Attack the Key
Own the Lock

by datagram & Schuyler Towne

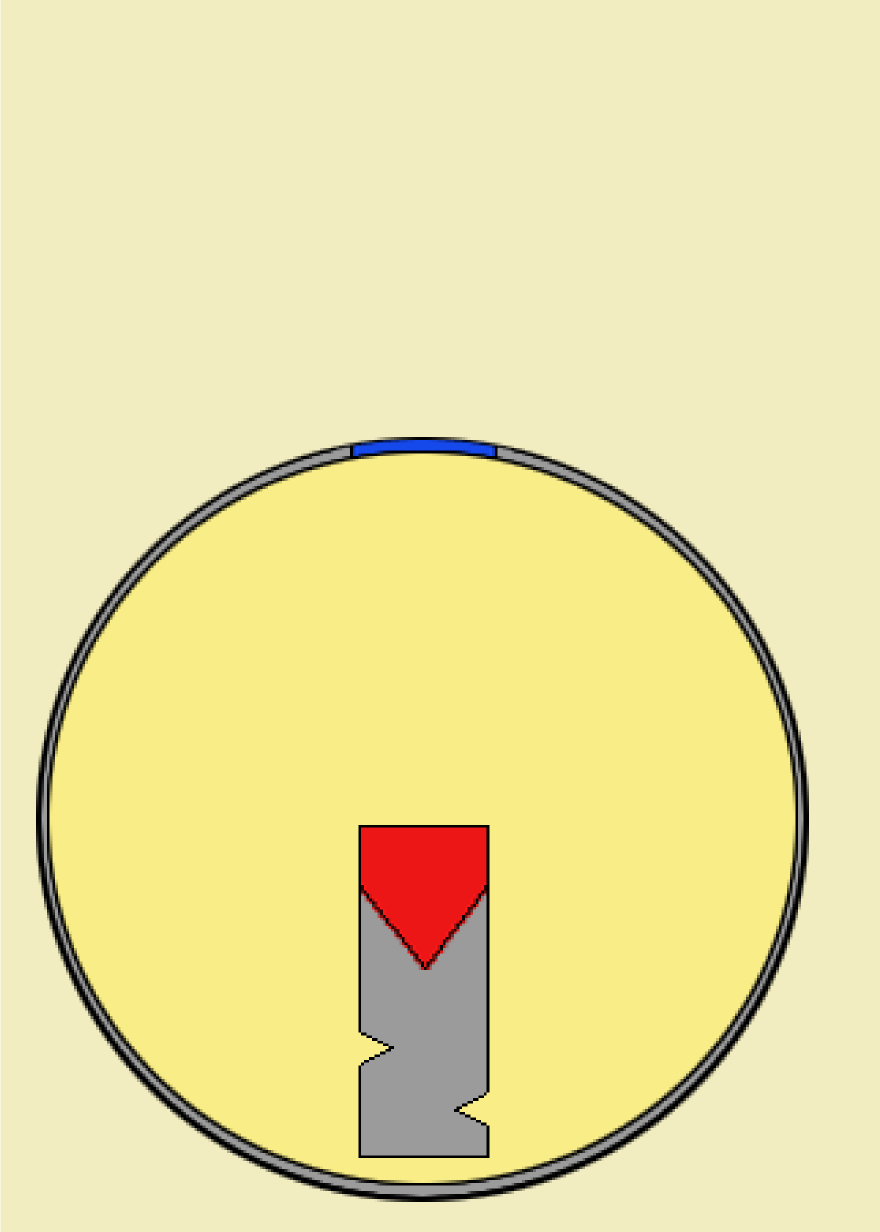
Defcon 18 (2010)
Las Vegas, NV

About Us

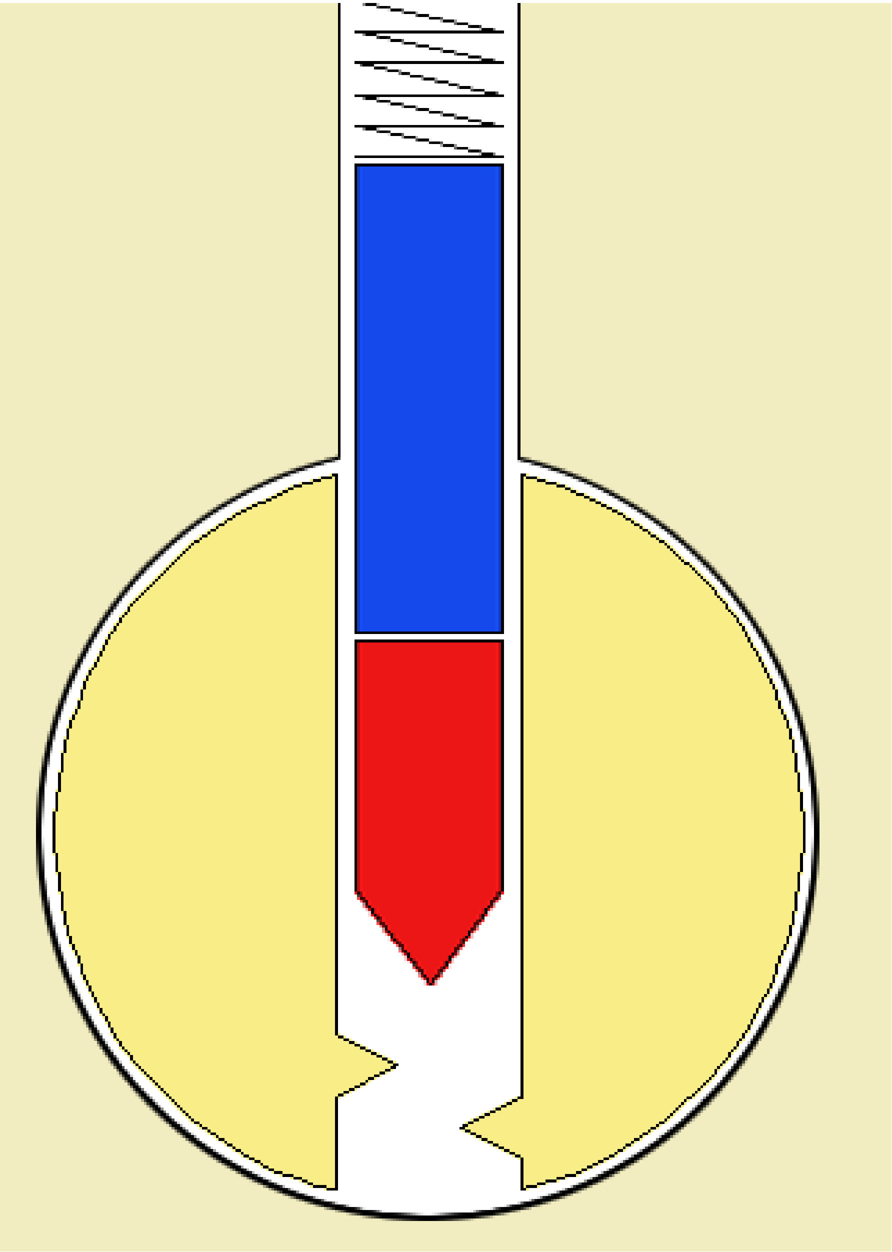
- Datagram
  - Forensic locksmith
  - Douchebag
  - No game shows :(

