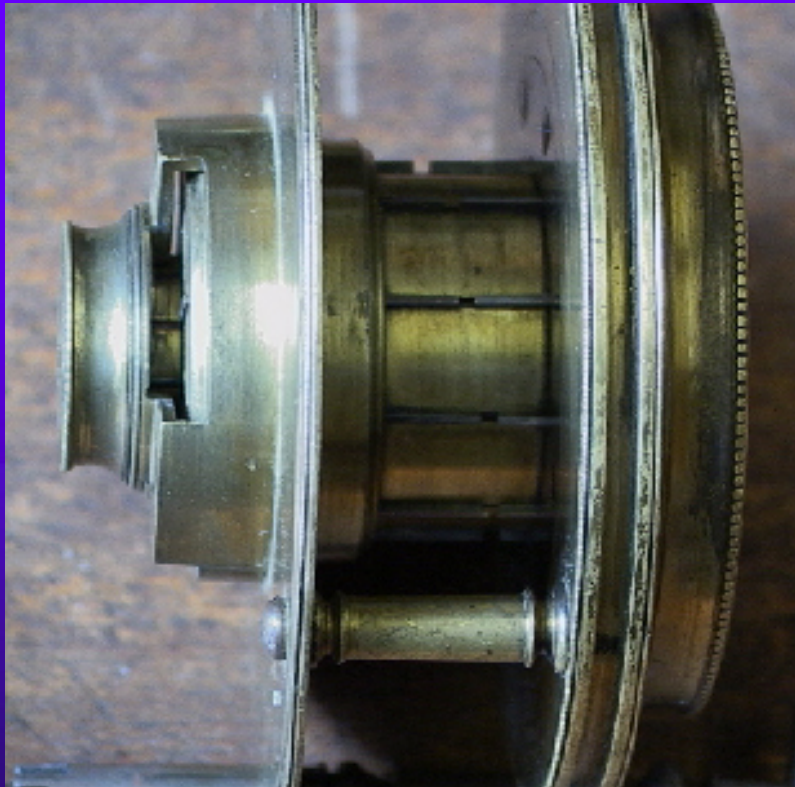
- ◆ 1851: The Great
Exposition in London



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
- ◆ Mechanical Bypass



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



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



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
- ◆ Plasticine reading
- ◆ Auto impressioning using foil
- ◆ Tryout keys
- ◆ Shim wire decoding
- ◆ Radioscopy
- ◆ Borescope
- ◆ Magnetic bypass

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

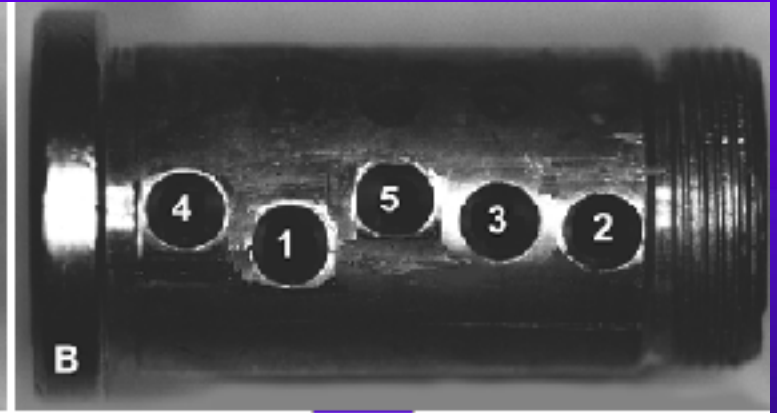
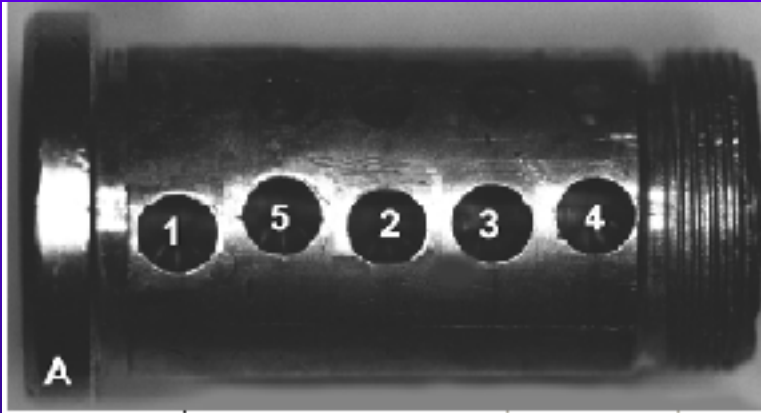
- ◆ Rocking with computer picks
- ◆ Pick guns
- ◆ Special pick and decode tools
- ◆ Cross keys
- ◆ Electronic signature analysis
- ◆ TMK Extrapolation



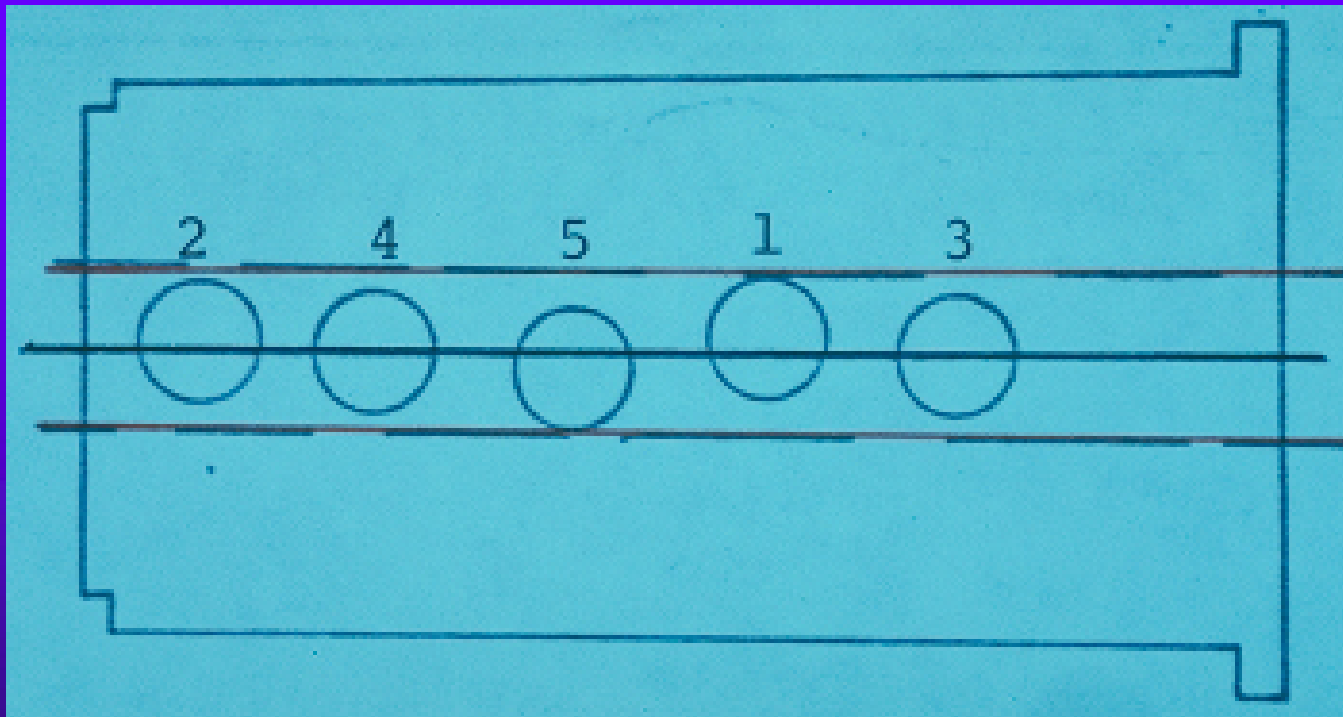
PICKING PIN TUMBLER LOCKS

PICKING TOOLS

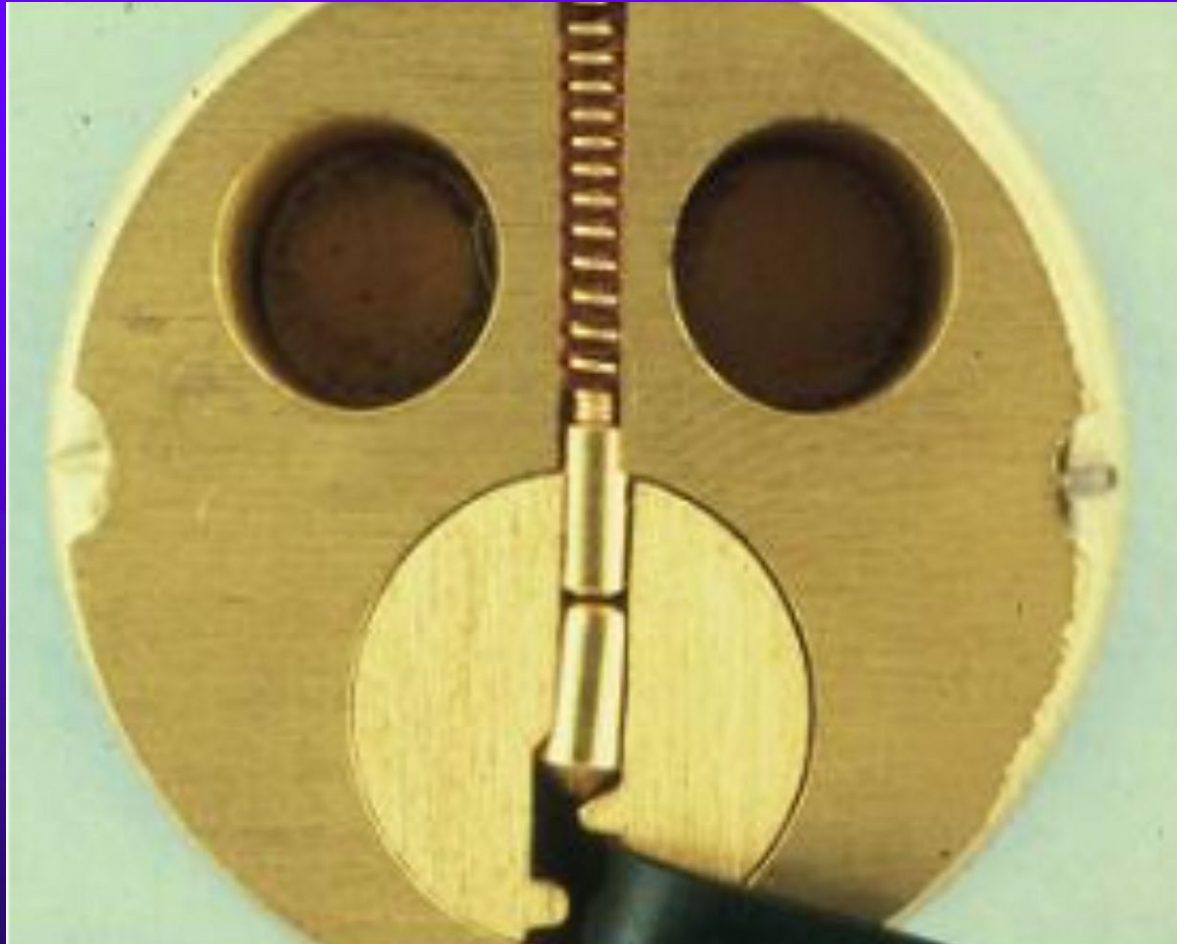
◆ What is Picking?



Order of Picking



PICKING A CYLINDER APPLY TENSION



Move Pins with Pick

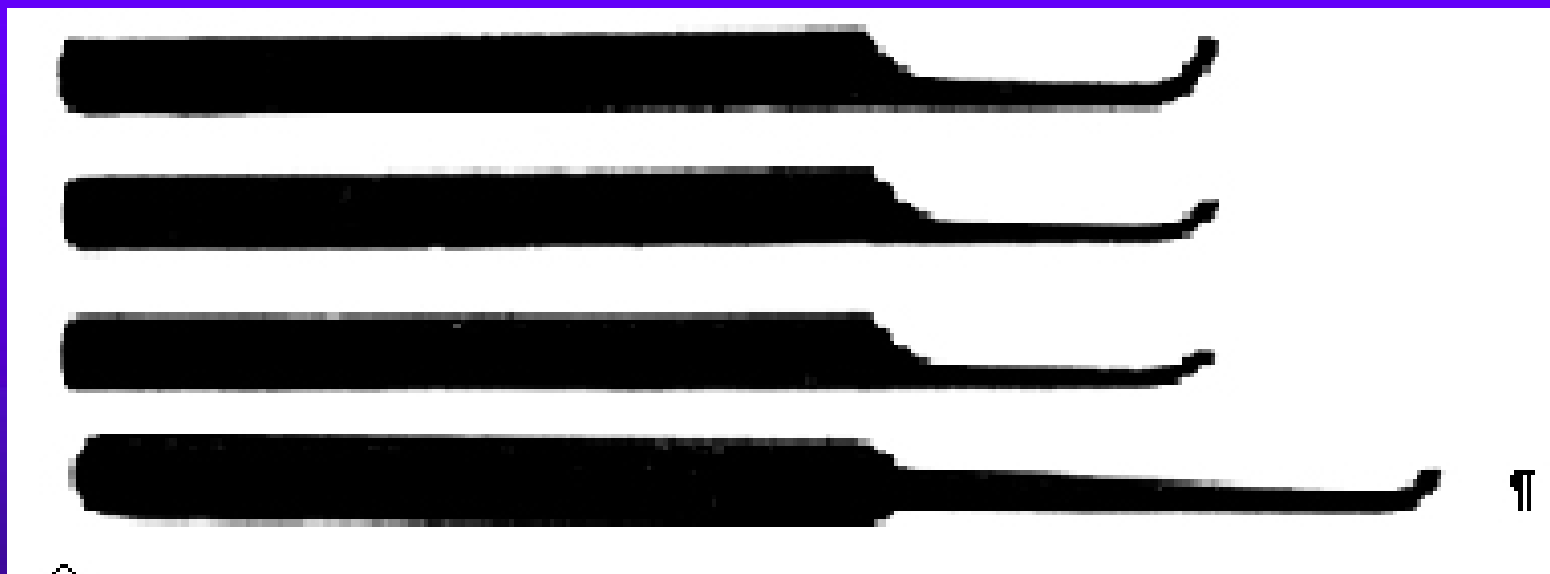


BASIC PICKS





More Picks

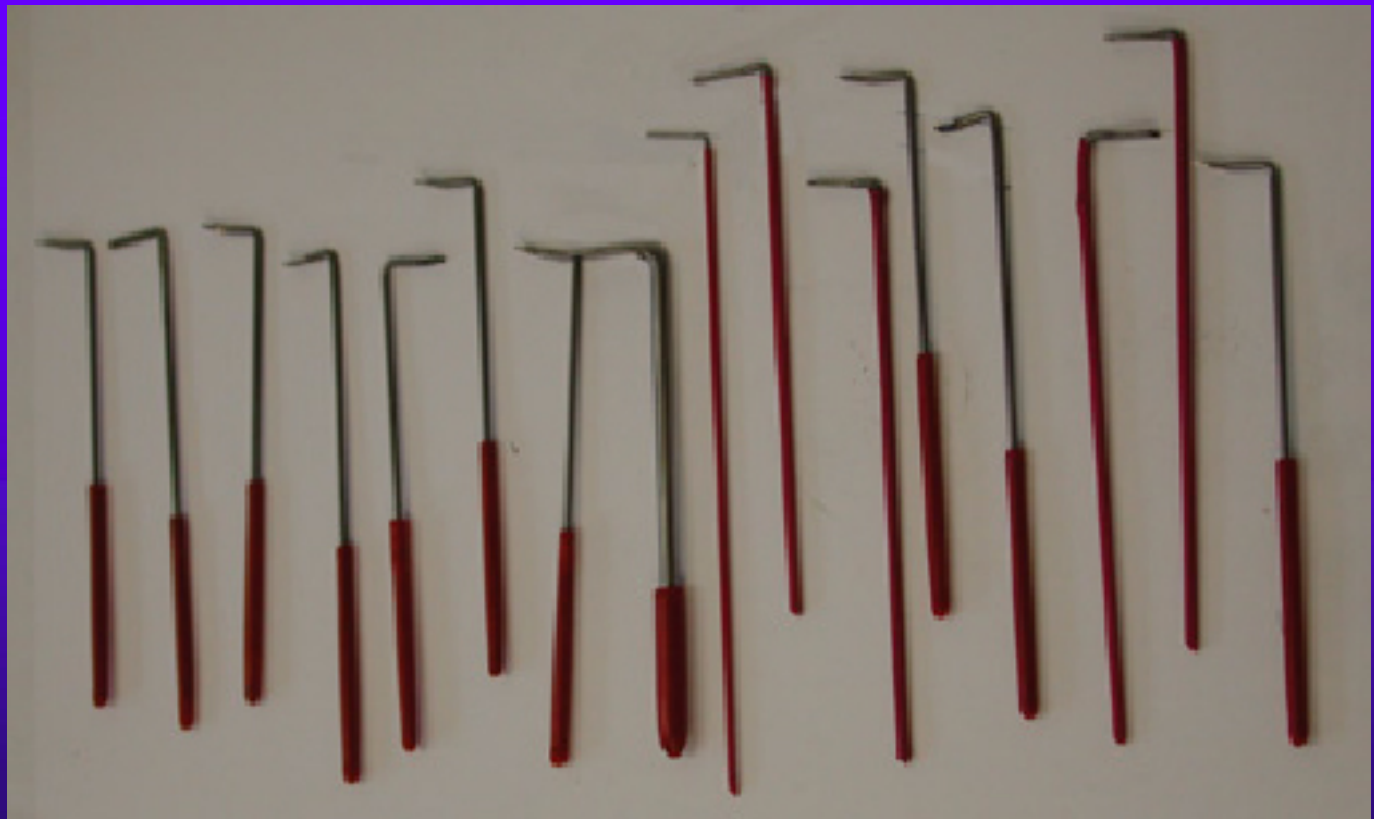


Pick sets





Tension wrench



Falle tension wrenches



Plug rotation blocked

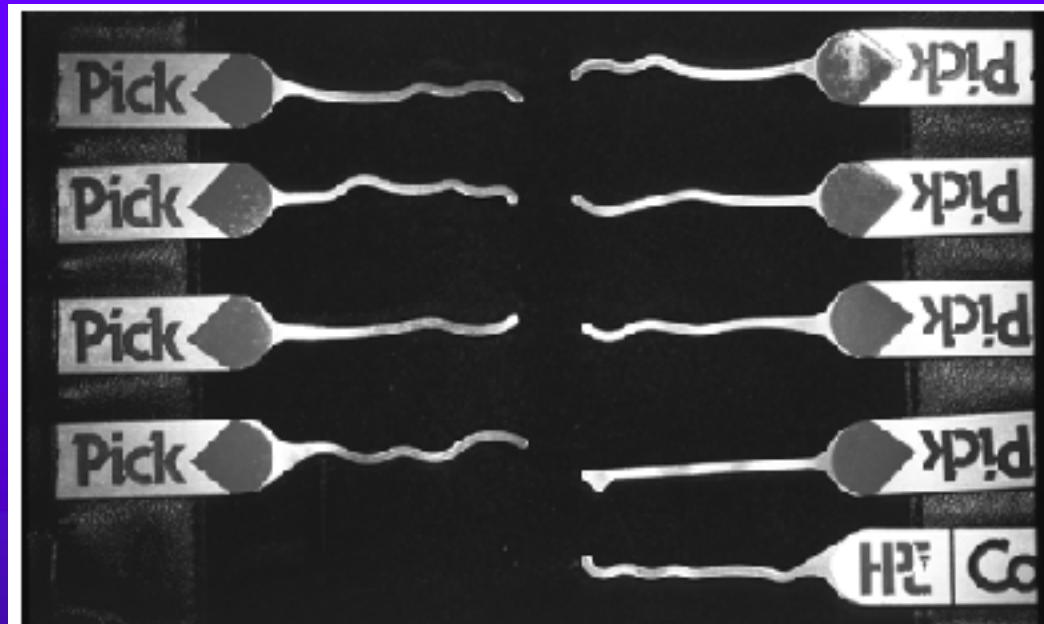
- ◆ Plug cannot turn with tension applied



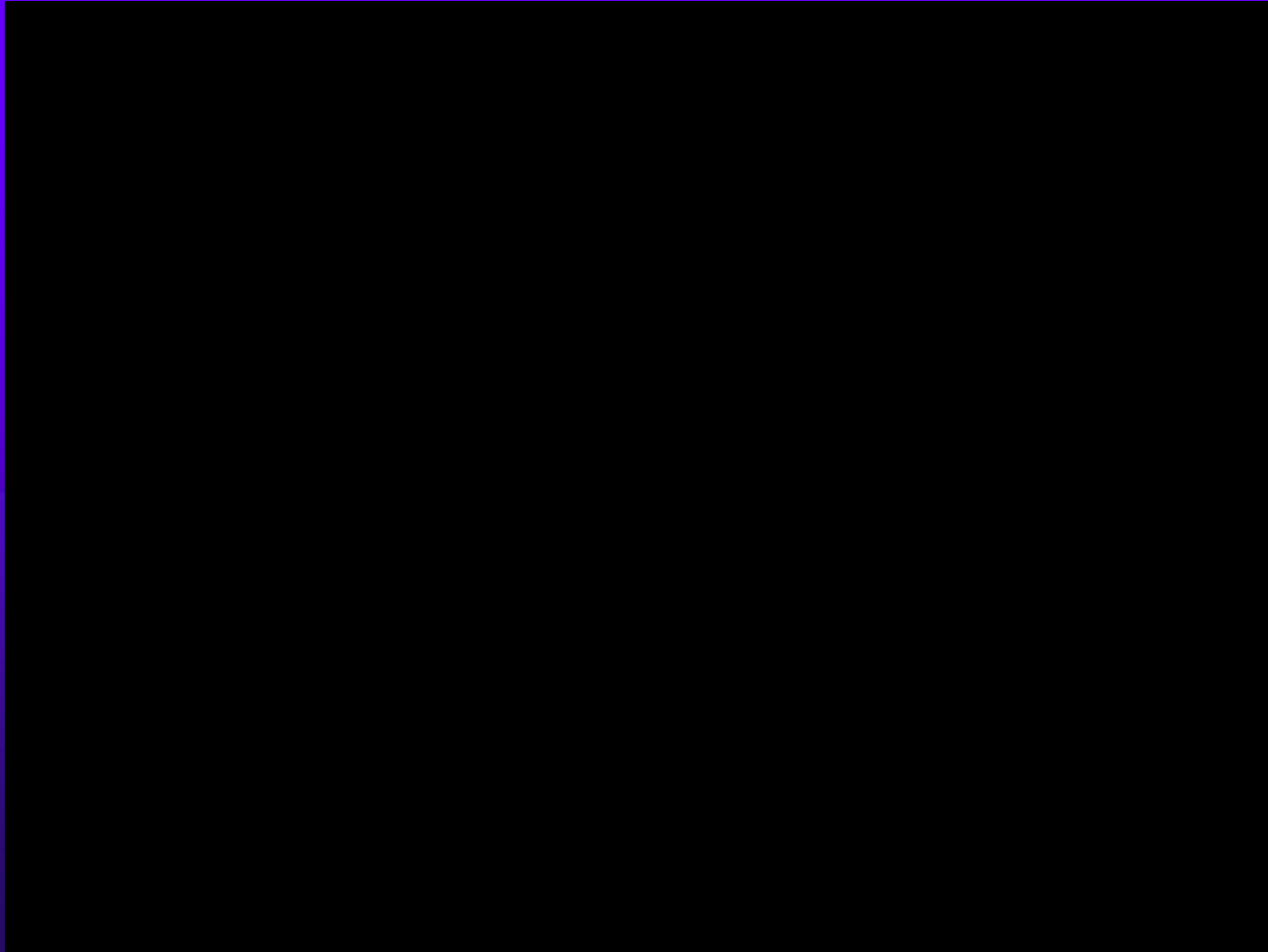
PICK SET – PROFESSIONAL



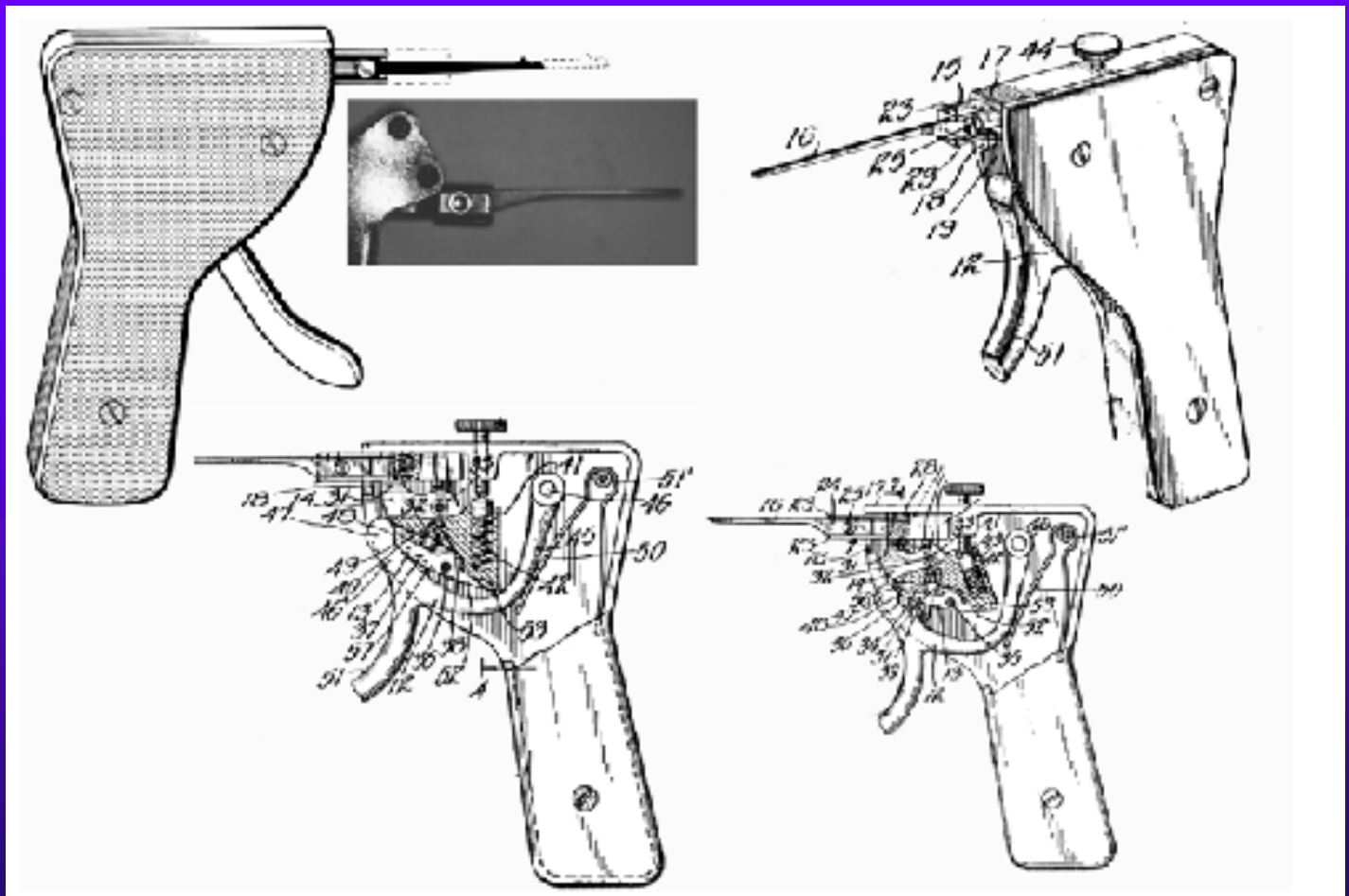
COMPUTER PICKS



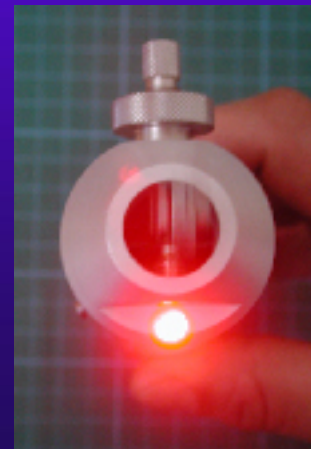
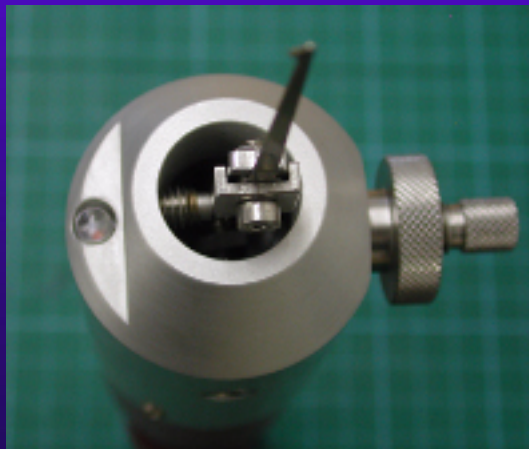
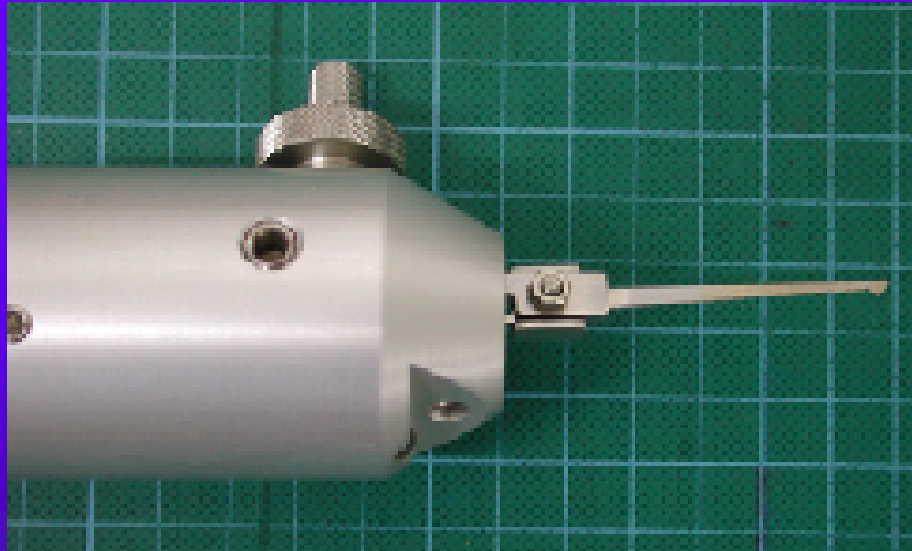
PICKING HIGH SECURITY LOCKS: MEDECO