- Schuyler
  - TOOOL US
  - NDE Magazine
  - Wheel of Fortune

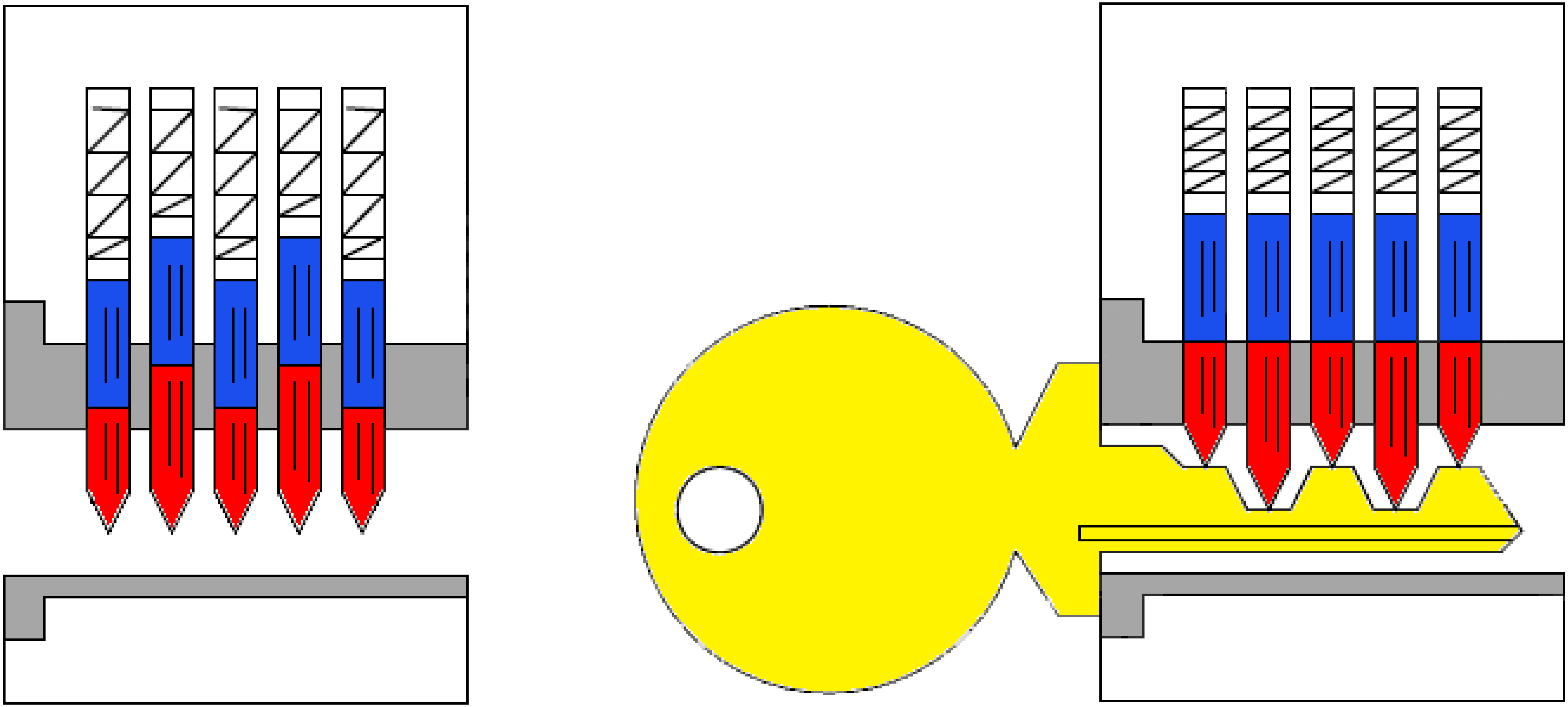
How Locks Work



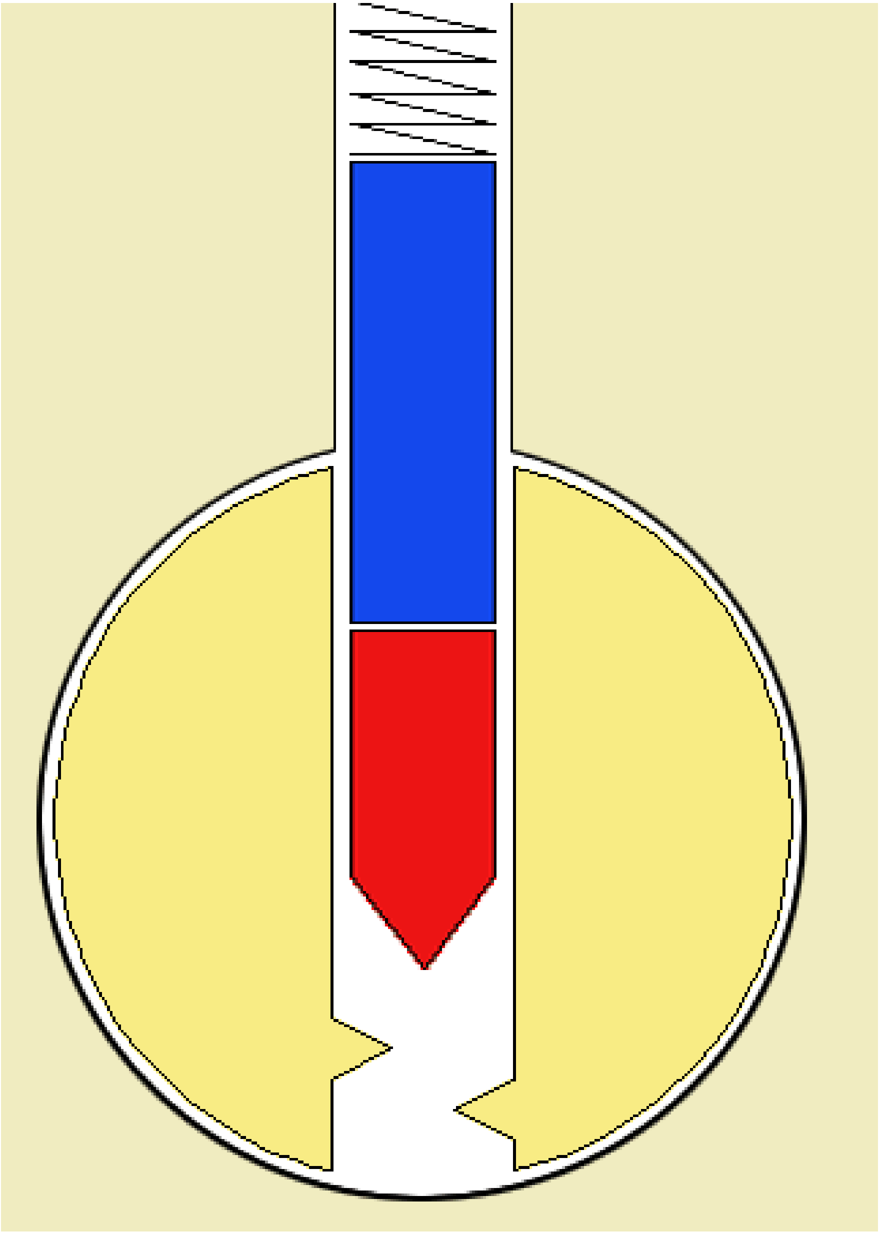
How Locks Work



How Locks Work



How Locks Work



Key Control

- Availability of blanks
- Distribution
- Duplication/simulation

Attacking the Key

- Bitting depths/code
- Keyway
- Model of the lock

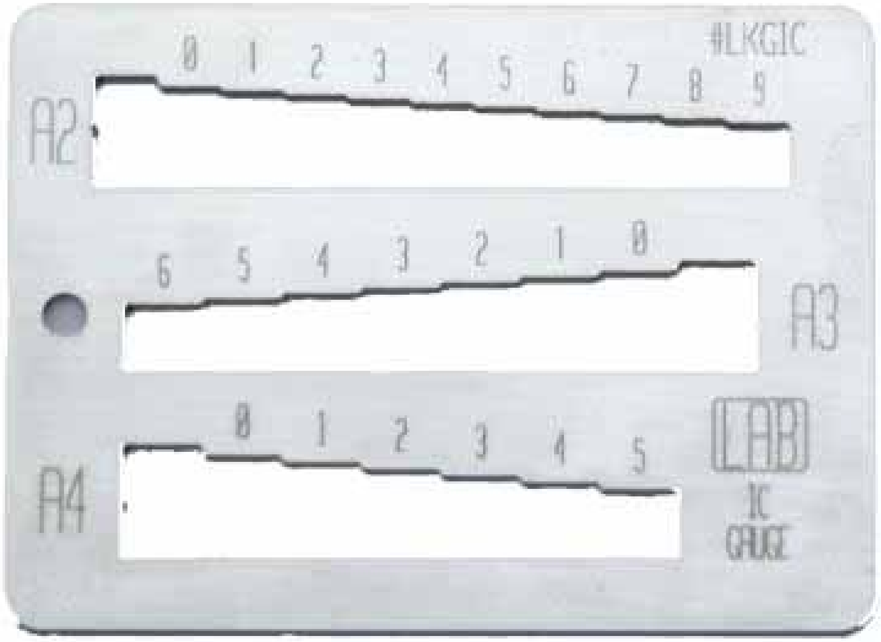
- Additional security features

Physical Access to Keys

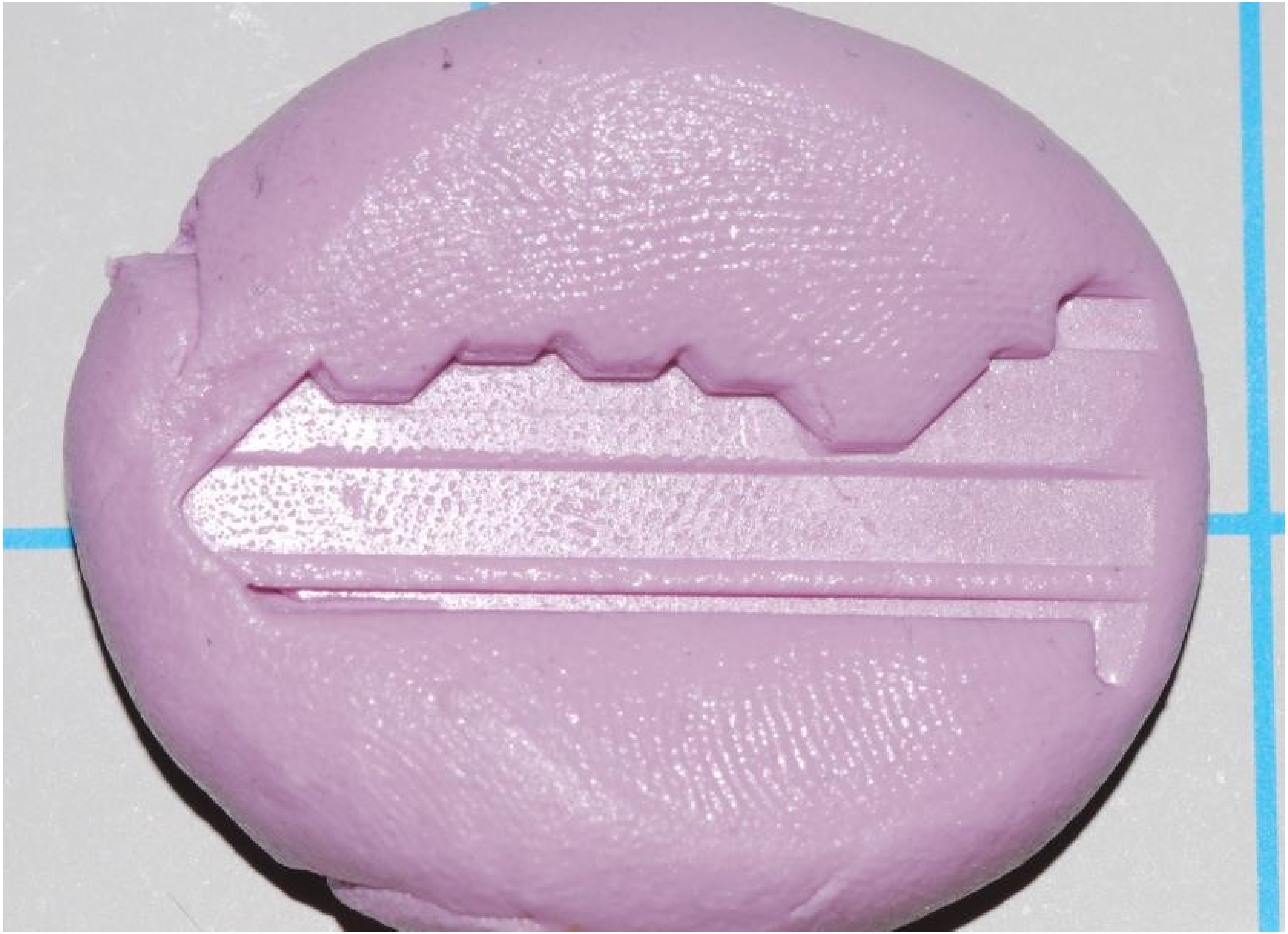
- Holy Grail
- Duration = Attack Quality
- Wrist Impressioning