PICK GUNS



Vibration pick gun



MSC: PICKING BY VIBRATION



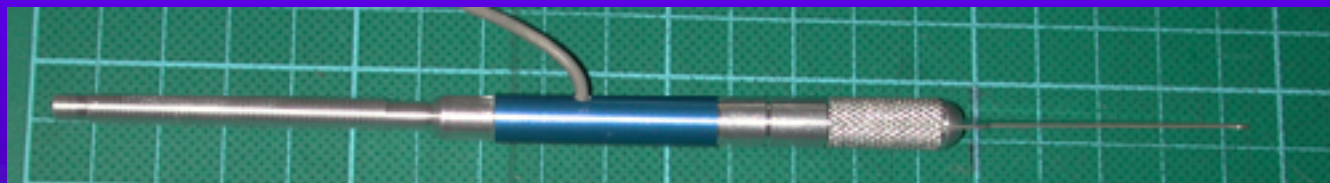
Axial lock picks



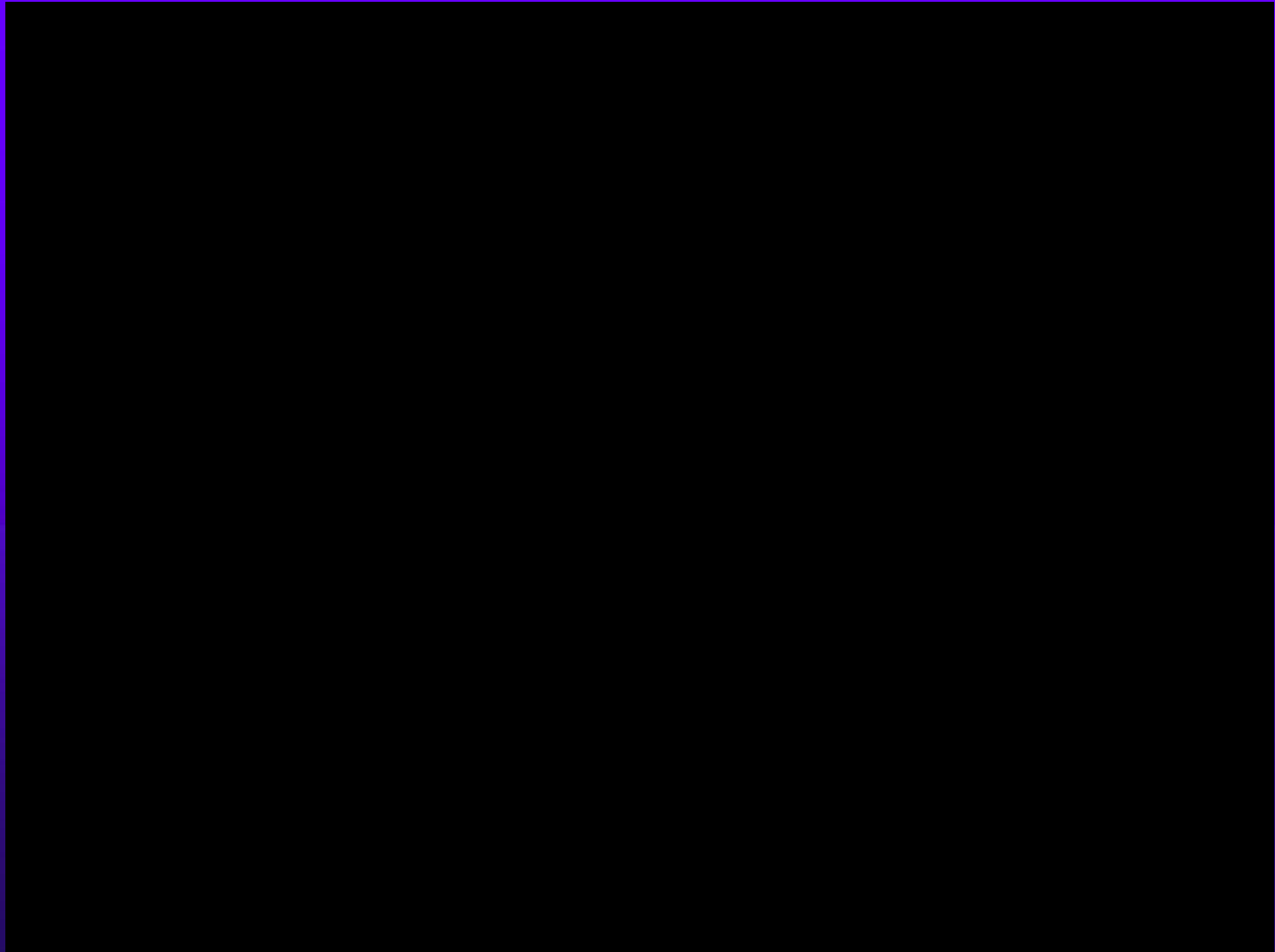
Peterson Pro-1 Axial pick



Acoustic Pick



MSC: ACOUSTIC PICK



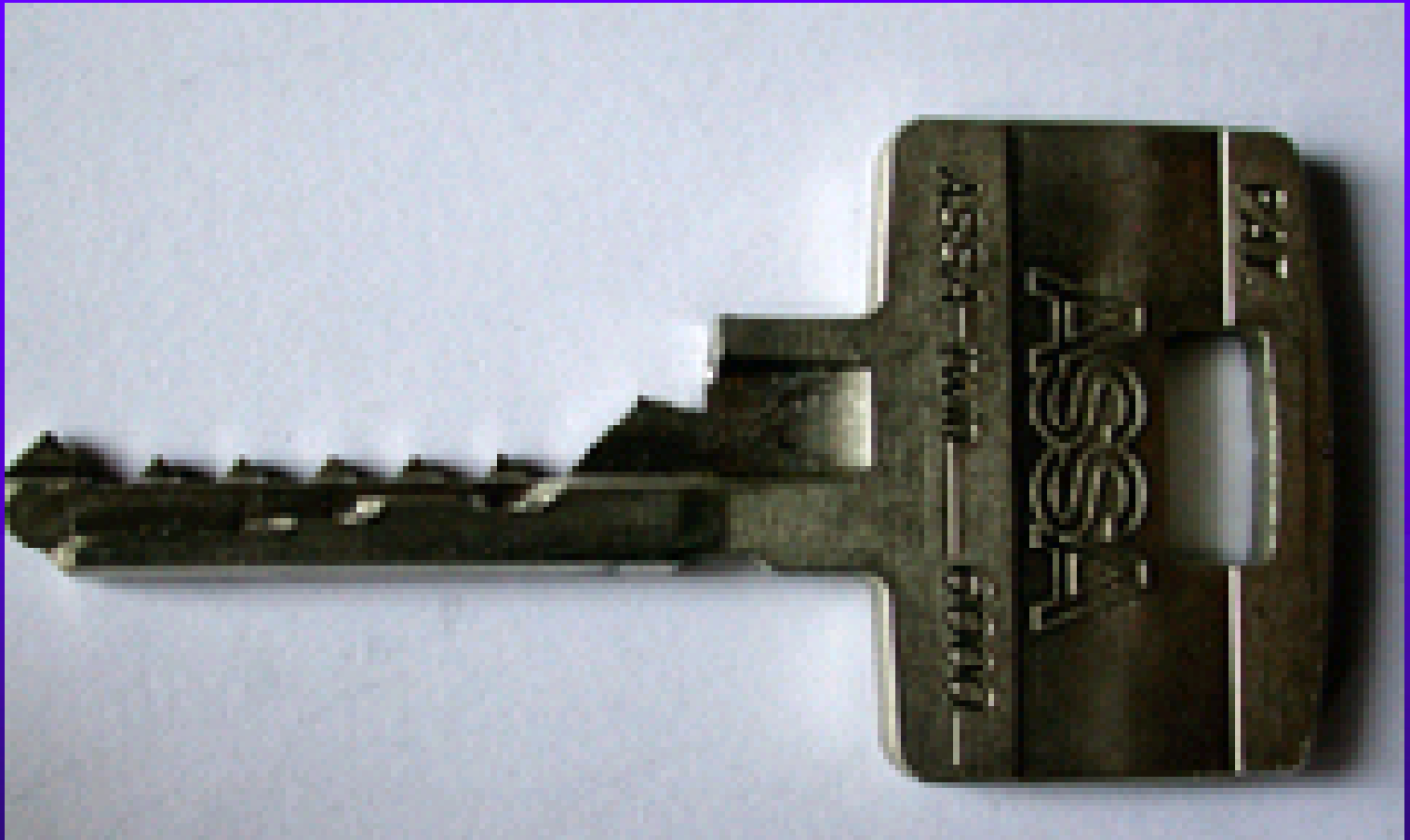
999 Bump Key



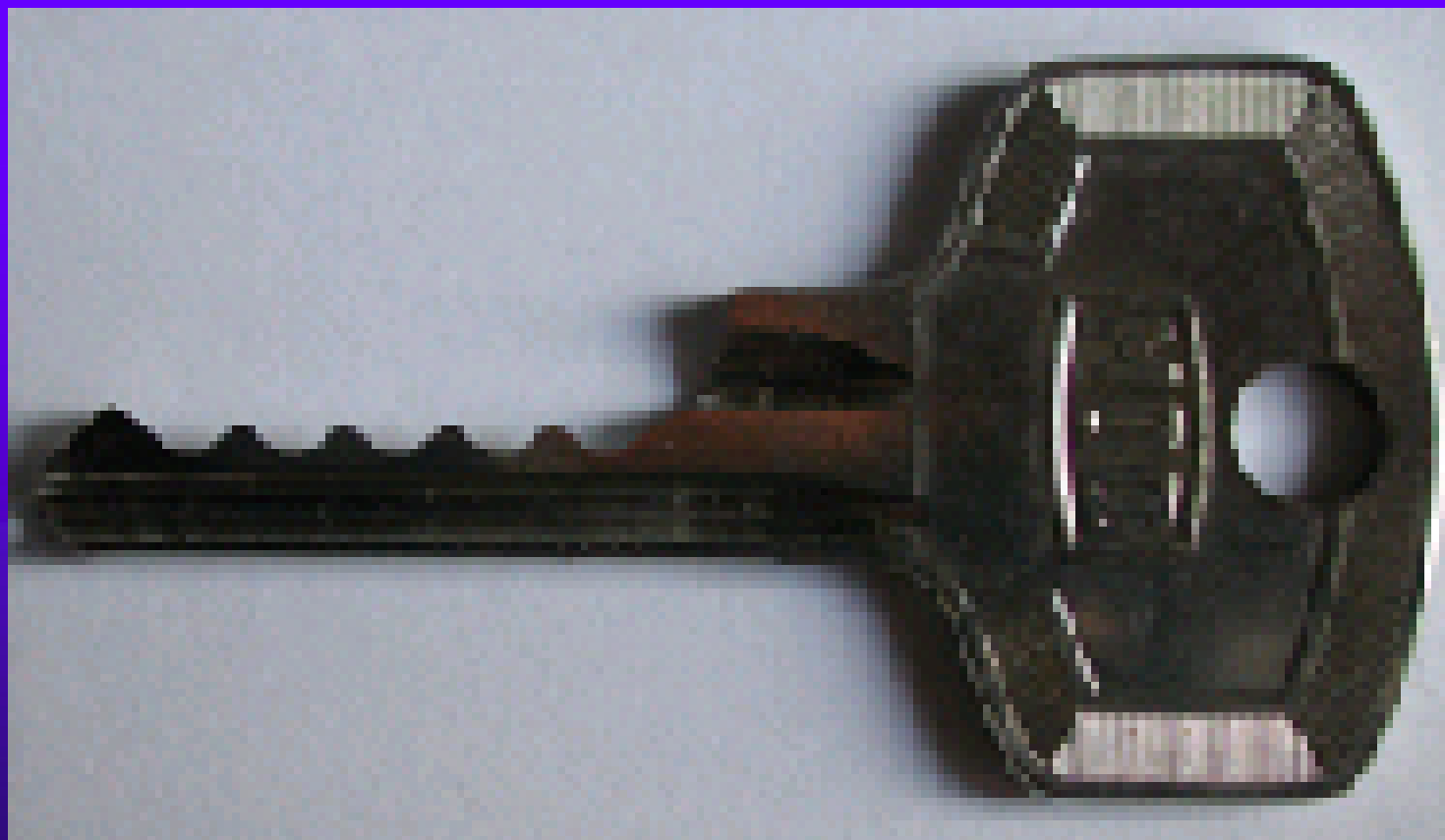
Bump Keys



Sidebar Locks



999 Key



Dimple lock



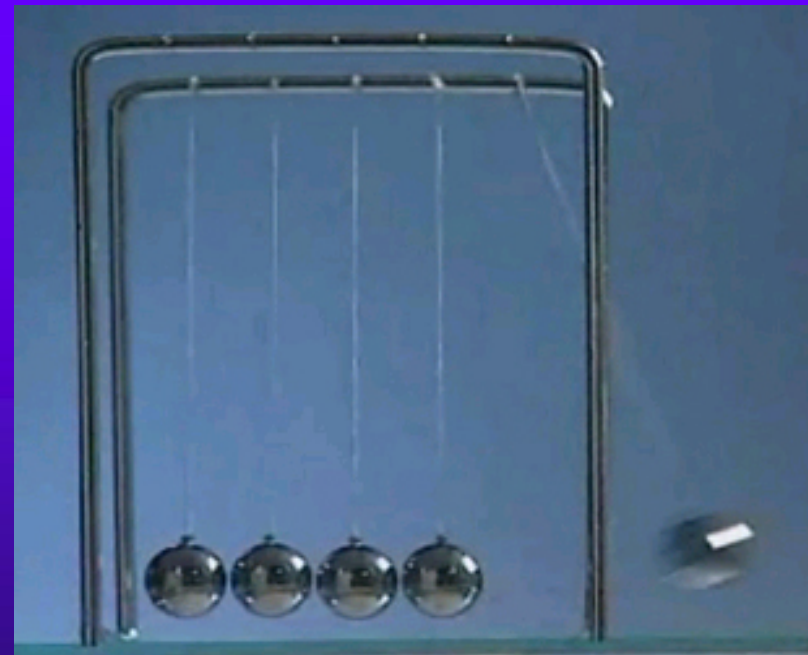
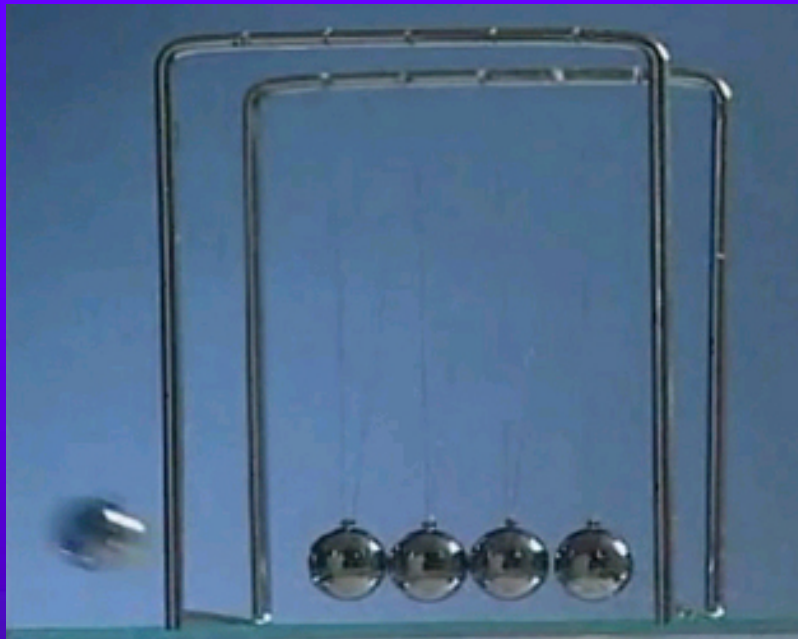
Dimple Locks



Axial Pin Tumbler



Bump Key Theory



Theory



Negative Shoulder



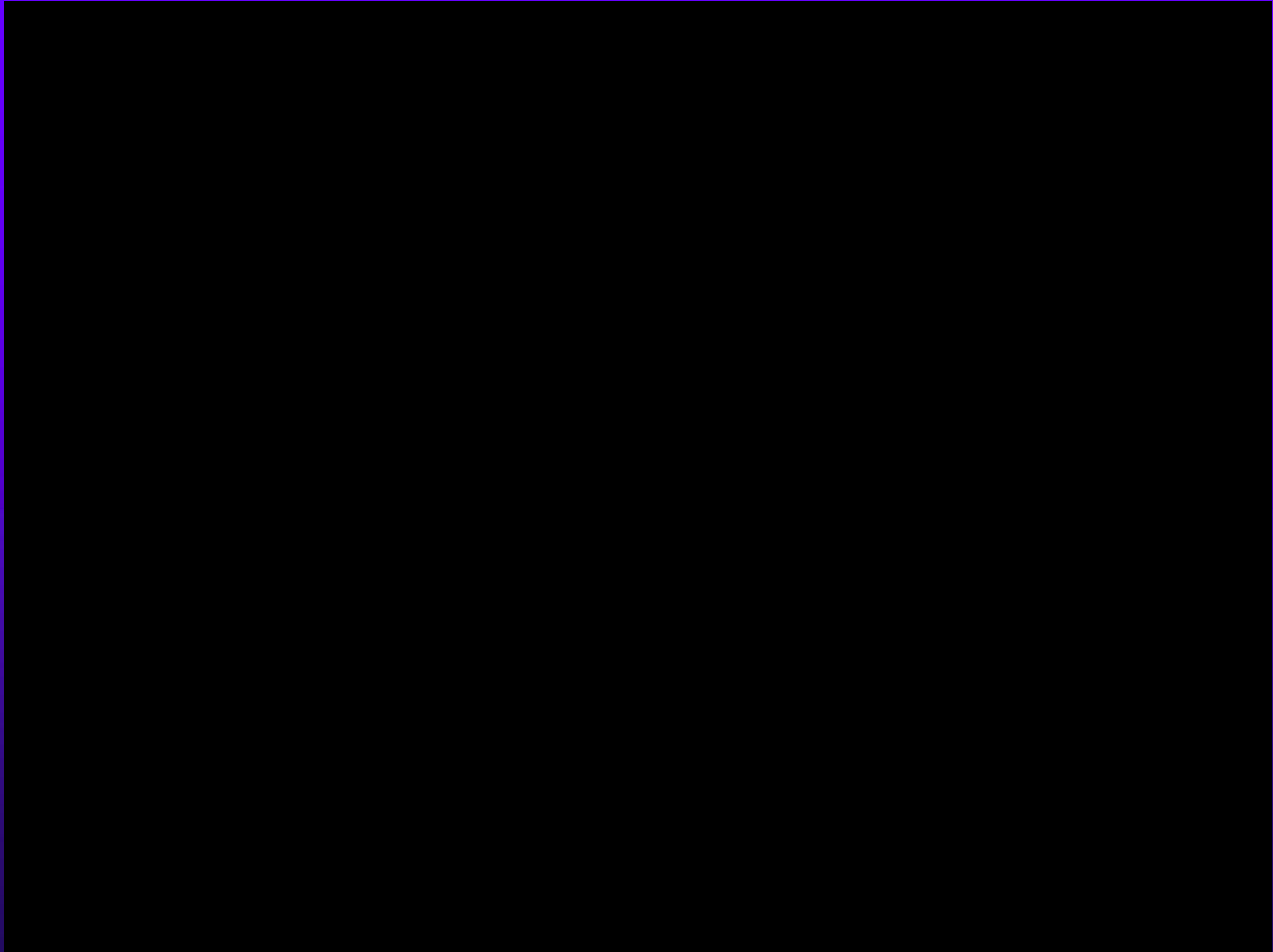
11-YEAR OLD BUMPS LOCK



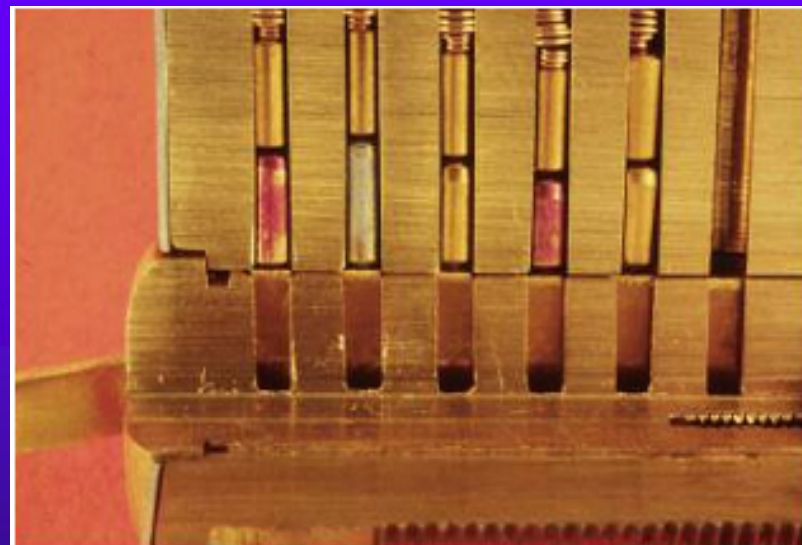
999 BUMP KEY DEMONSTRATION



BUMPING HIGH SECURITY: ASSA



Comb picking



Comb pick set: Falle

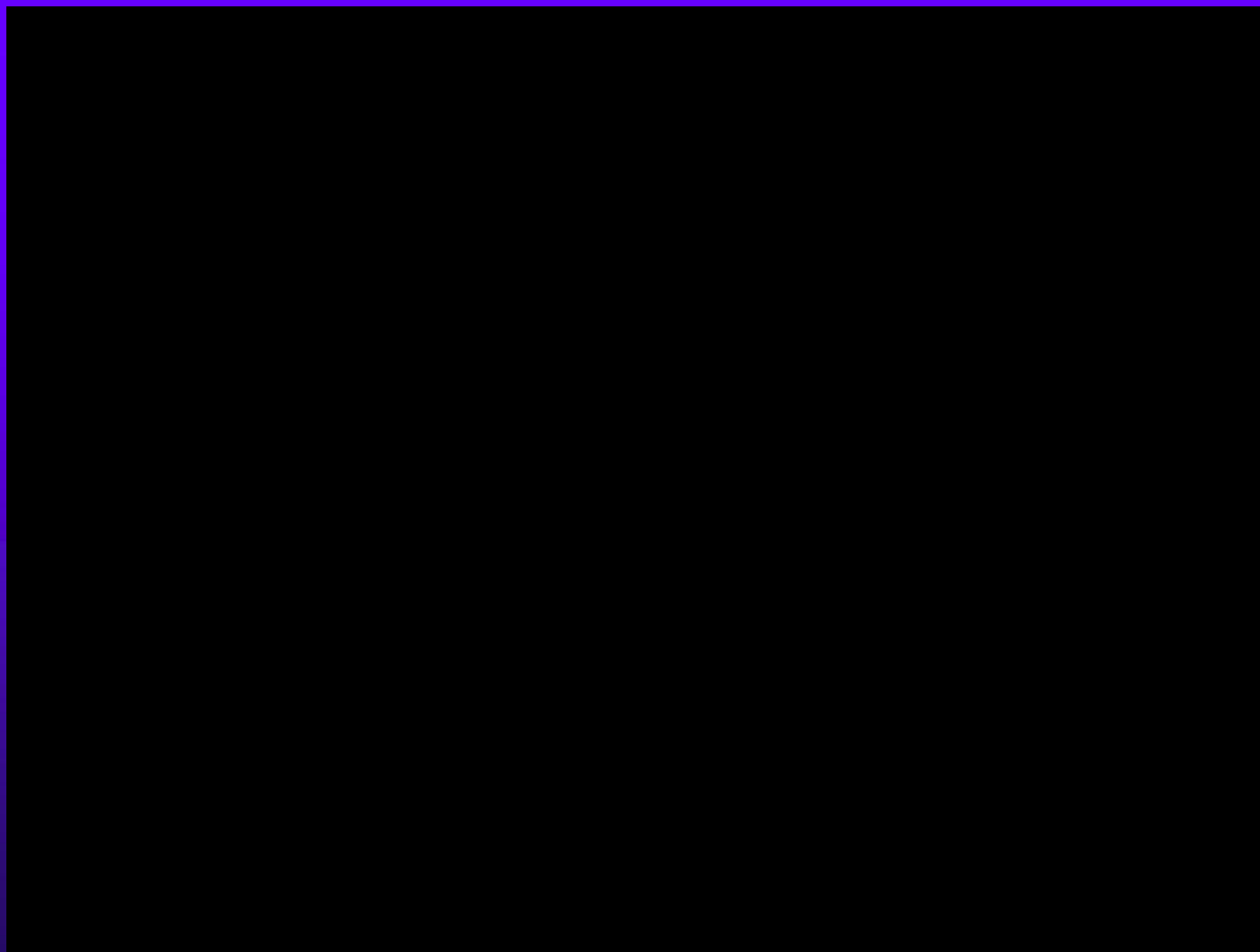


Cross pick

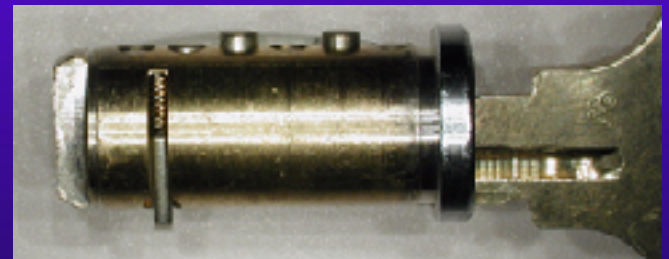
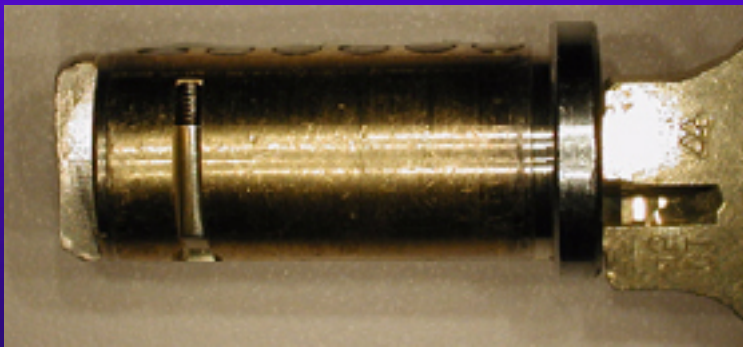