Direct Measurement

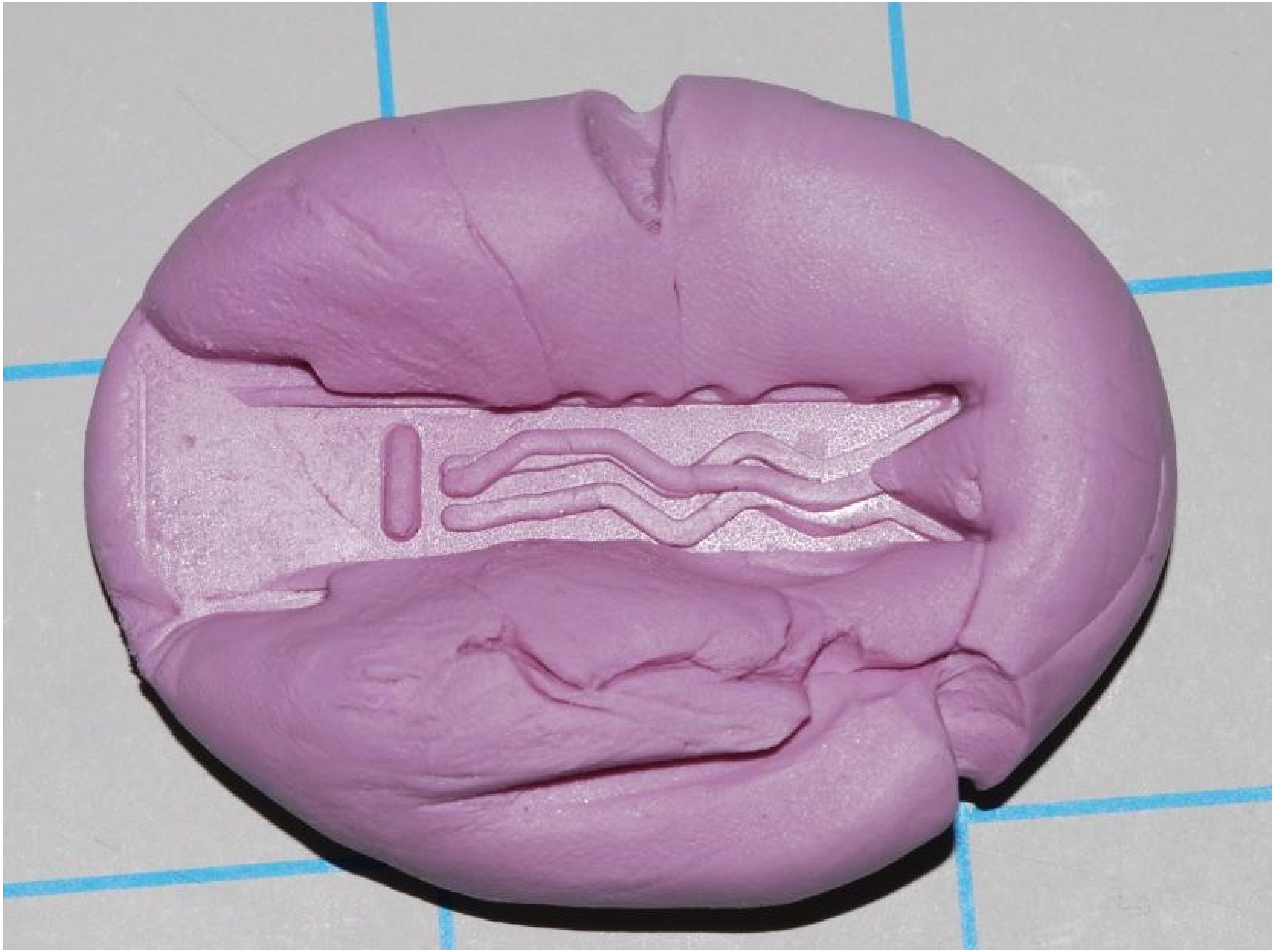
- Key gauges
- Micrometer
- Calipers



Copy Impressioning



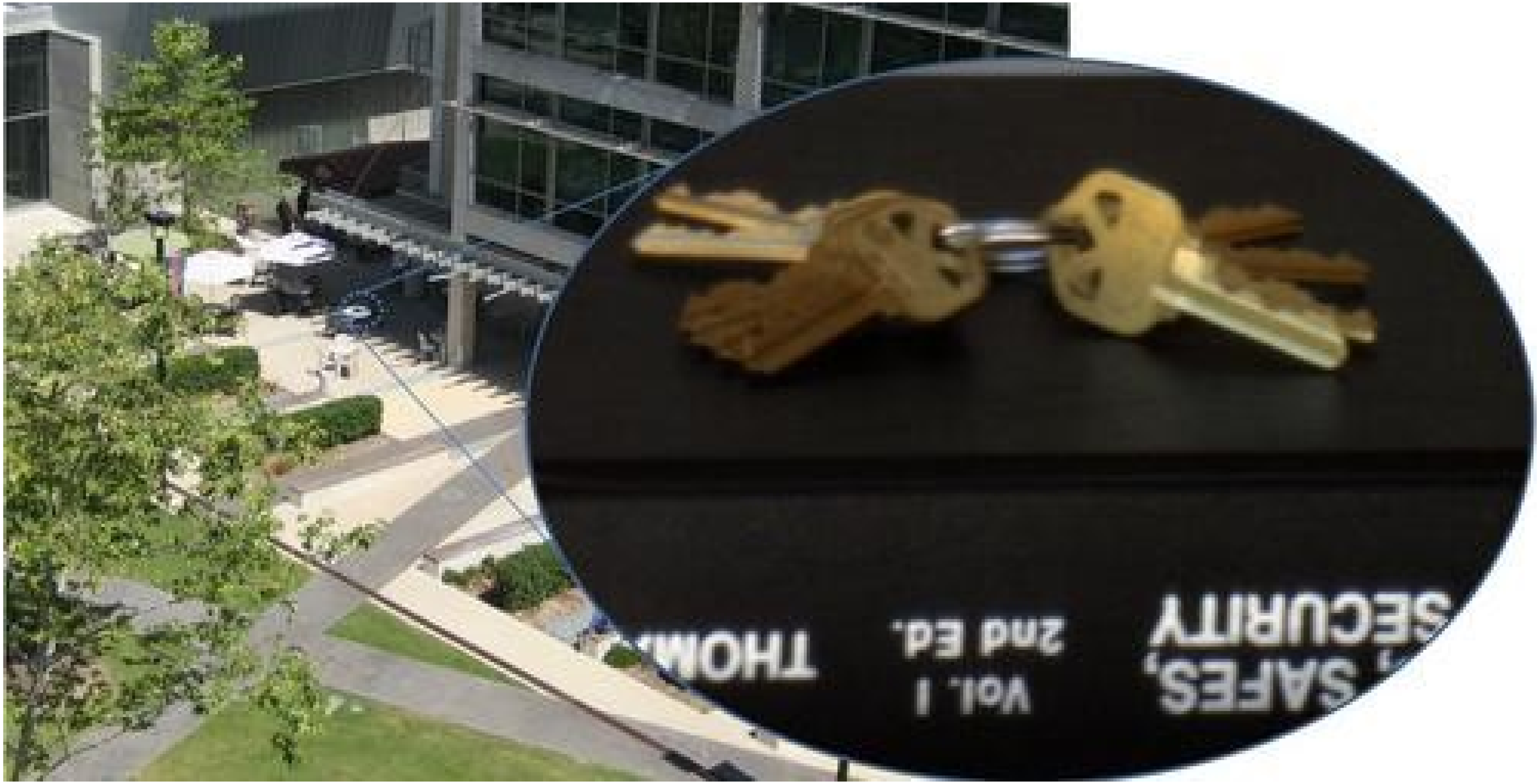
Copy Impressioning



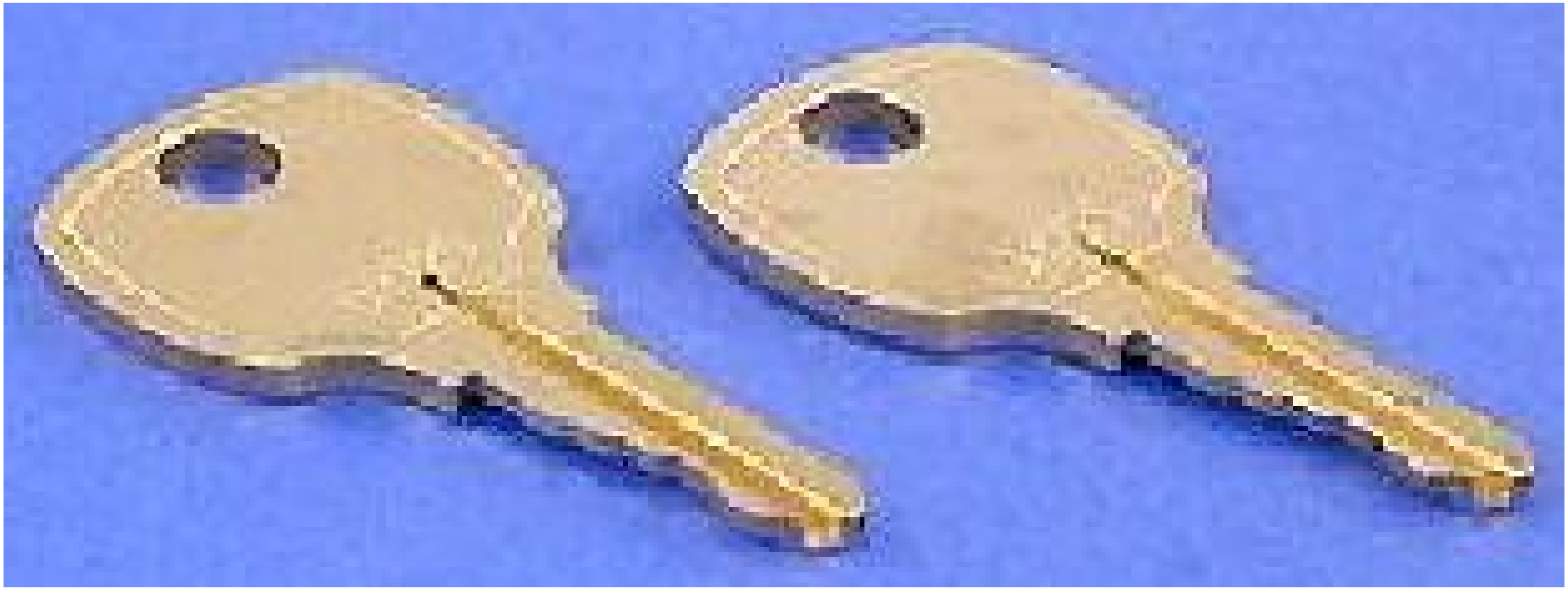
Visual Access to Key

- Sight reading
- Estimation
- Photography

Visual Access – UCSD



Visual Access - Diebold

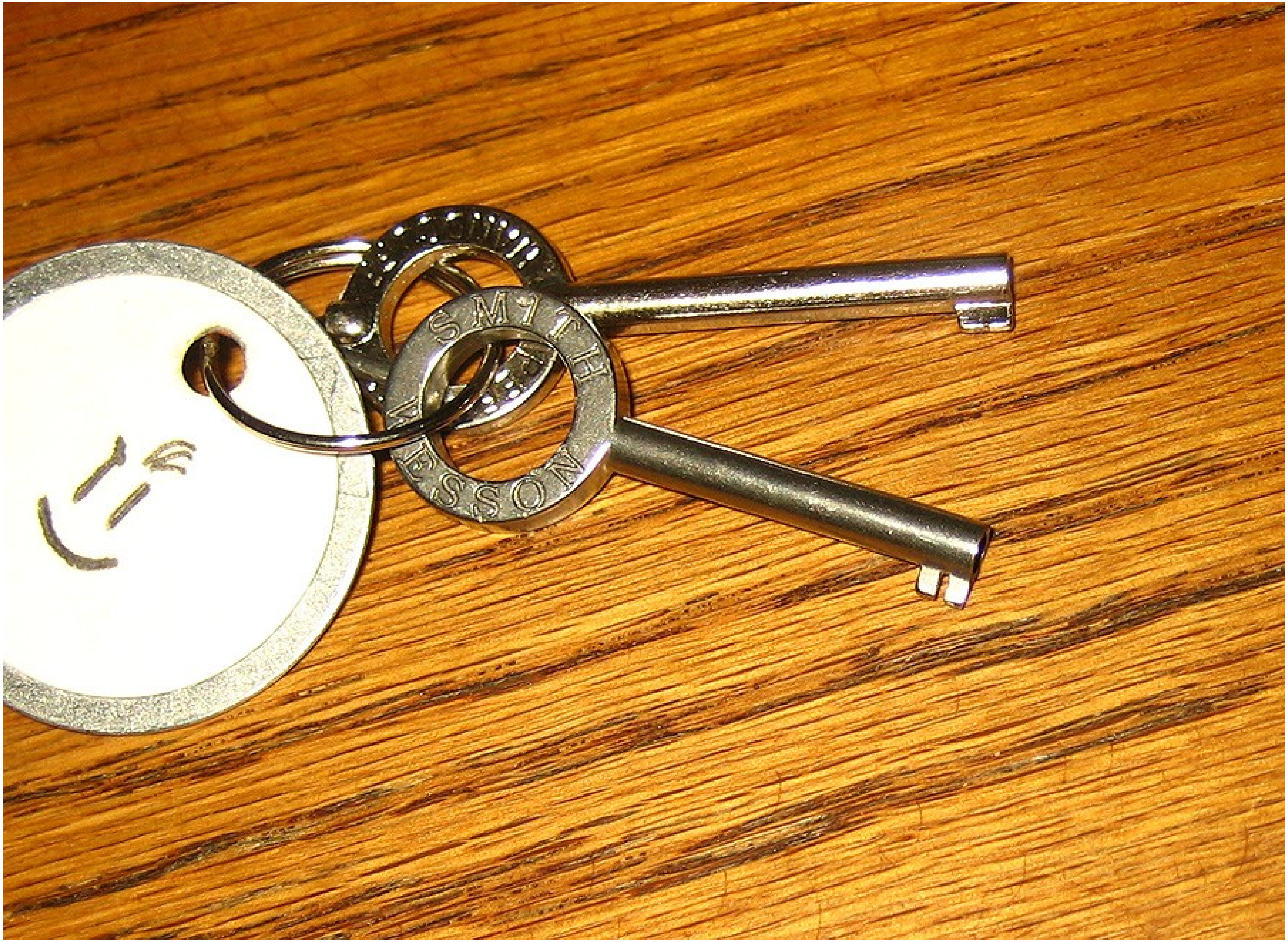


Visual Access – NY MTA

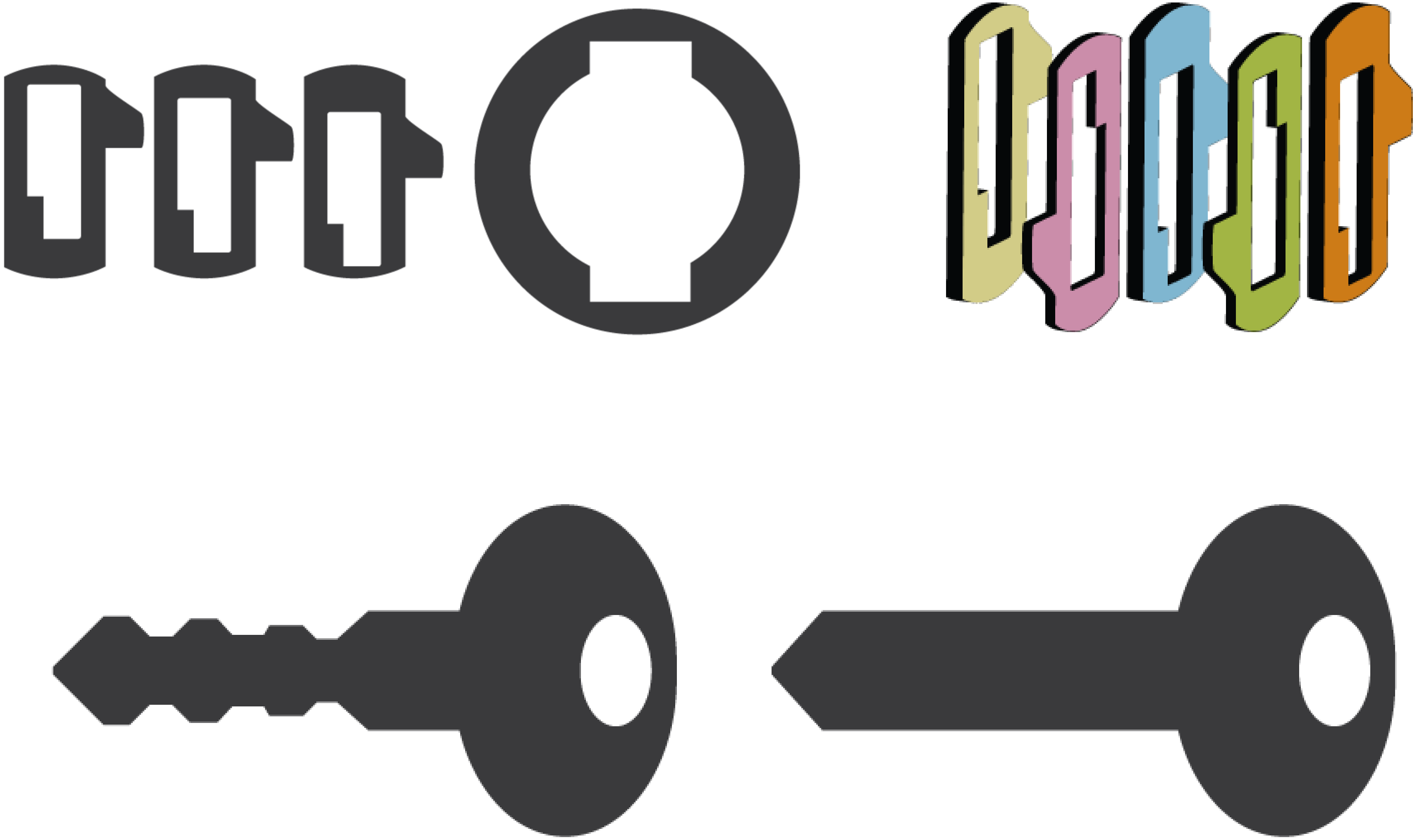
Key Blanks

- Impressioning
- Overlifting
- “Reflecting” keys
- Sectional keyways
- Rake keys
- Key bumping