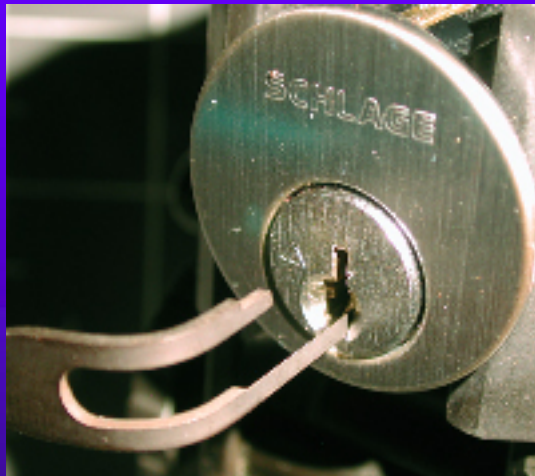
MSC: CROSS PICK



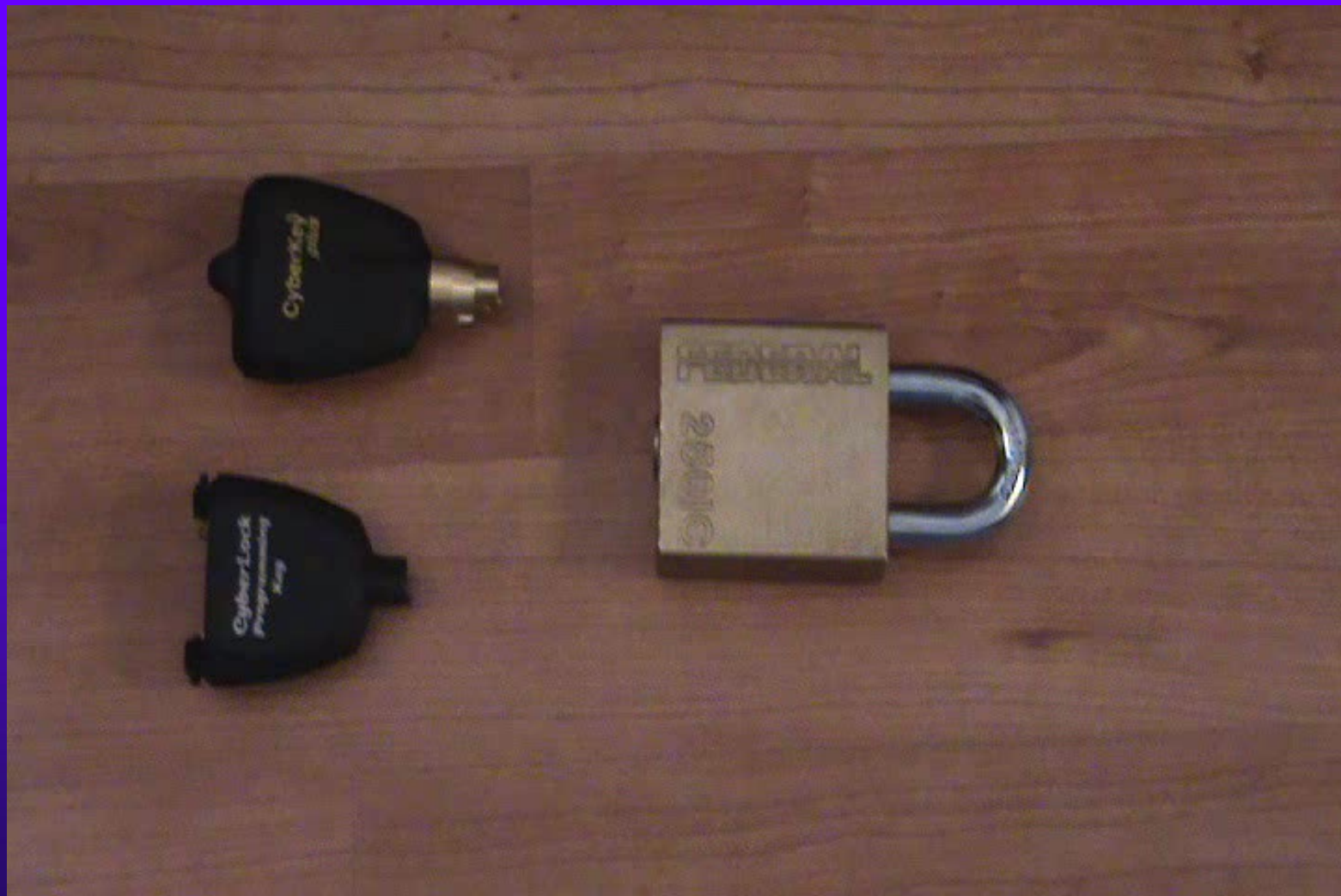
Schlage Everest



Schlage Everest: Picking



MAGNETIC BYPASS

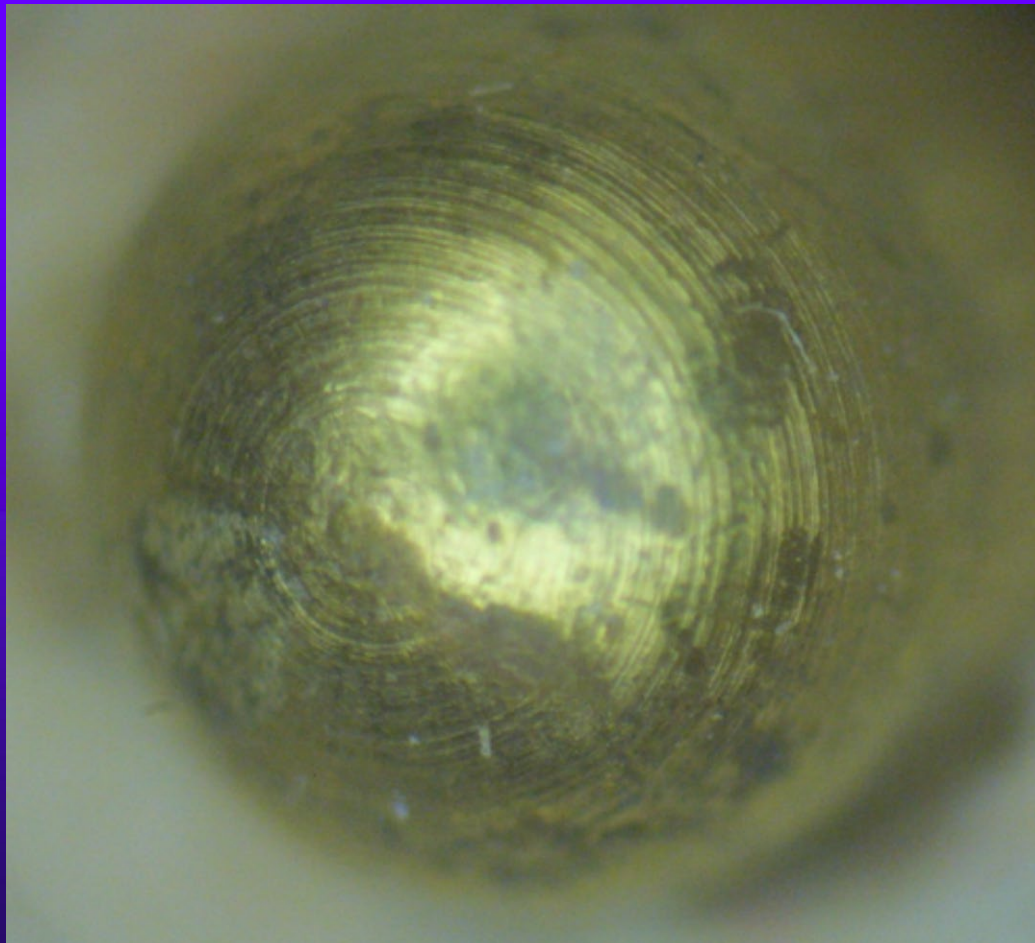




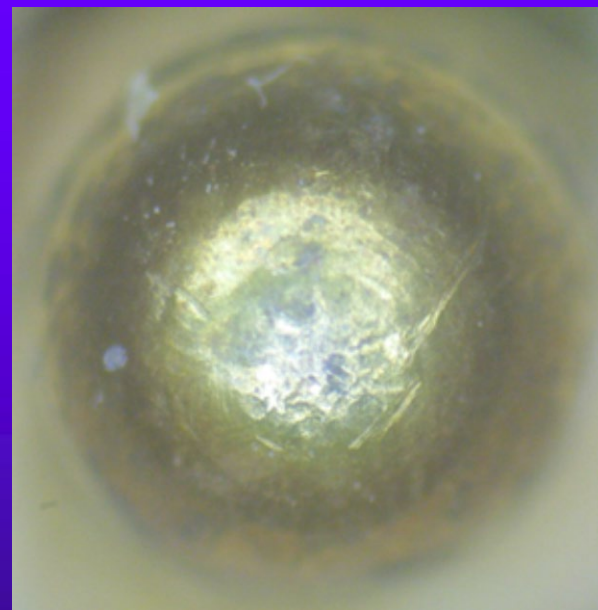
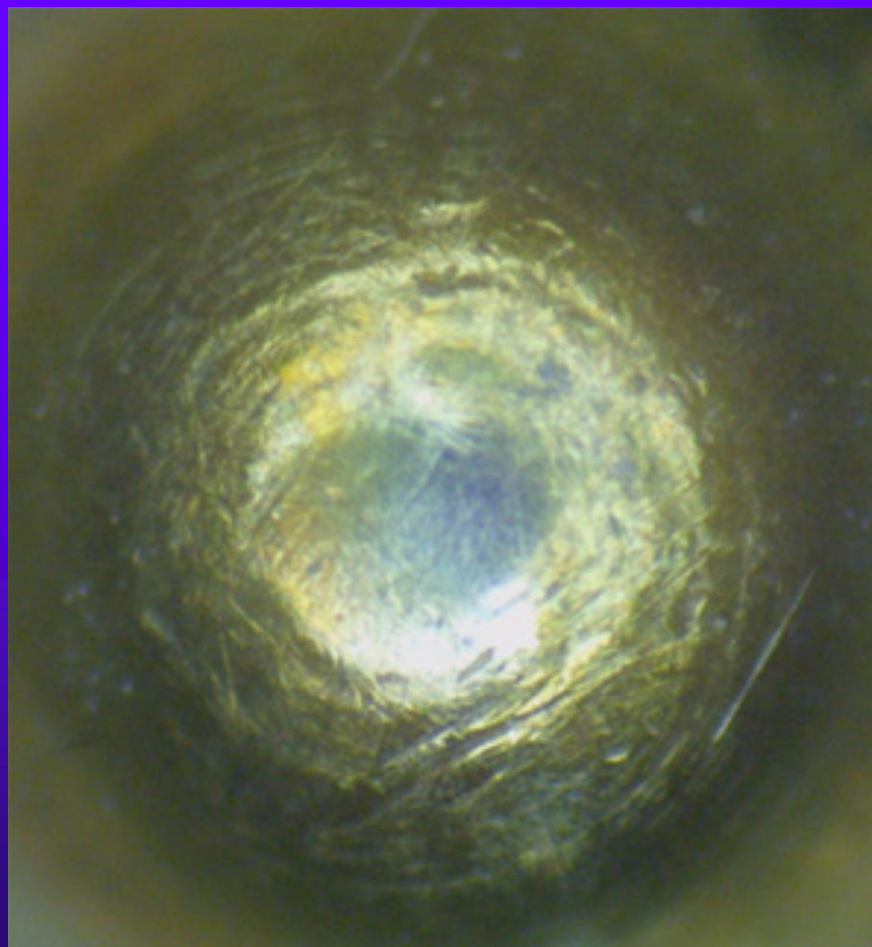
FORENSICS OF PICKING



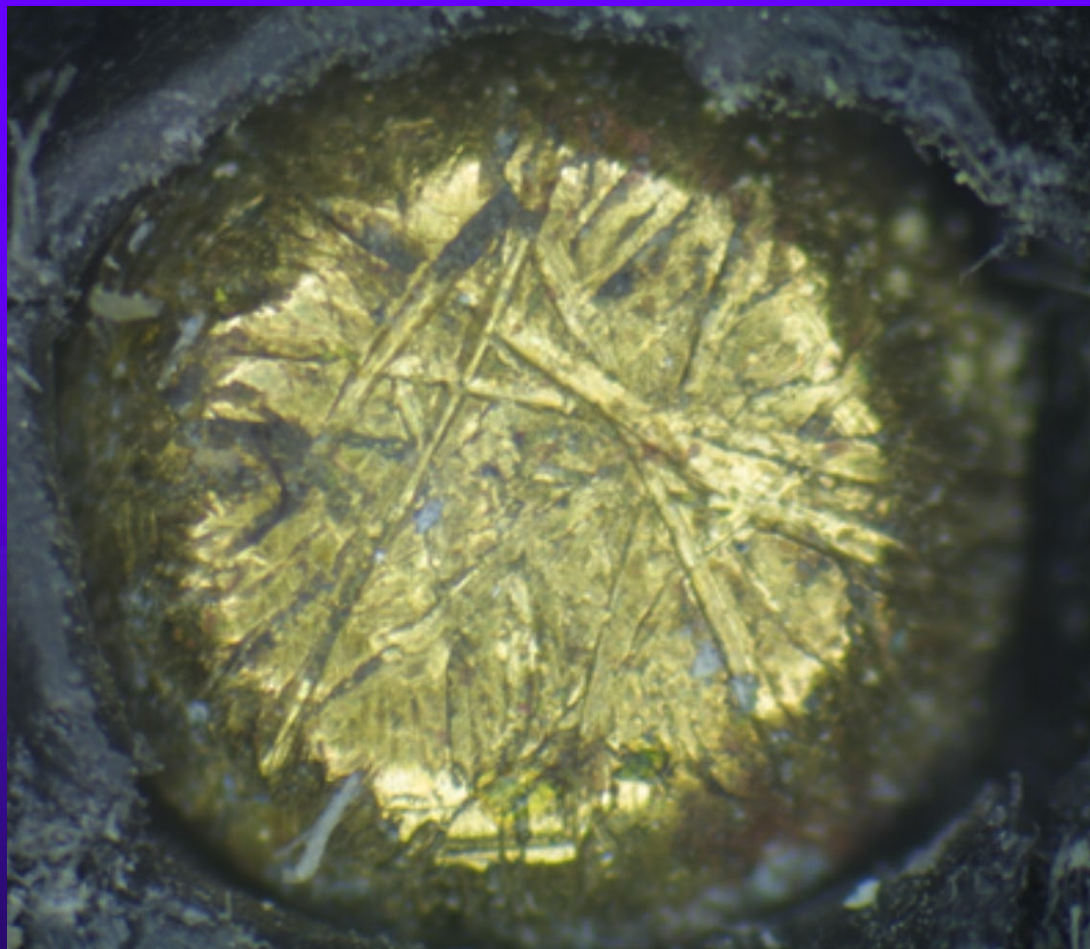
FORENSIC INDICIA OF BYPASS



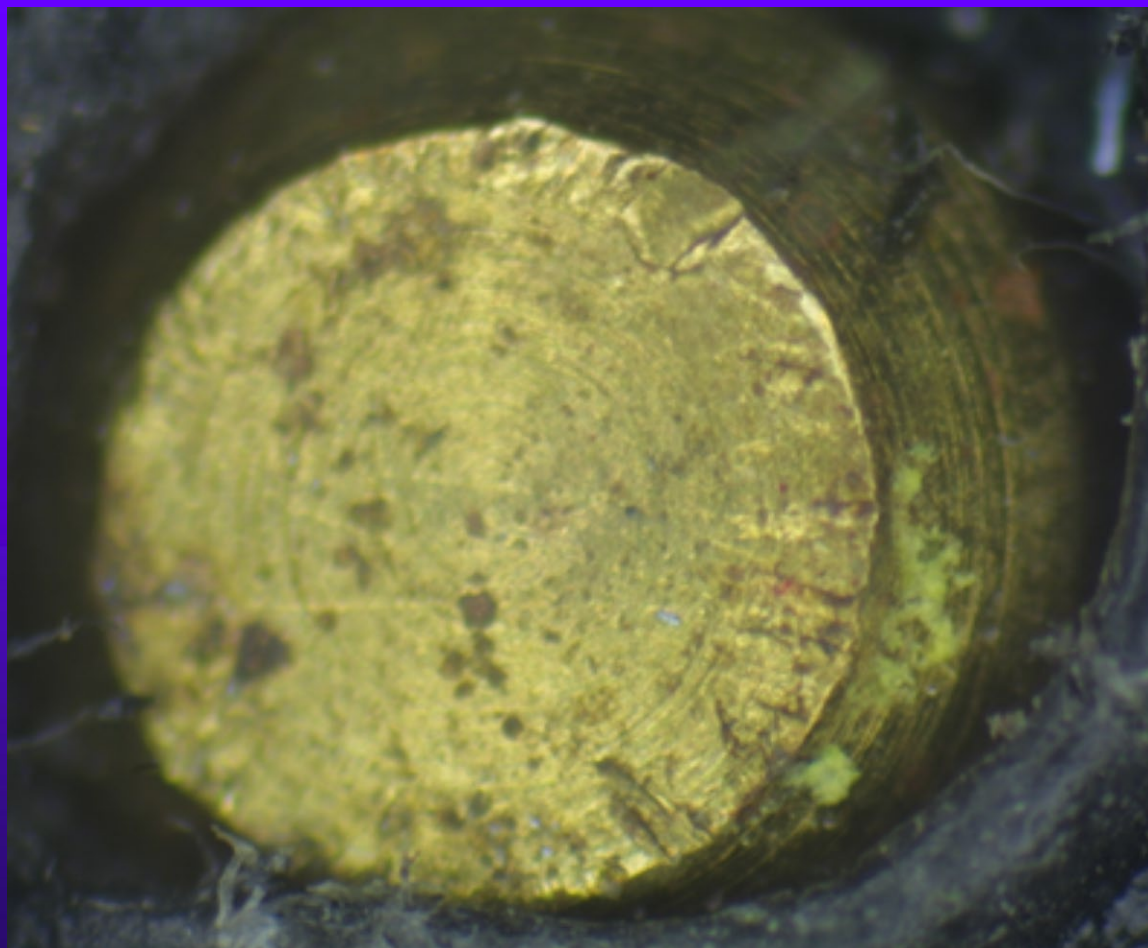
Pick Marks on Pin



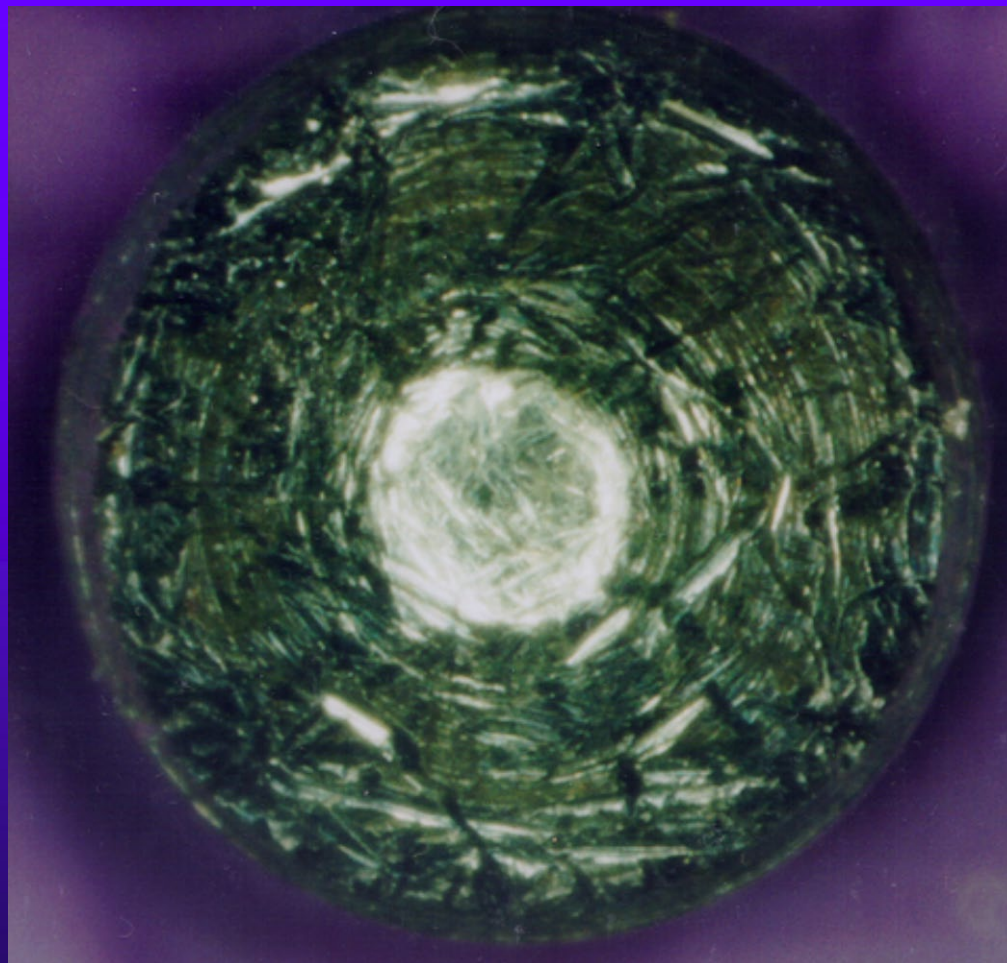
Marks from Pick Gun



Pick Gun Markings



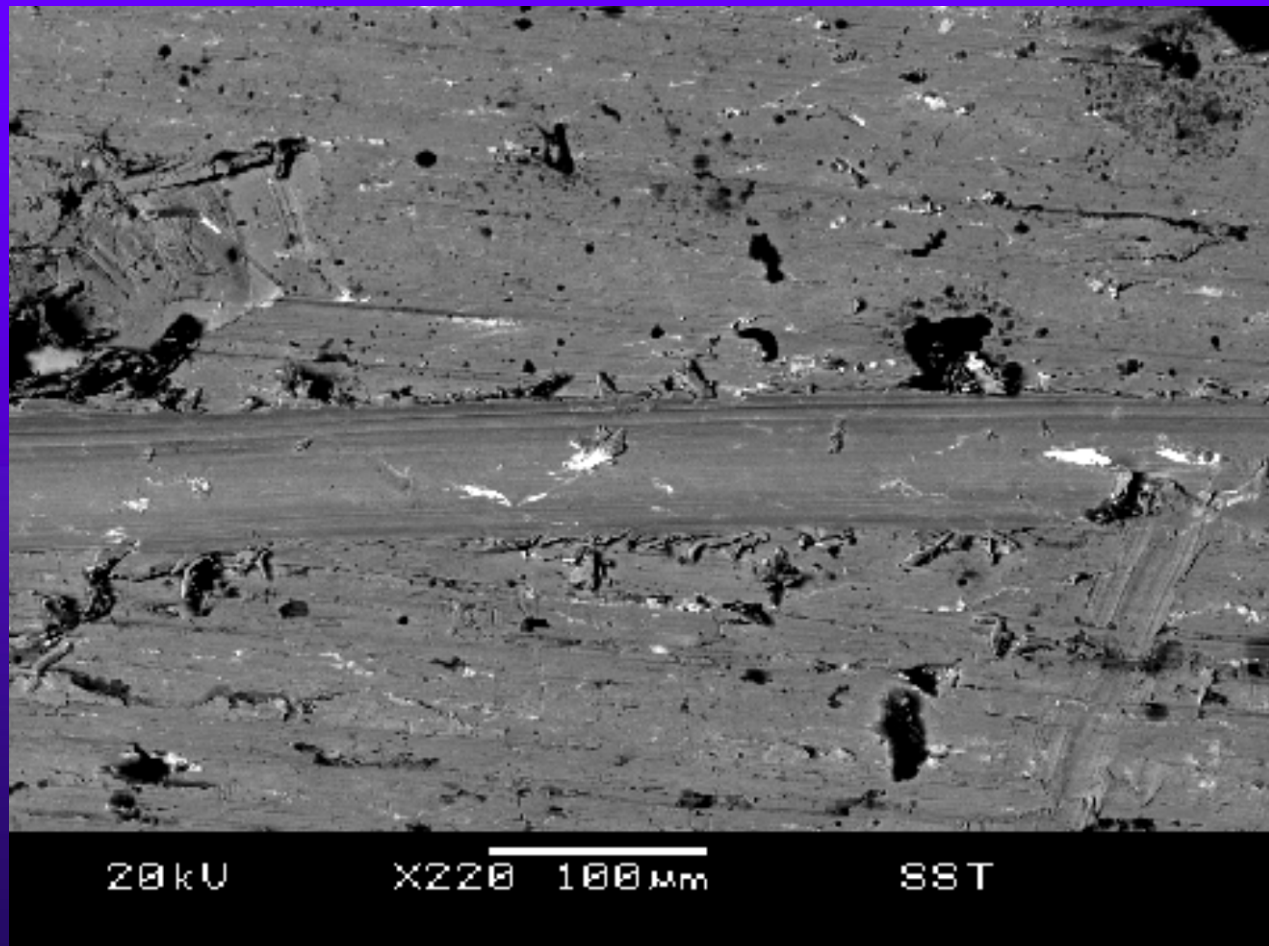
Impact Pick Marks



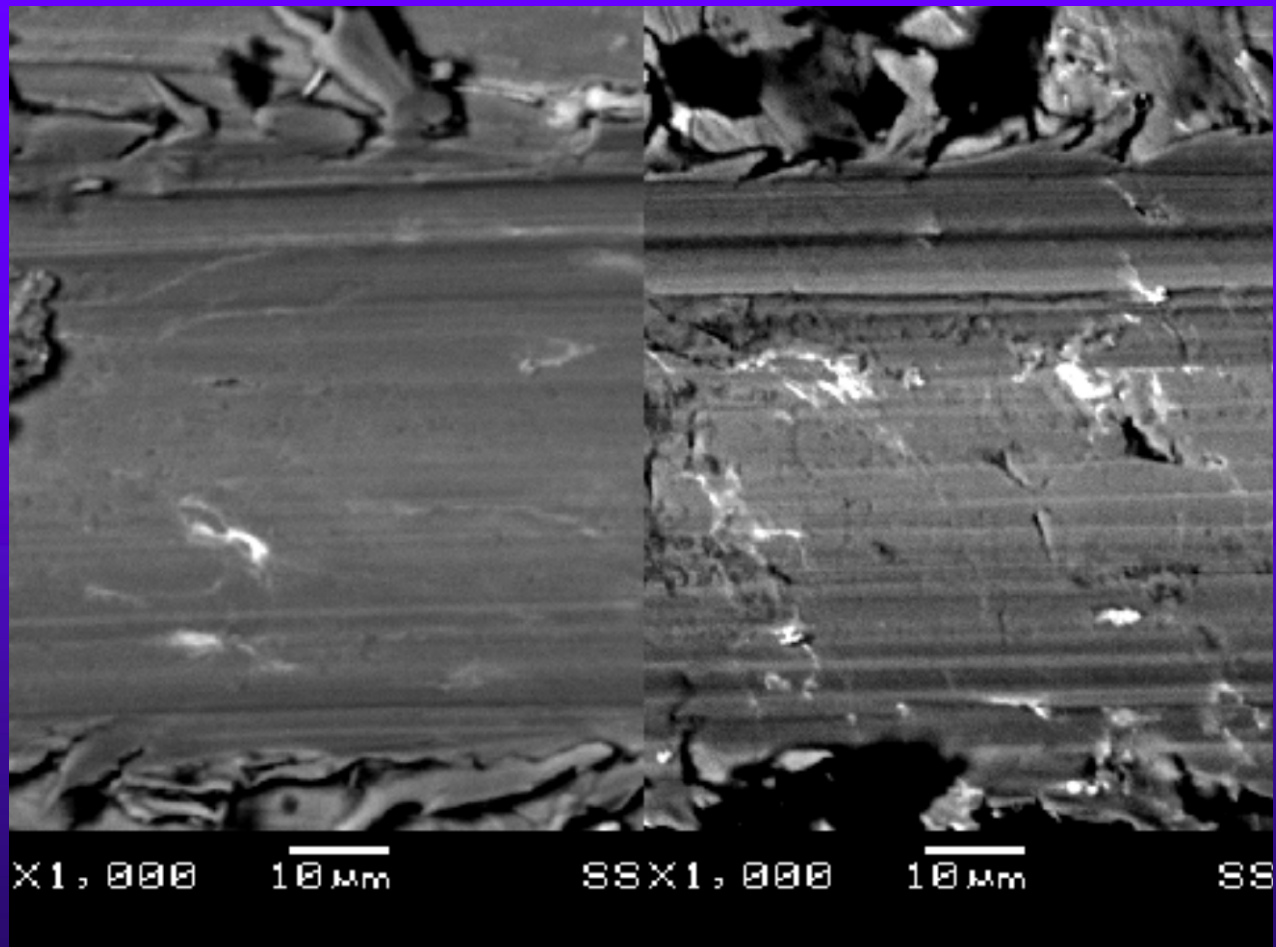
USE OF S E M



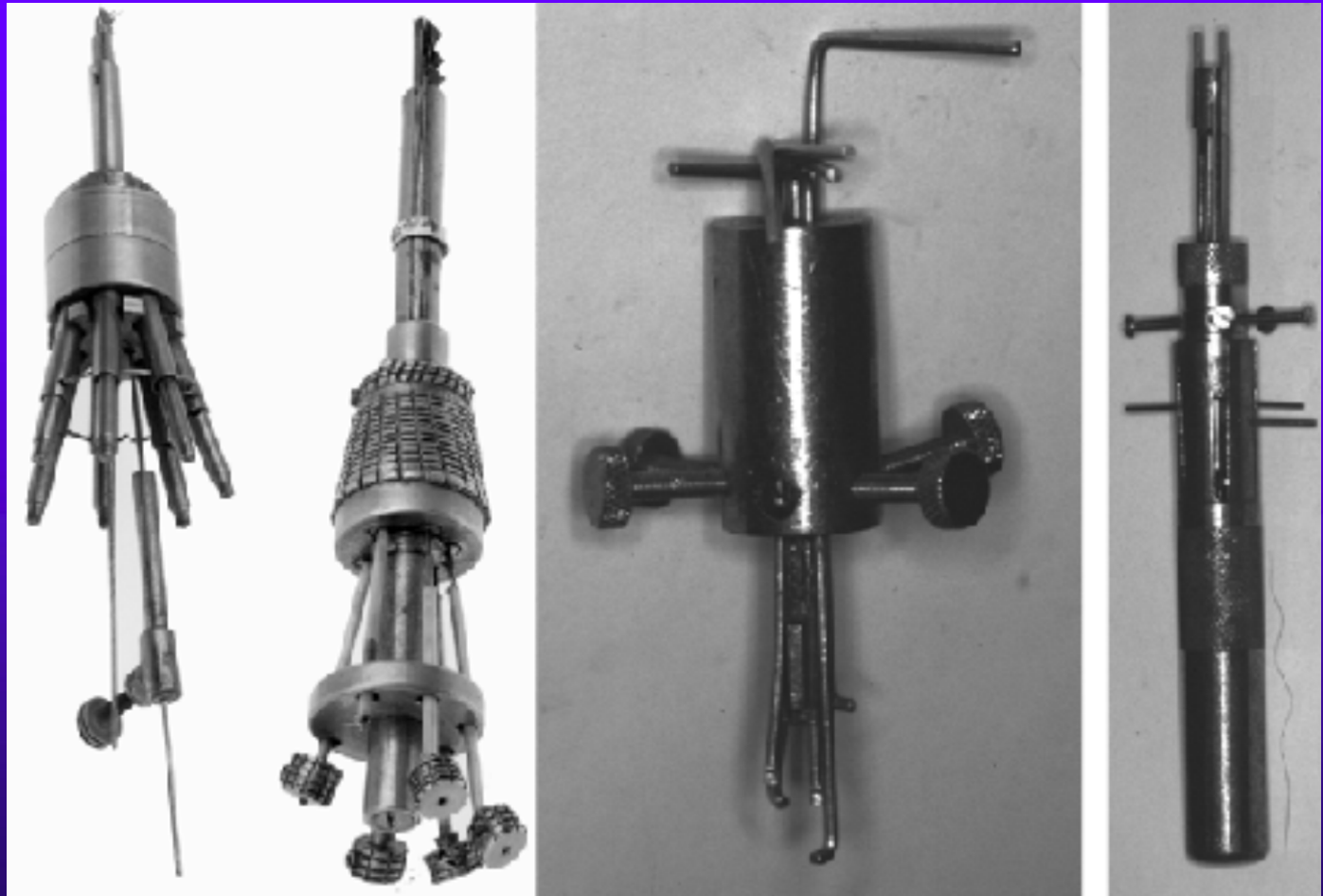
Pick Tracks



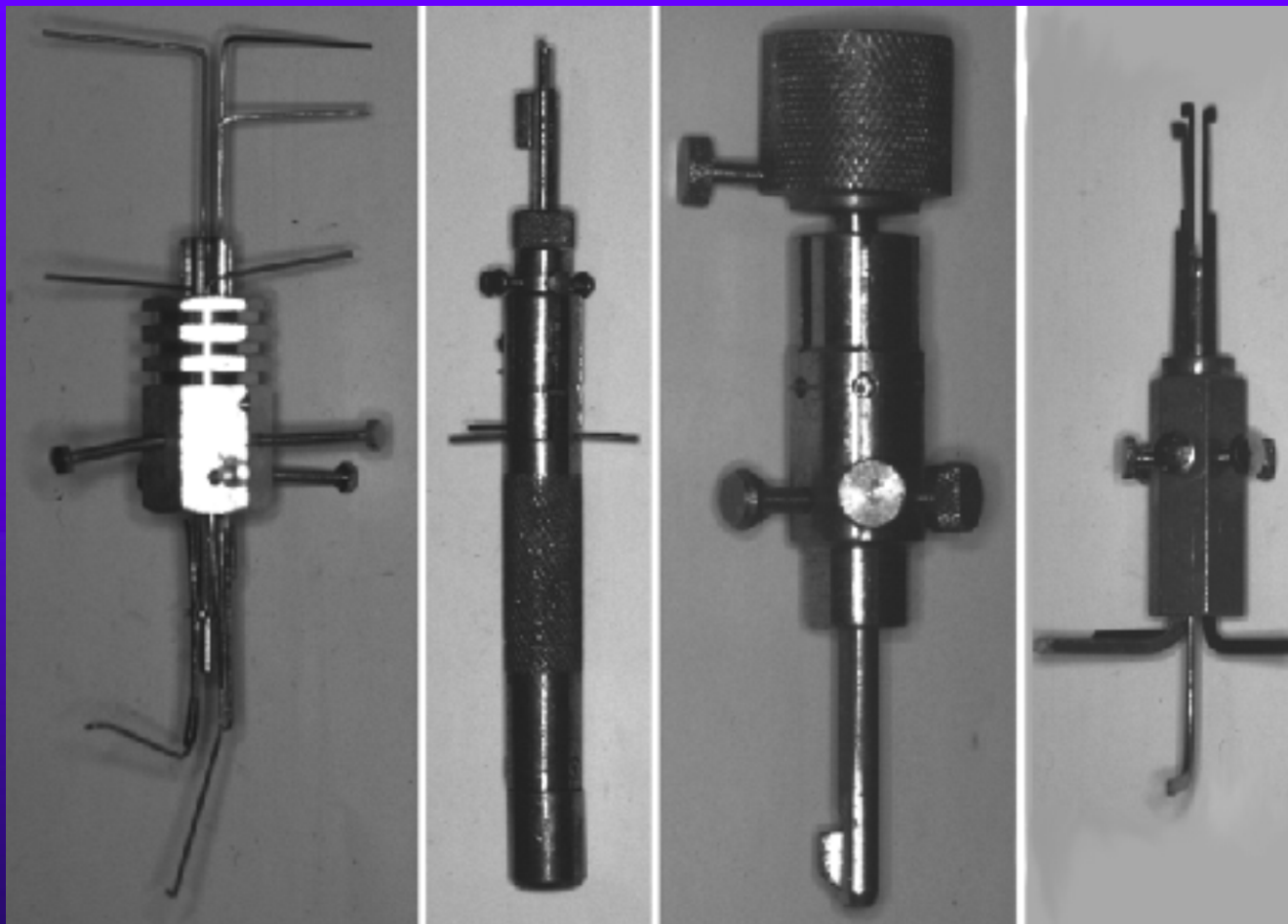
SEM Pick Track Comparison



More Special Picks – Europe



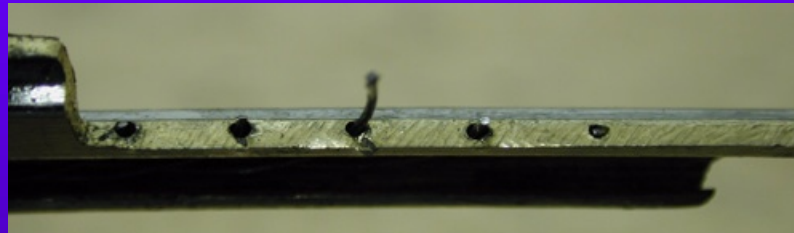
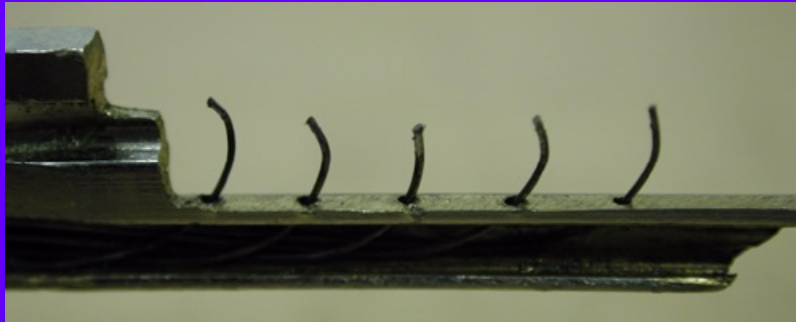
SPECIAL PICKS