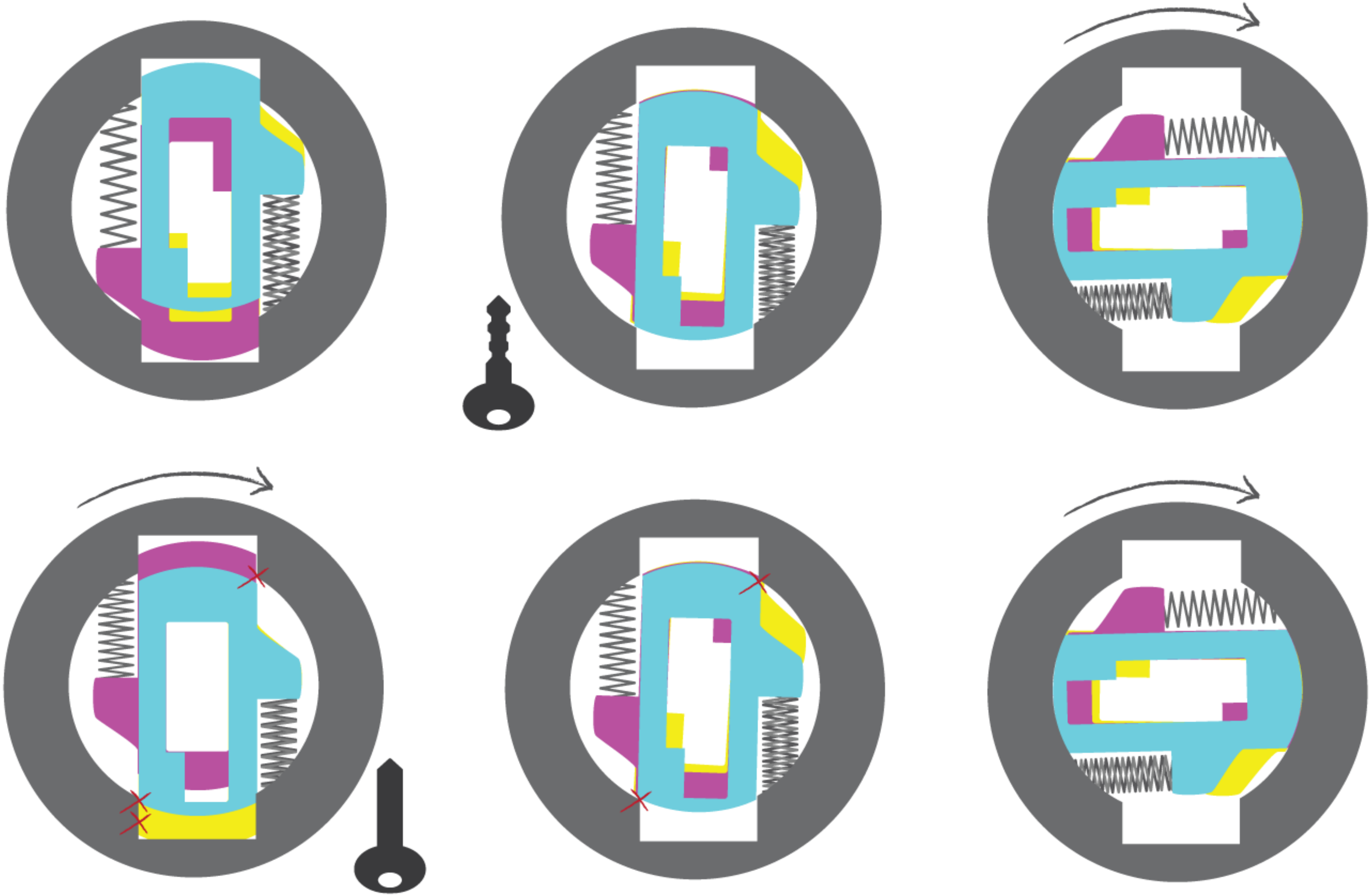
Universal Handcuff Keys



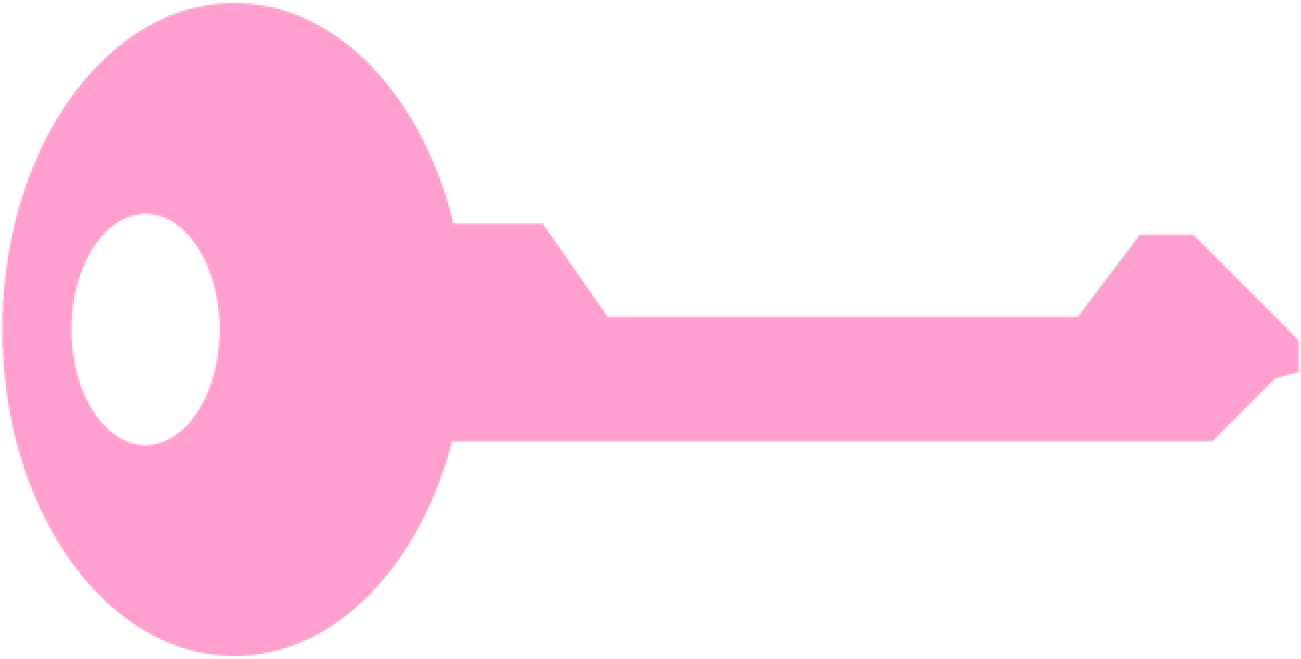
Overlifting



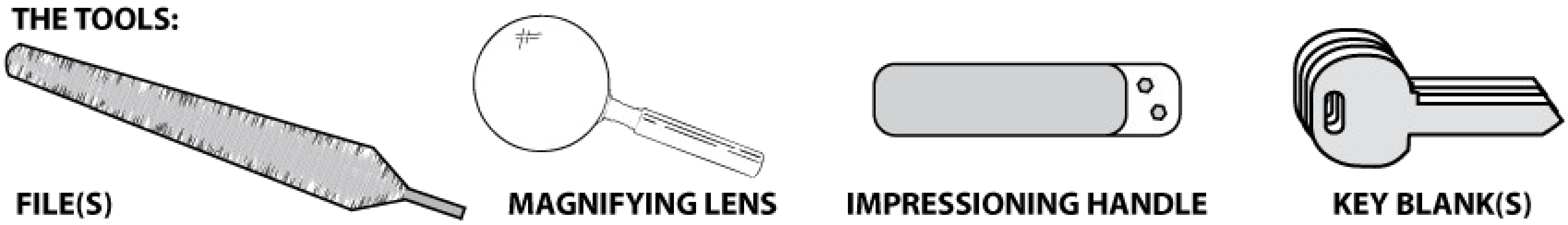
Overlifting

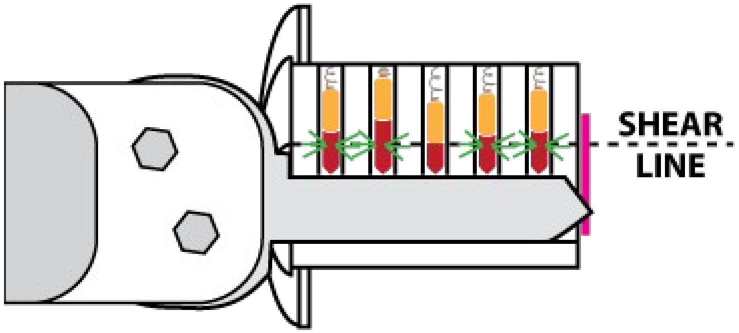


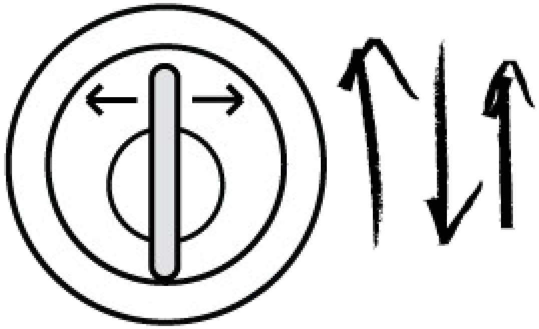
Rake/Gypsy Keys

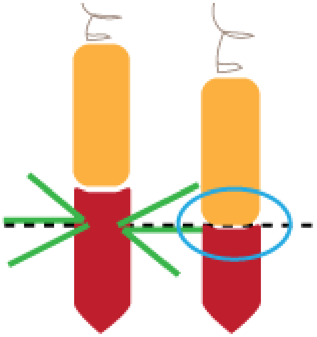