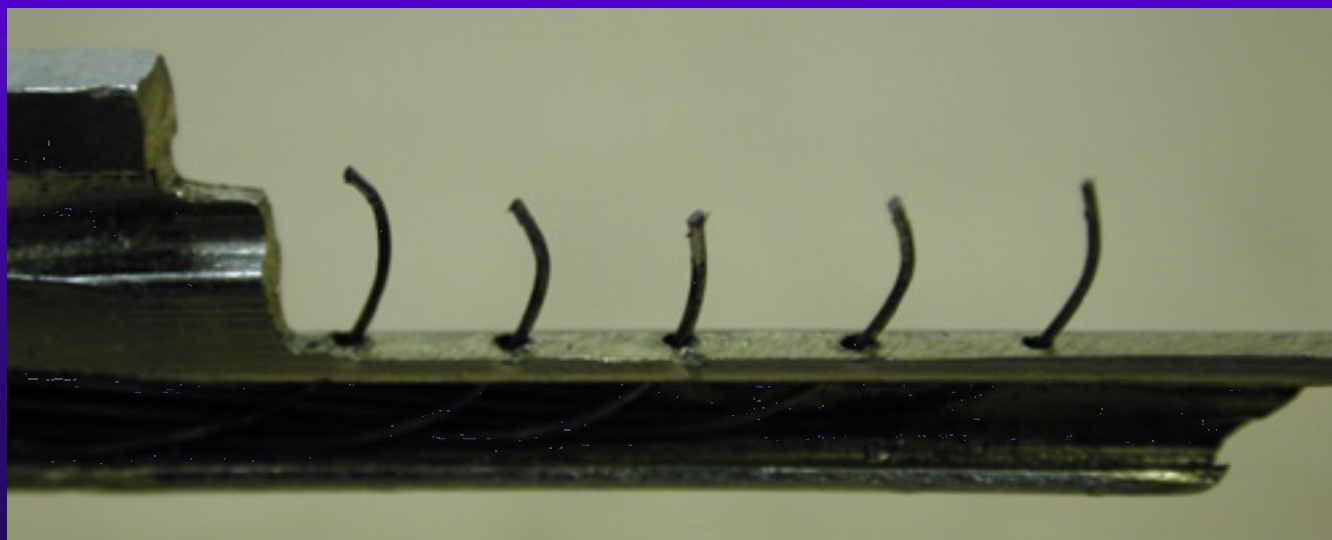
Rake pick for dimple locks



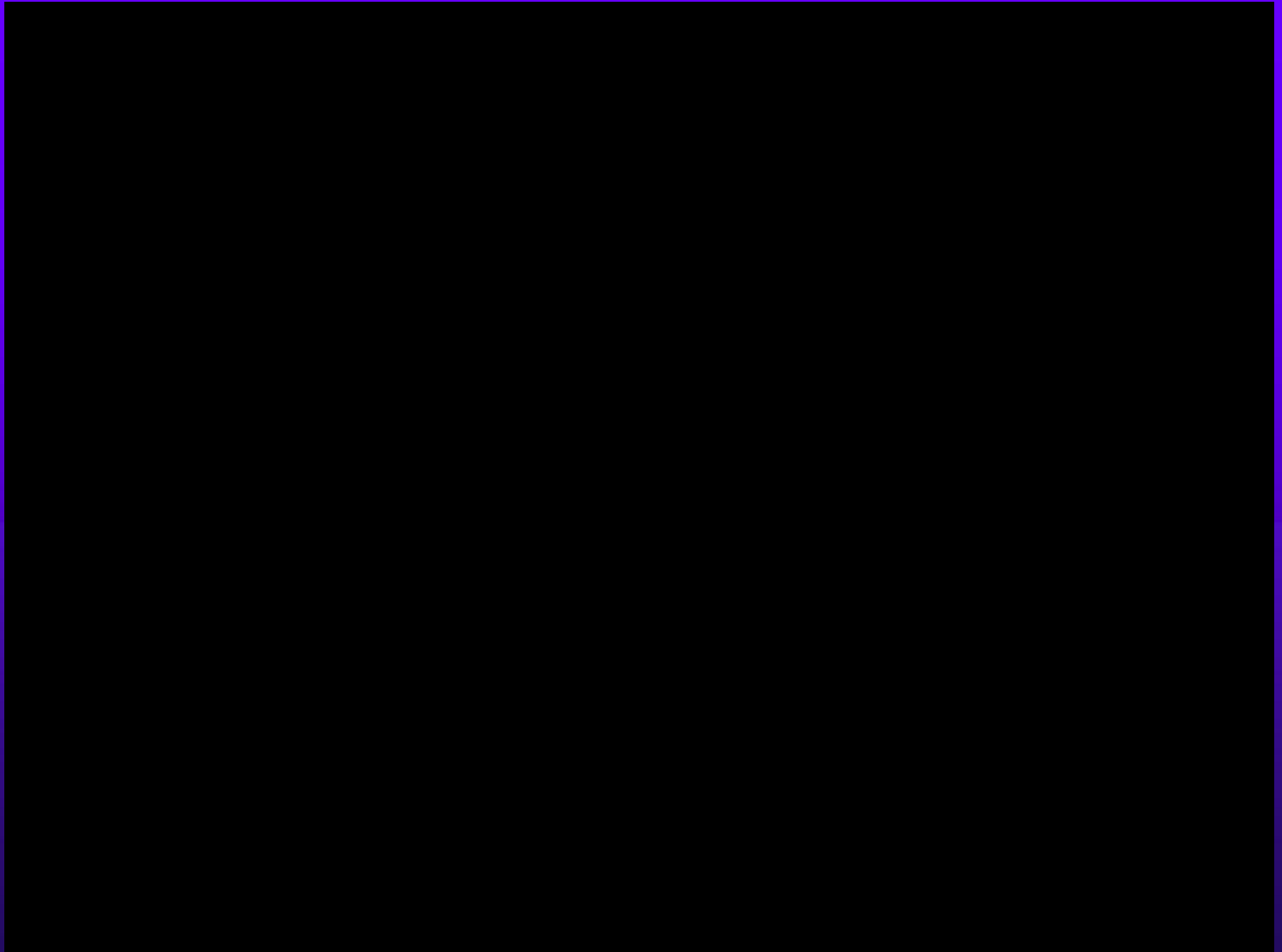
Feeler Wires for Picking



SPUTNIK PICK



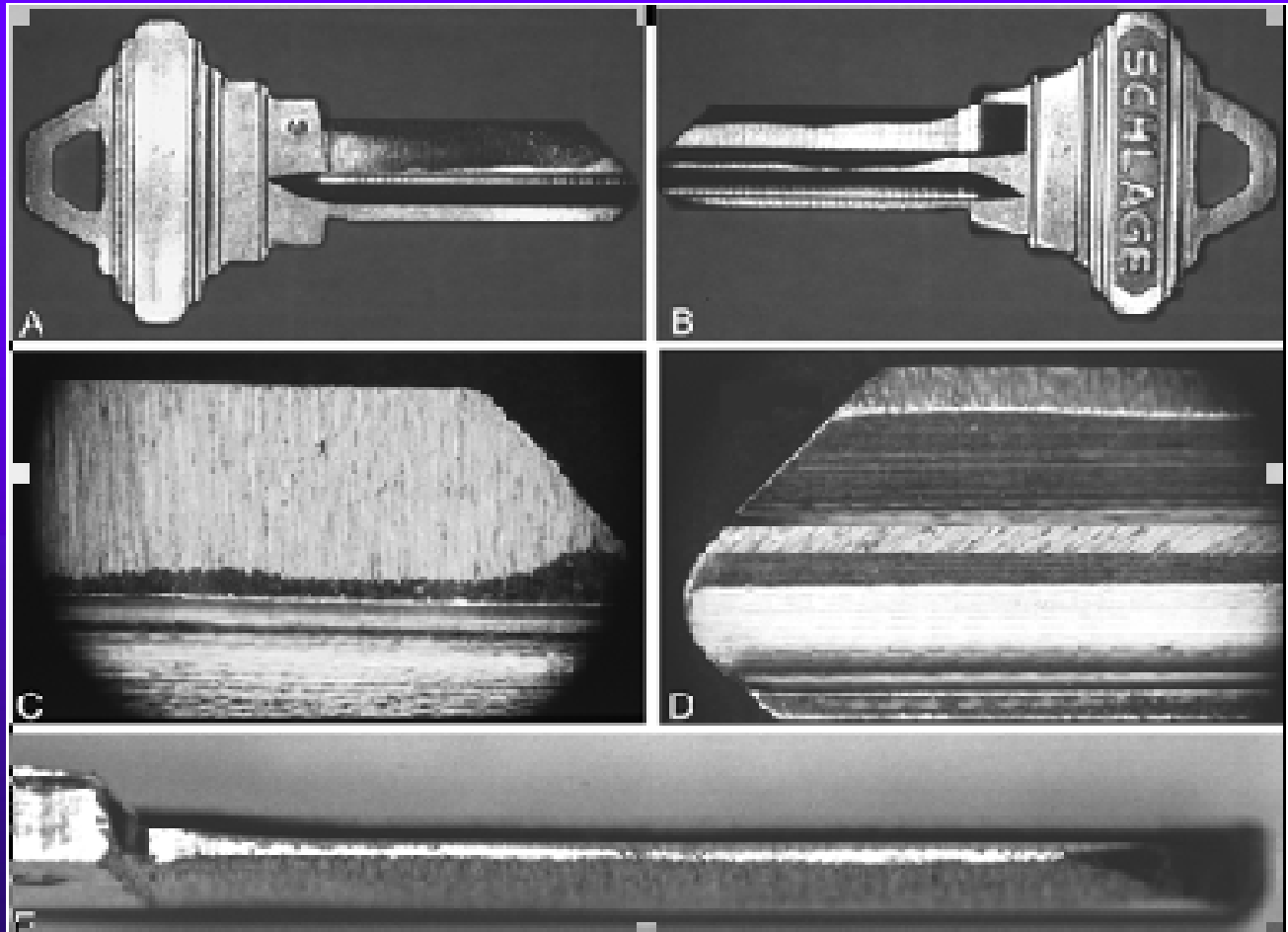
SPUTNIK DEMONSTRATION



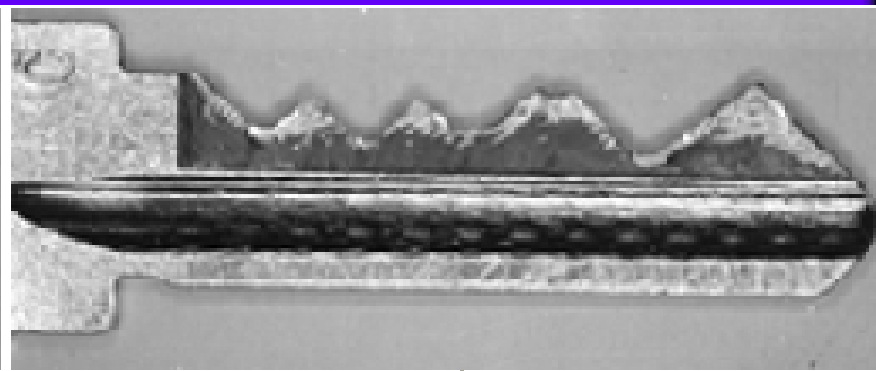
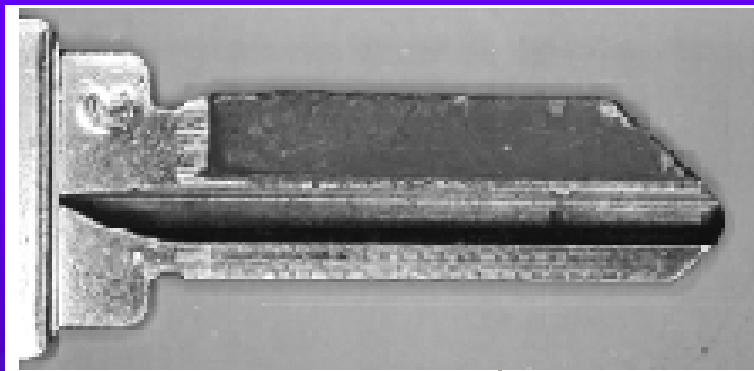


IMPRESSIONING TOOLS

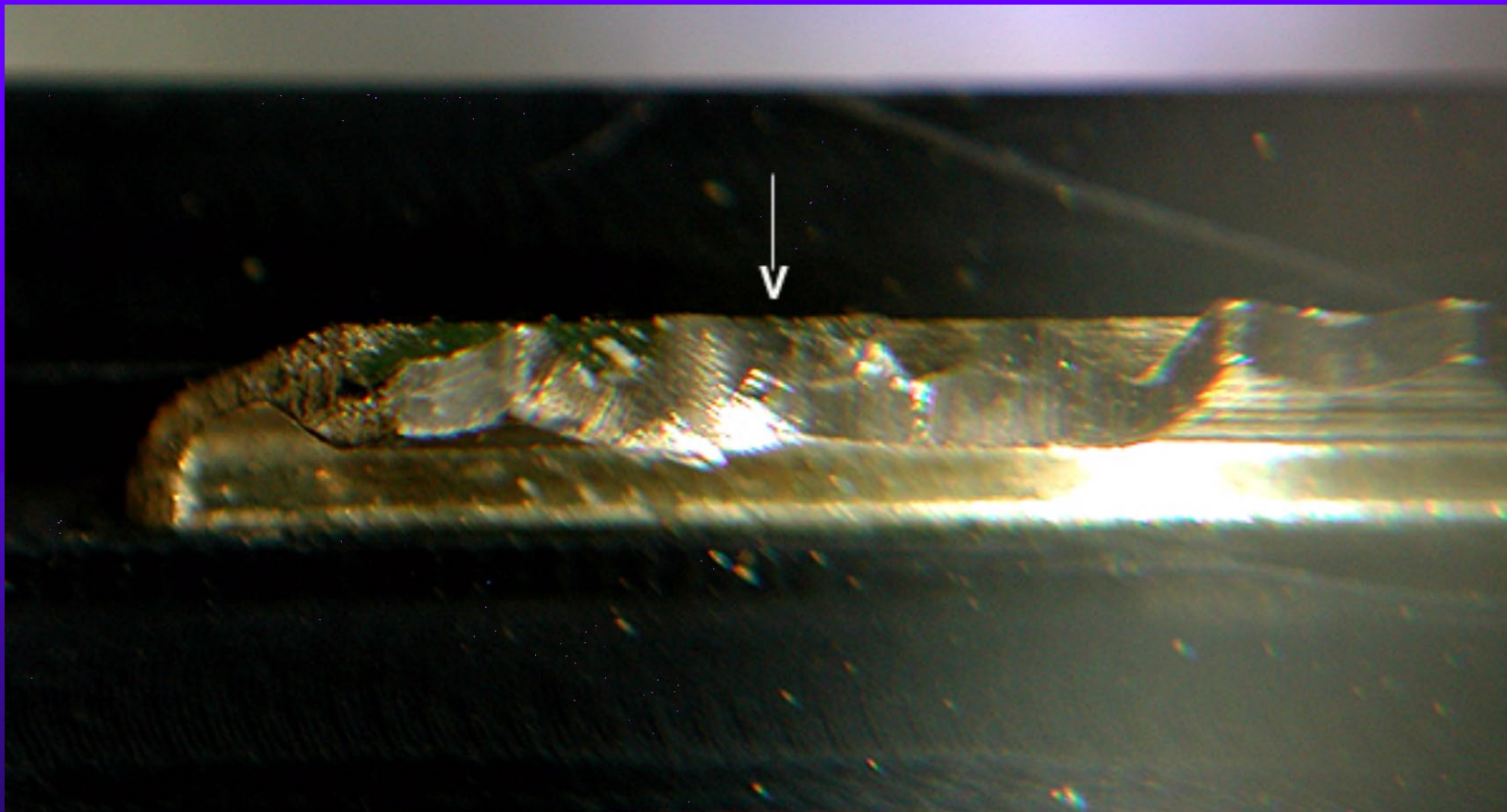
IMPRESSIONING



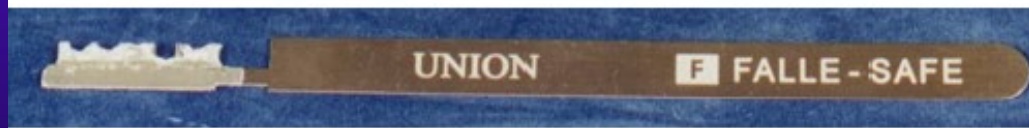
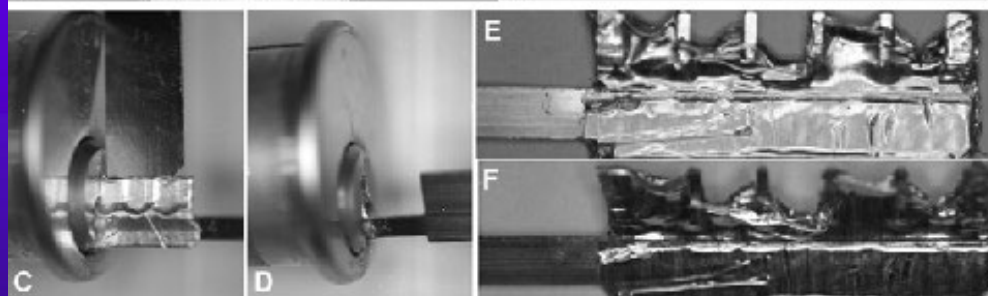
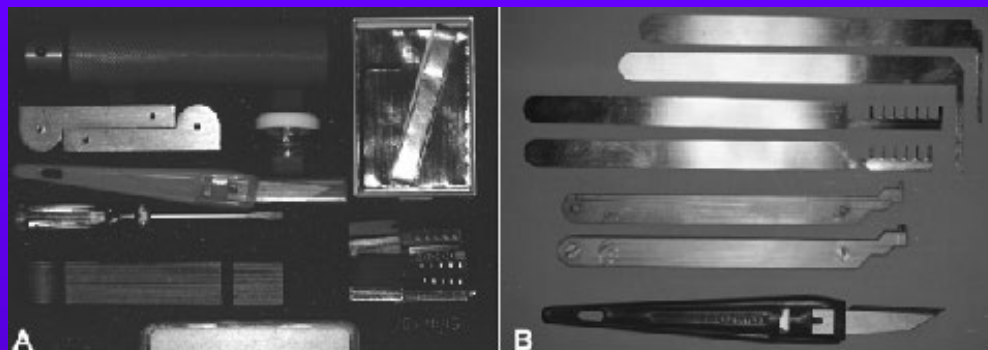
LEAD COMPOSITE IMPRESSIONING