Impressioning

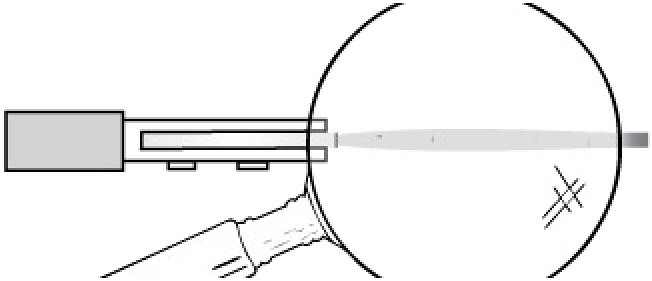


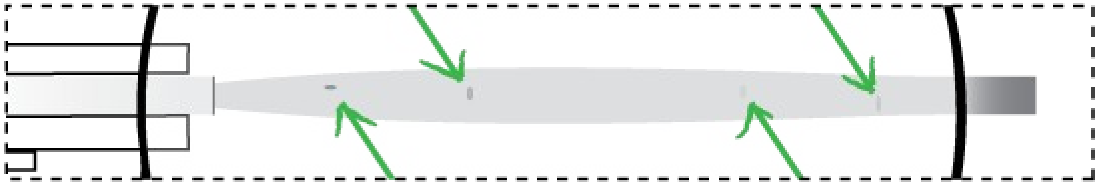


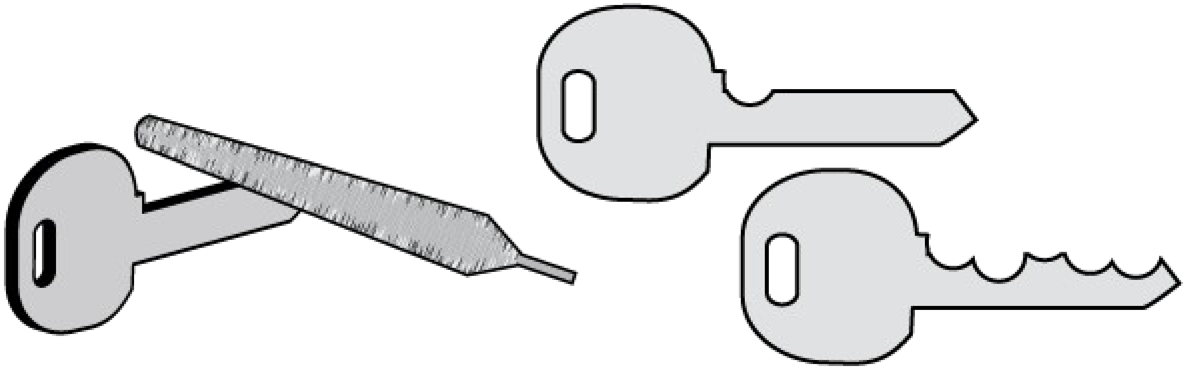




Impressioning

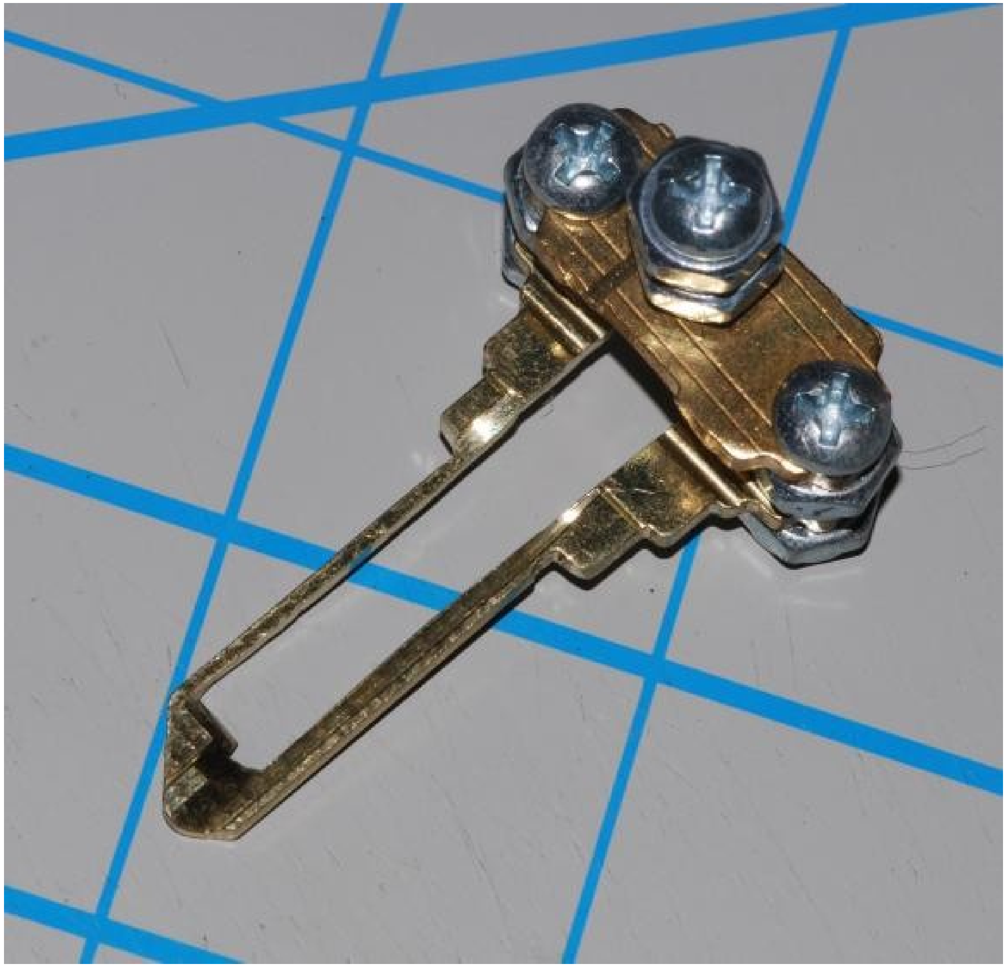


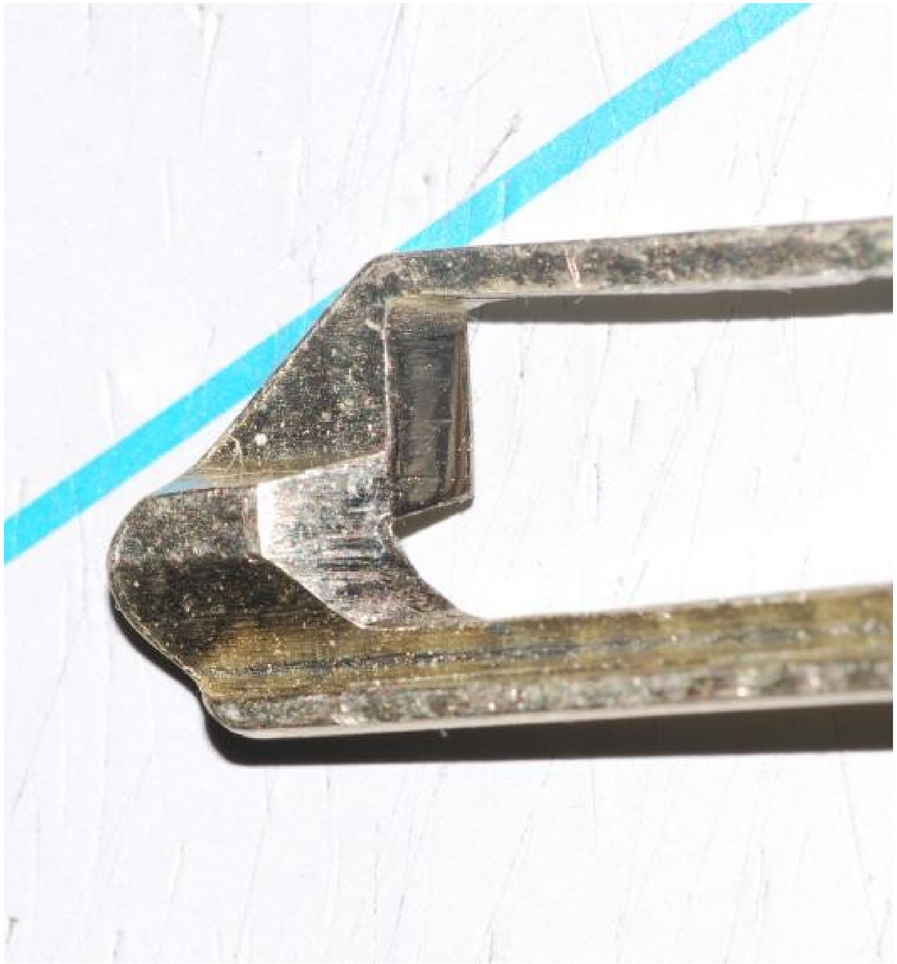




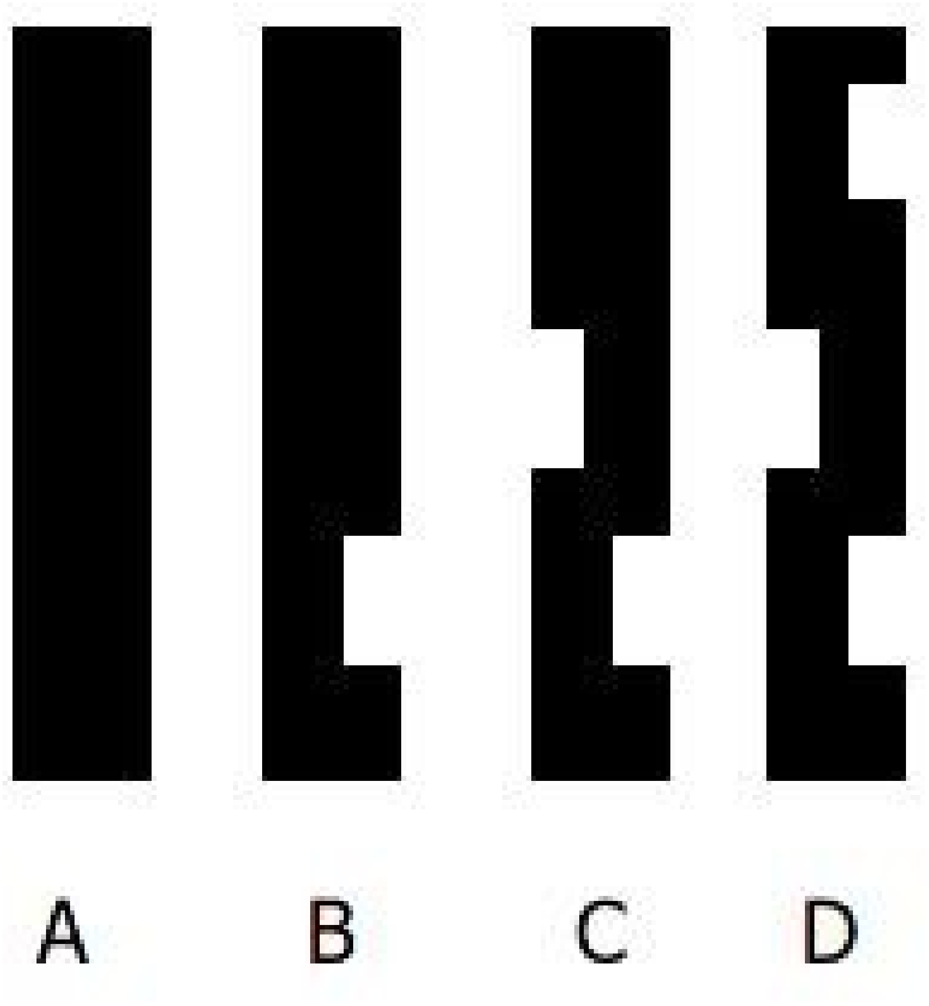
Works Forever!

Reflecting Keys

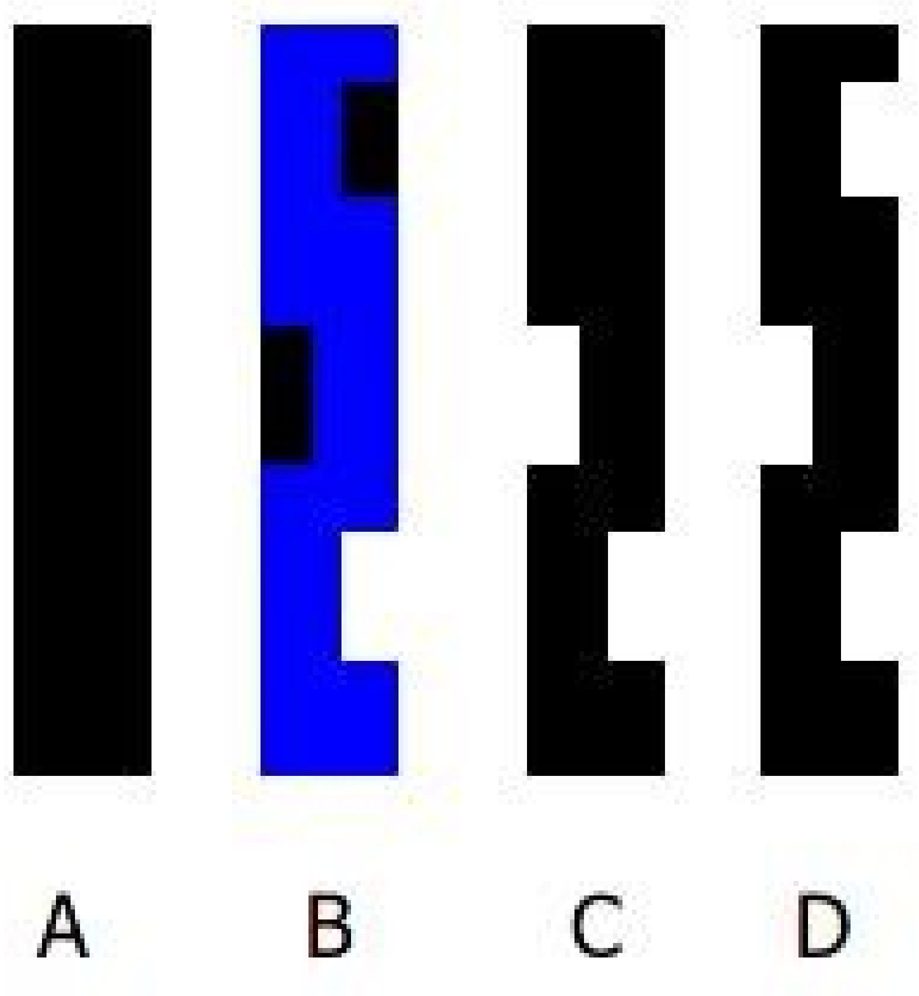




Sectional Keyways



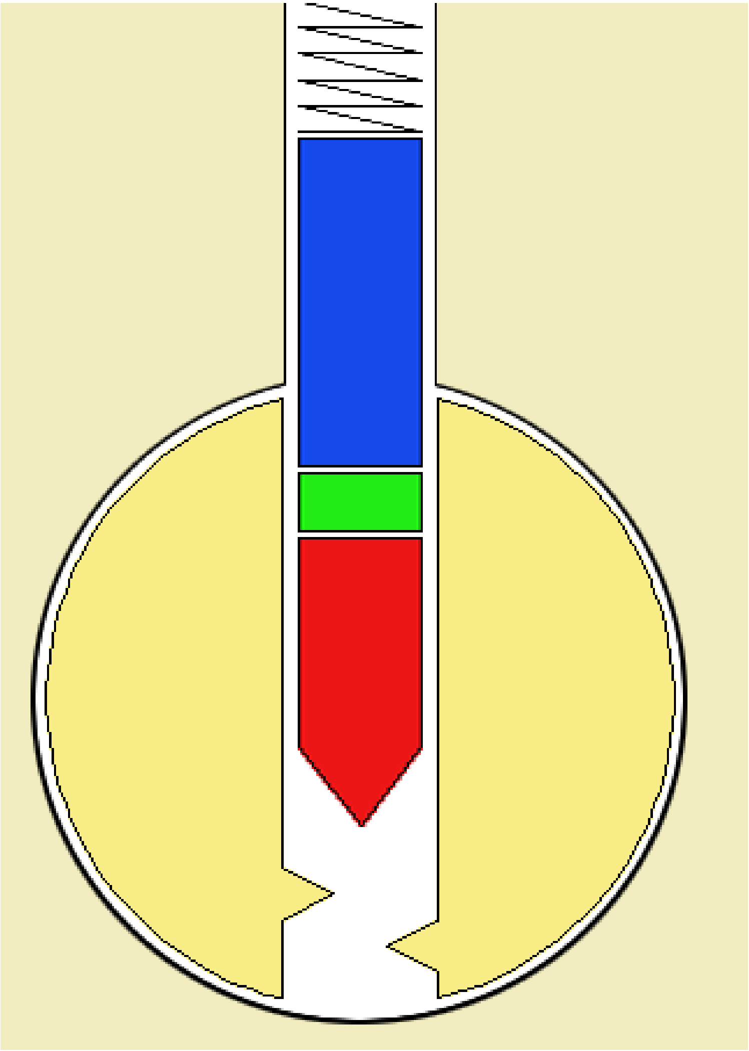
Sectional Keyways

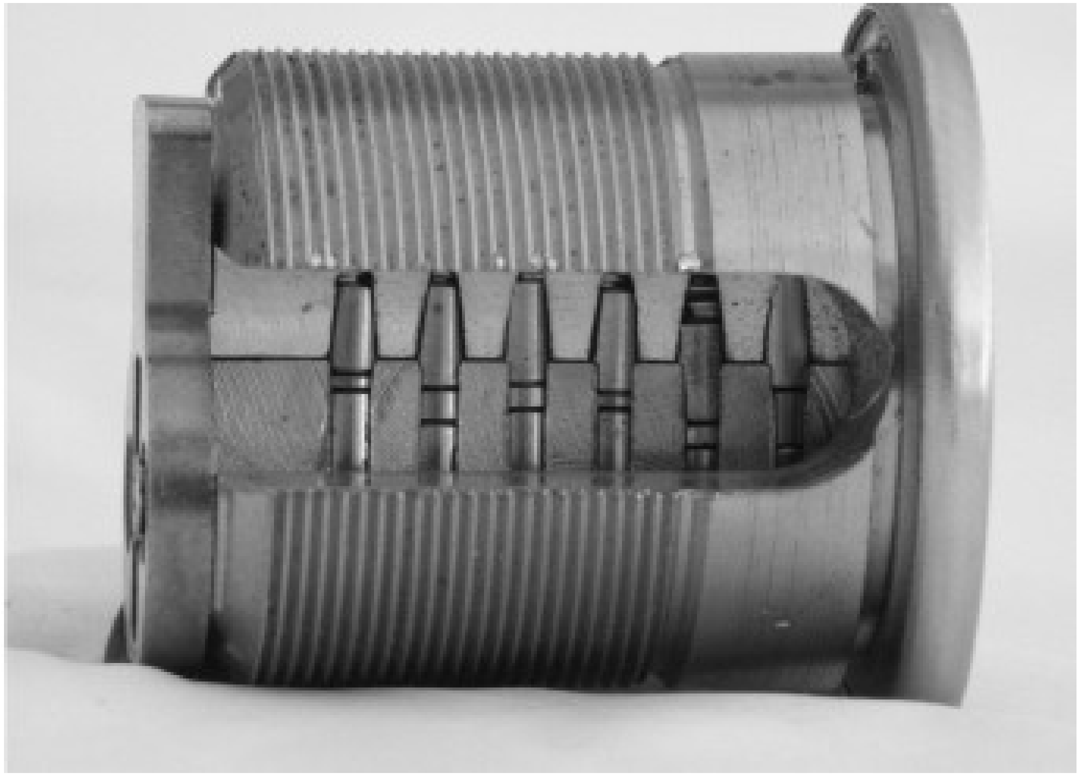


Incorrect Key

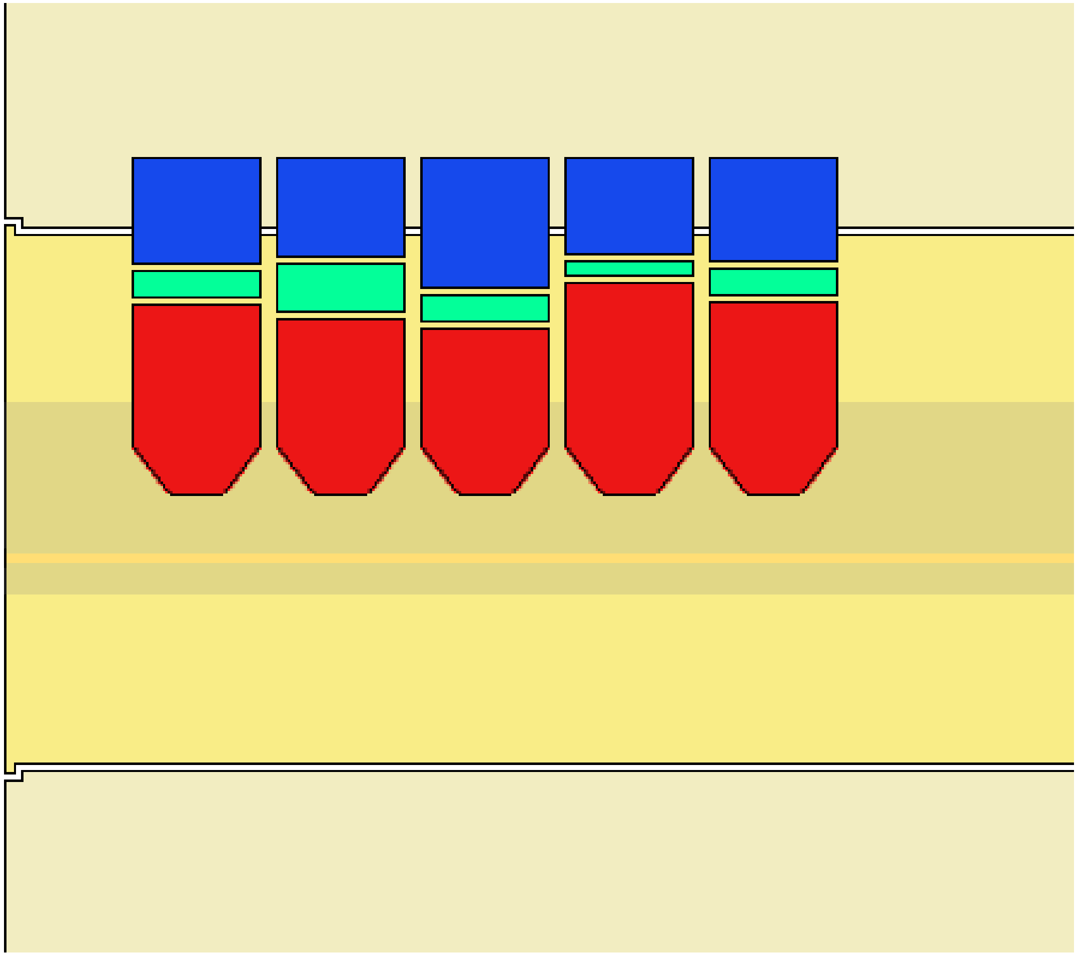
- Master key decoding
- Bumping
- Skeleton keys
- Sidebar attacks
- Passive component bypasses
- Decoding attacks