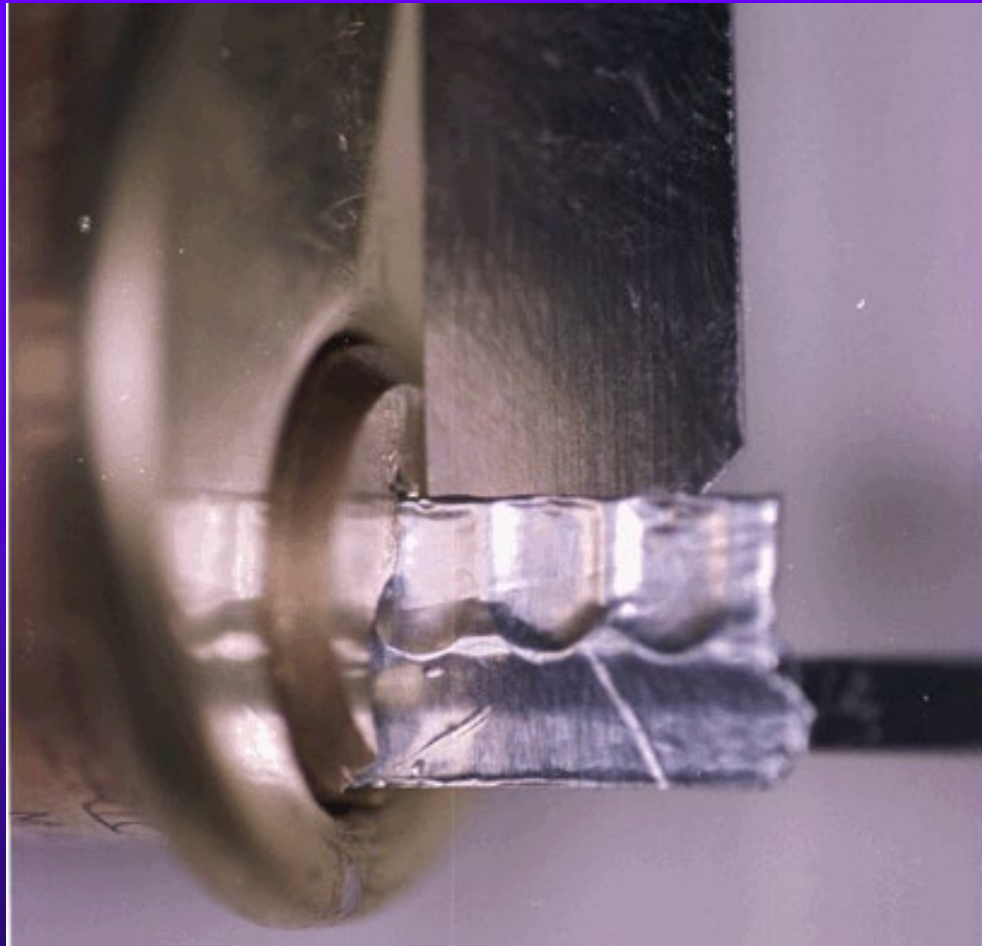
Marks are Produced



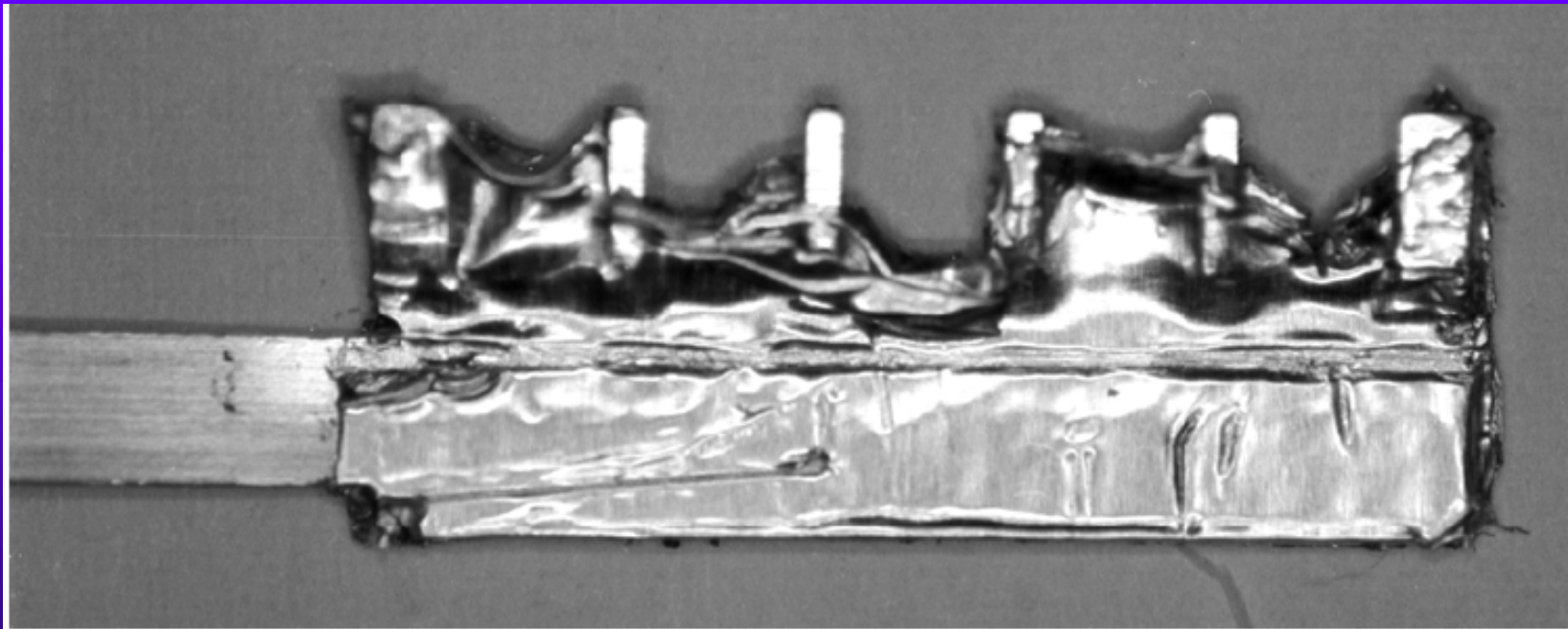
FOIL IMPRESSIONING TOOLS



Foil Blank Key is Inserted



Foil Key is Produced



Falle Foil impressioning



IMPRESSIONING LEVER LOCKS



IMPRESSIONING DIMPLE LOCKS



IMPRESSIONING DIMPLE WITH VIBRATION





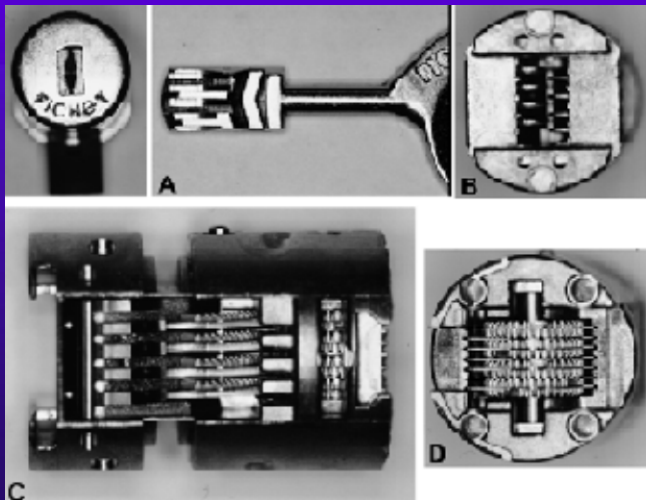
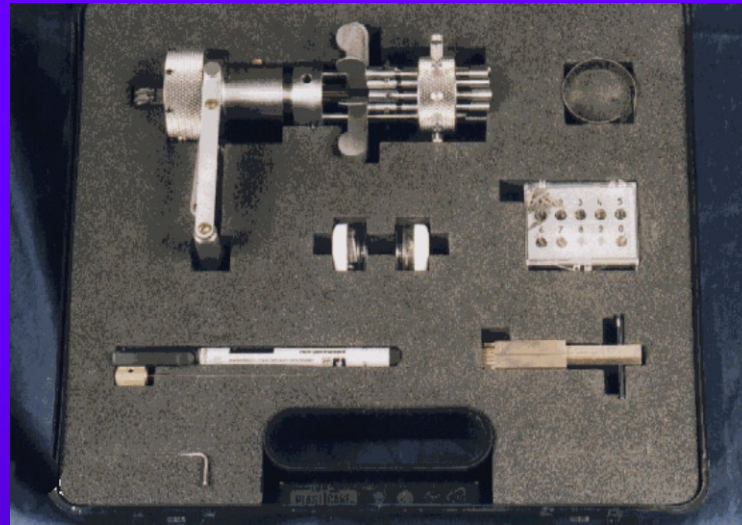
DECODING OF LOCKS

Many techniques

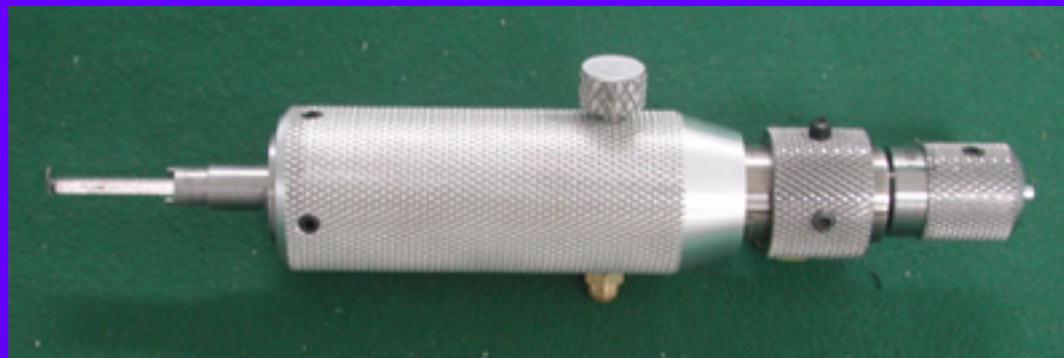
Many specialized tools

Derive key codes to simulate or generate a key

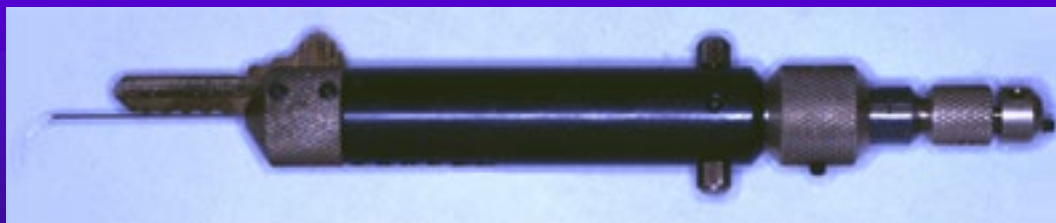
DECODING OF LOCKS



DECODING OF LOCKS



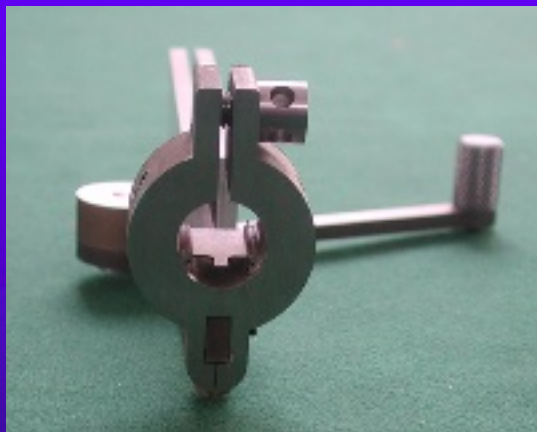
DECODING OF LOCKS



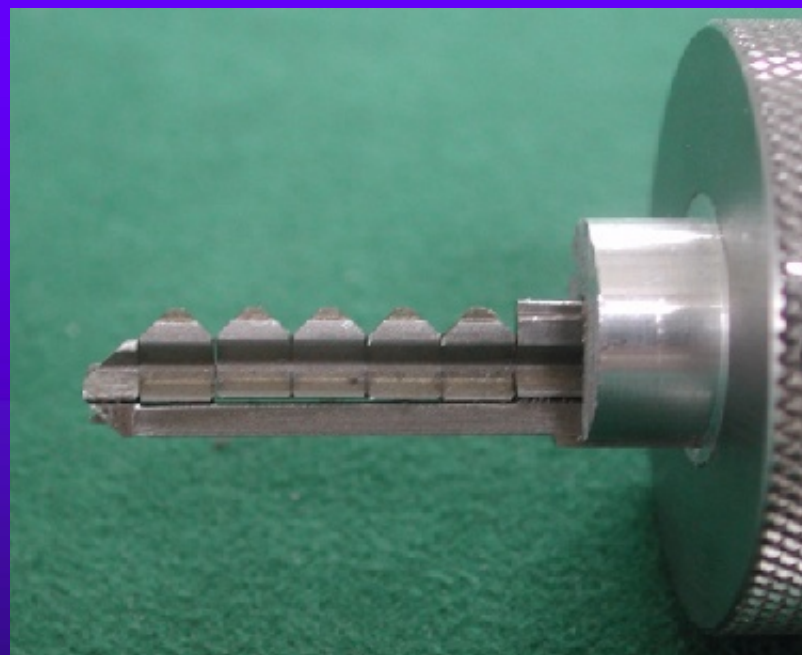
PICARD Pick



Evva 3KS Decoder



FALLE Pin Lock Decoder v.2



FALLE Pin lock decoder



Variable Key Generation



BORESCOPE DECODING



**Decoding
Medeco Biaxial
and m3 angles**

**Olympus Borescope
0.87mm diameter**



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

© 2004 Marc Weber Tobias