Master Key Systems

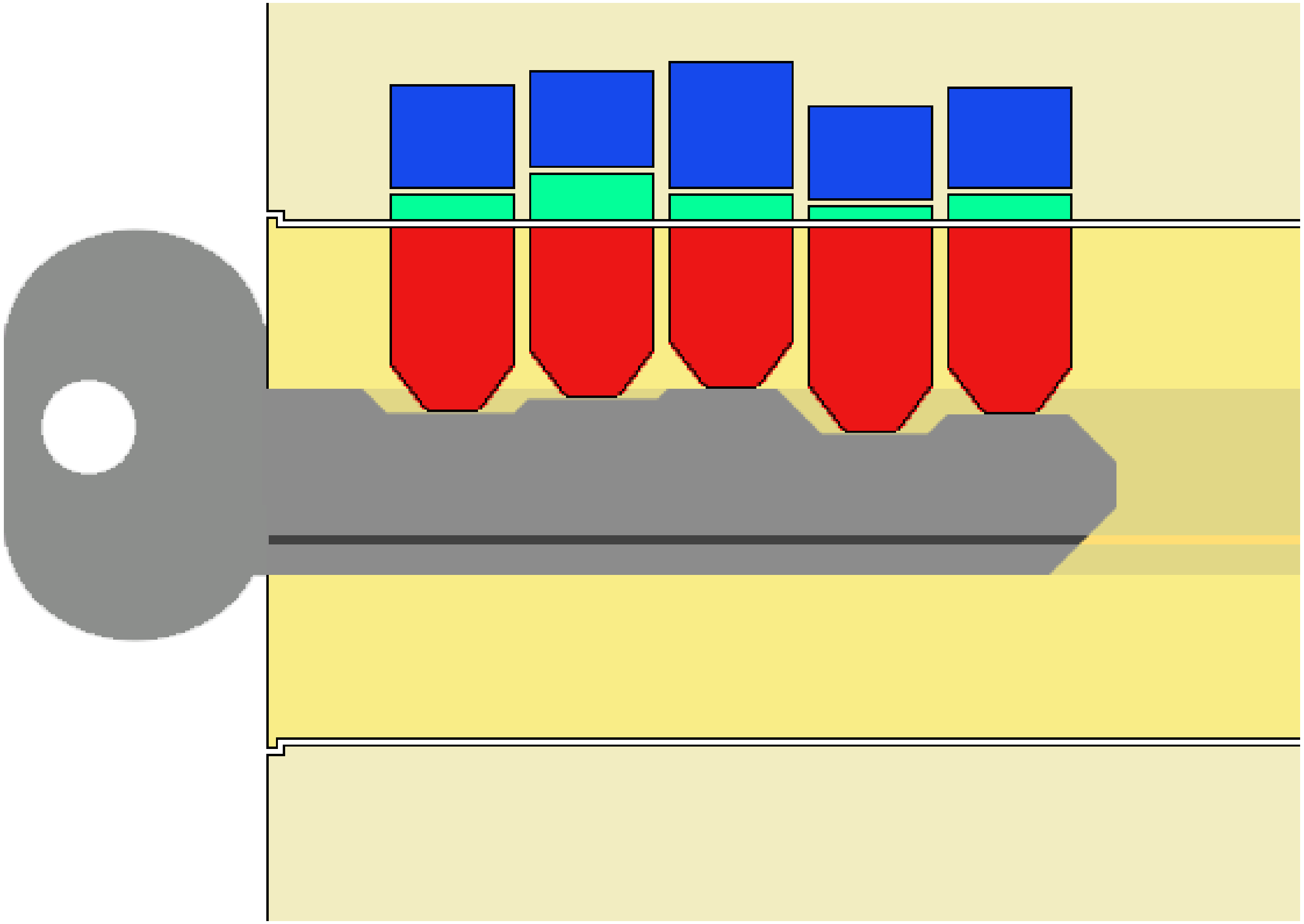




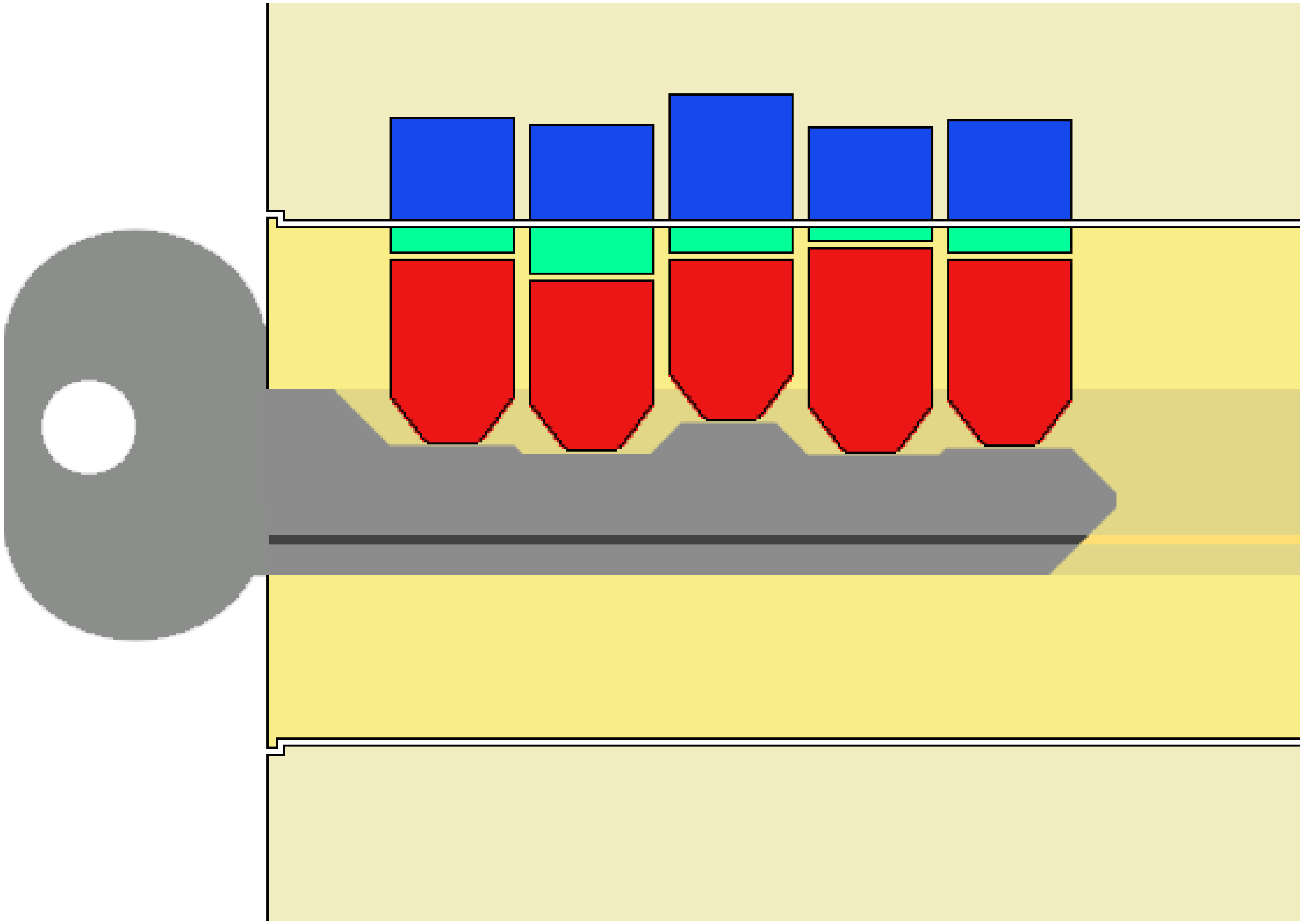
Master Key Systems



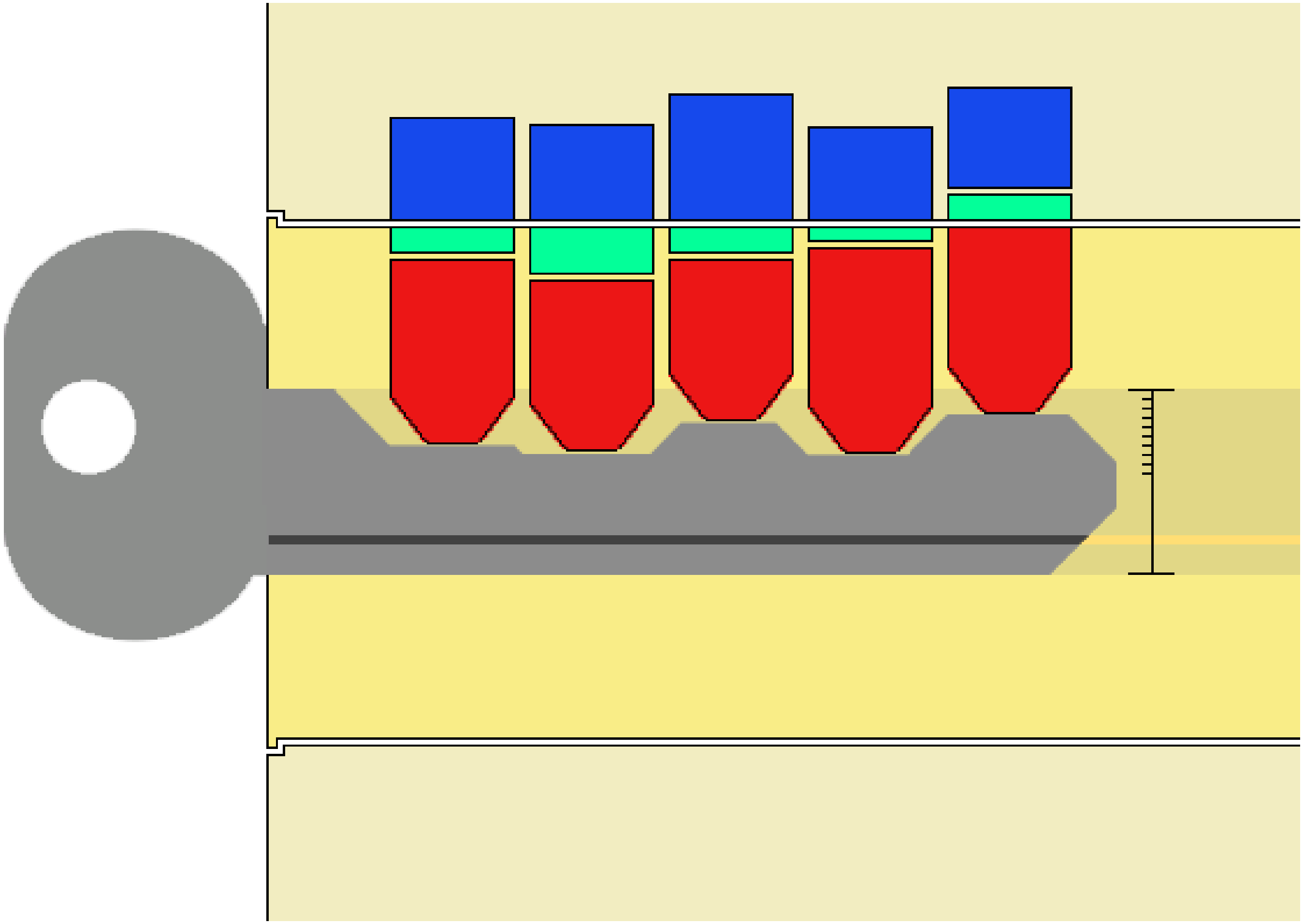
Master Key Systems



Master Key Systems

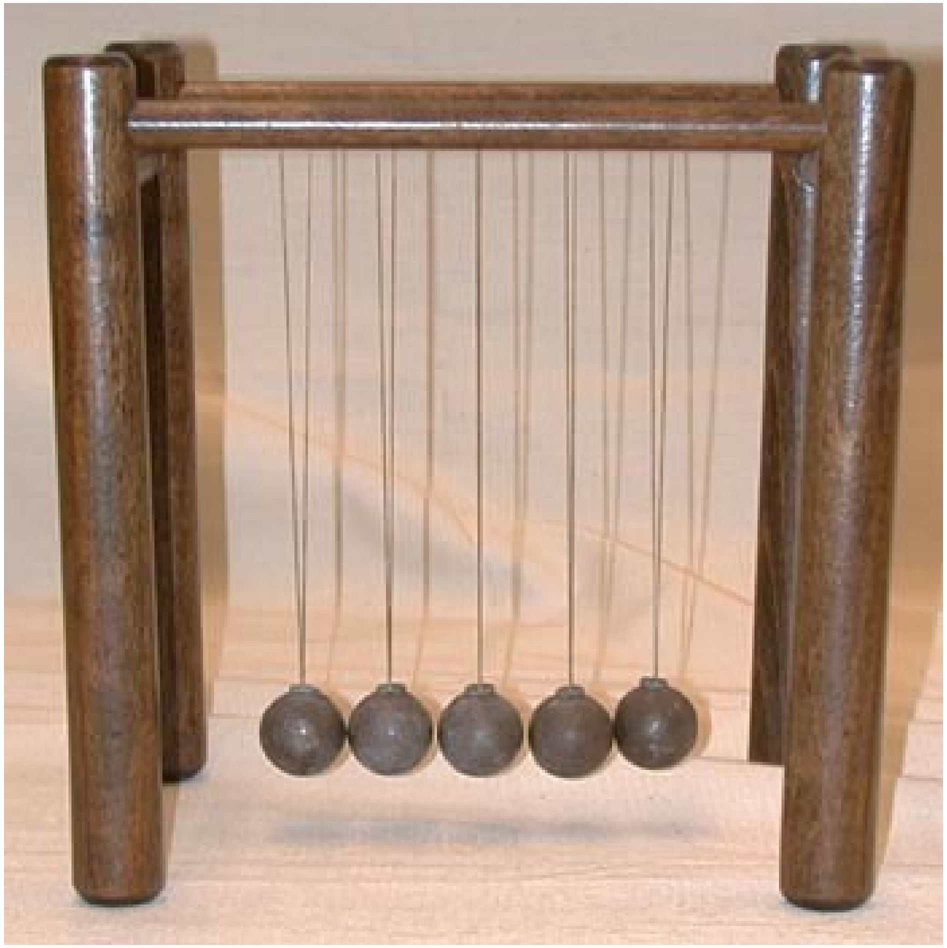


Master Key Systems

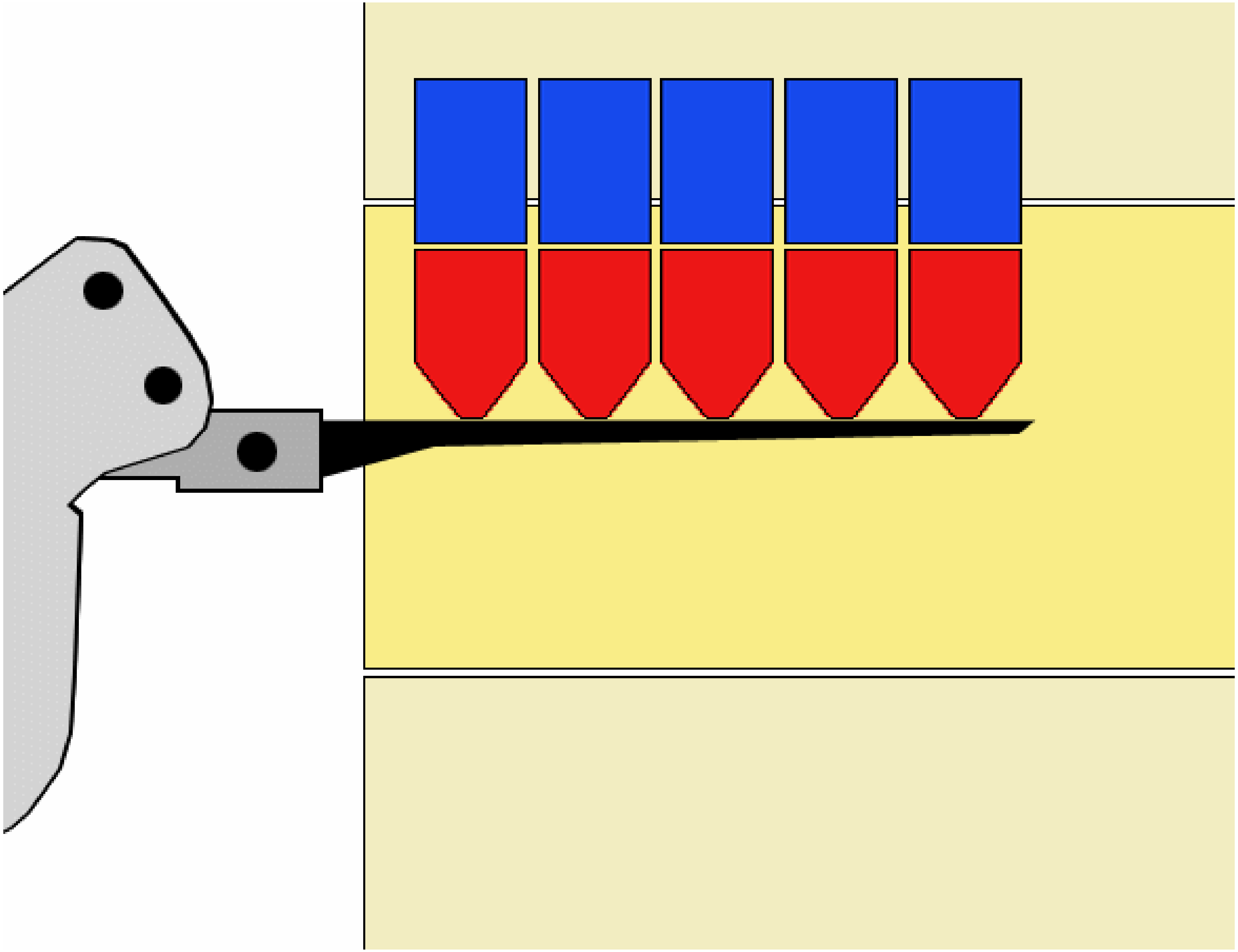


Key Bumping

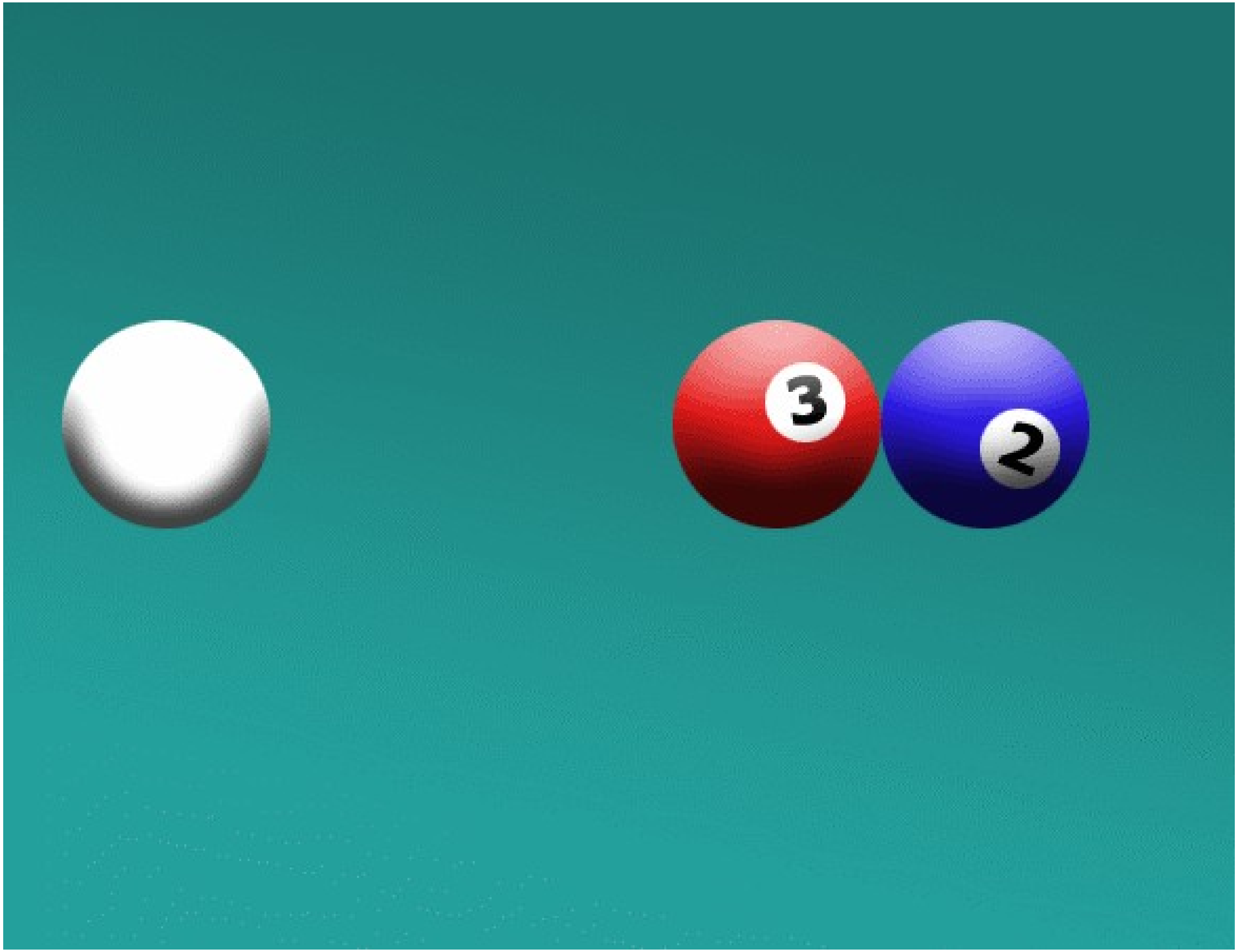
- Basic physics
- Specialized key
- Easy, effective
- Vendor response



Pick Gun Mechanics

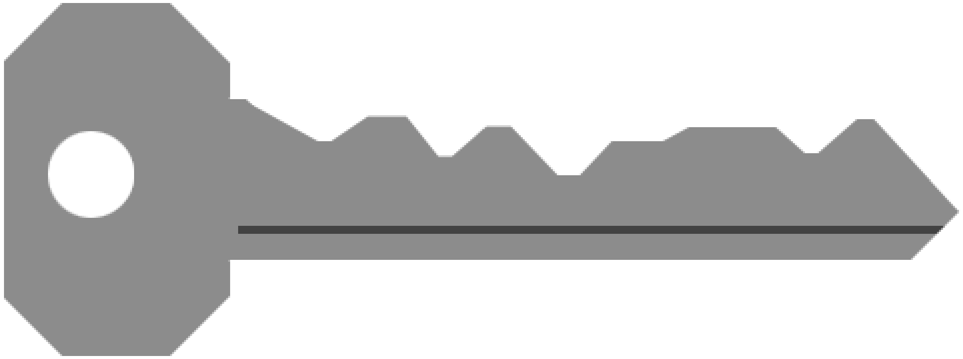


How Bumping Works



Creating Bump Keys

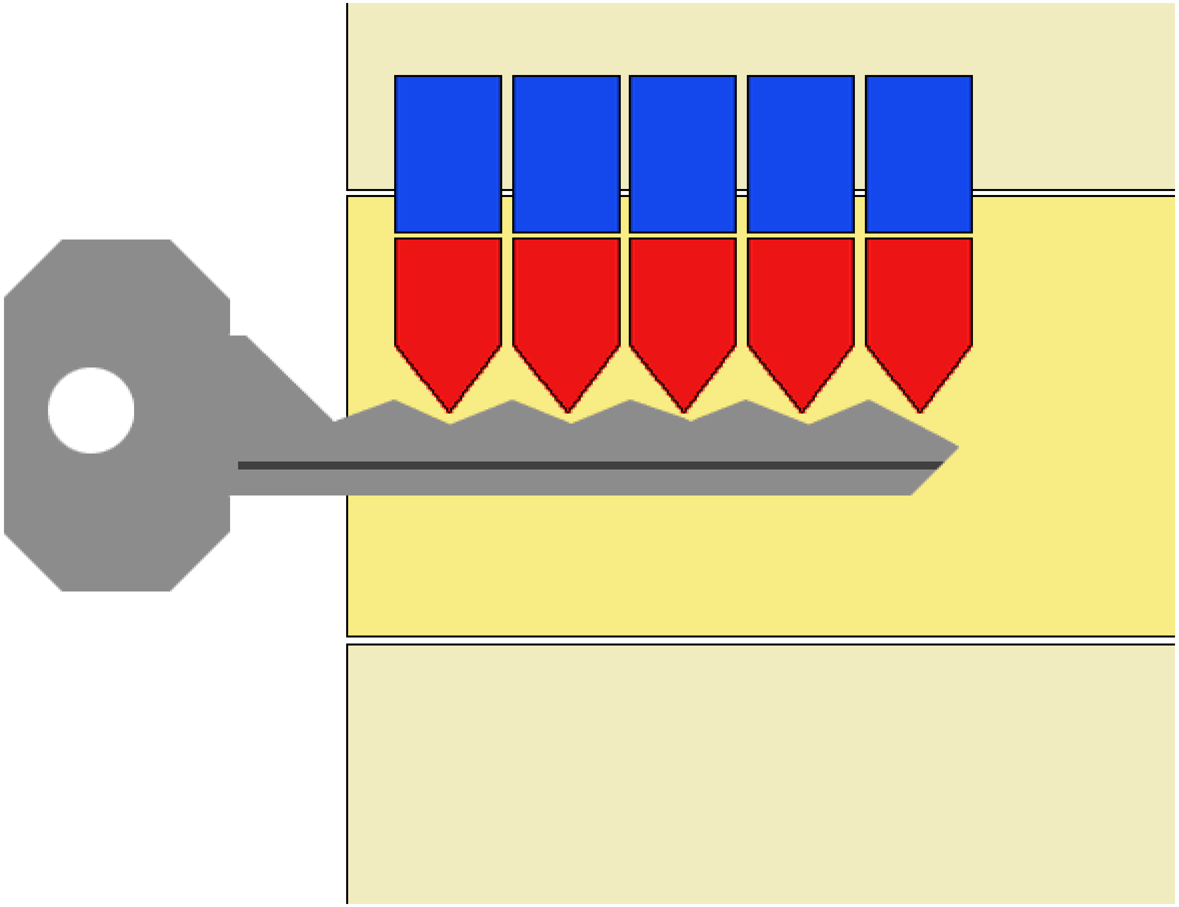
- Any key that fits
- Cut “999” key (deepest pin depths)
  - Use key gauges



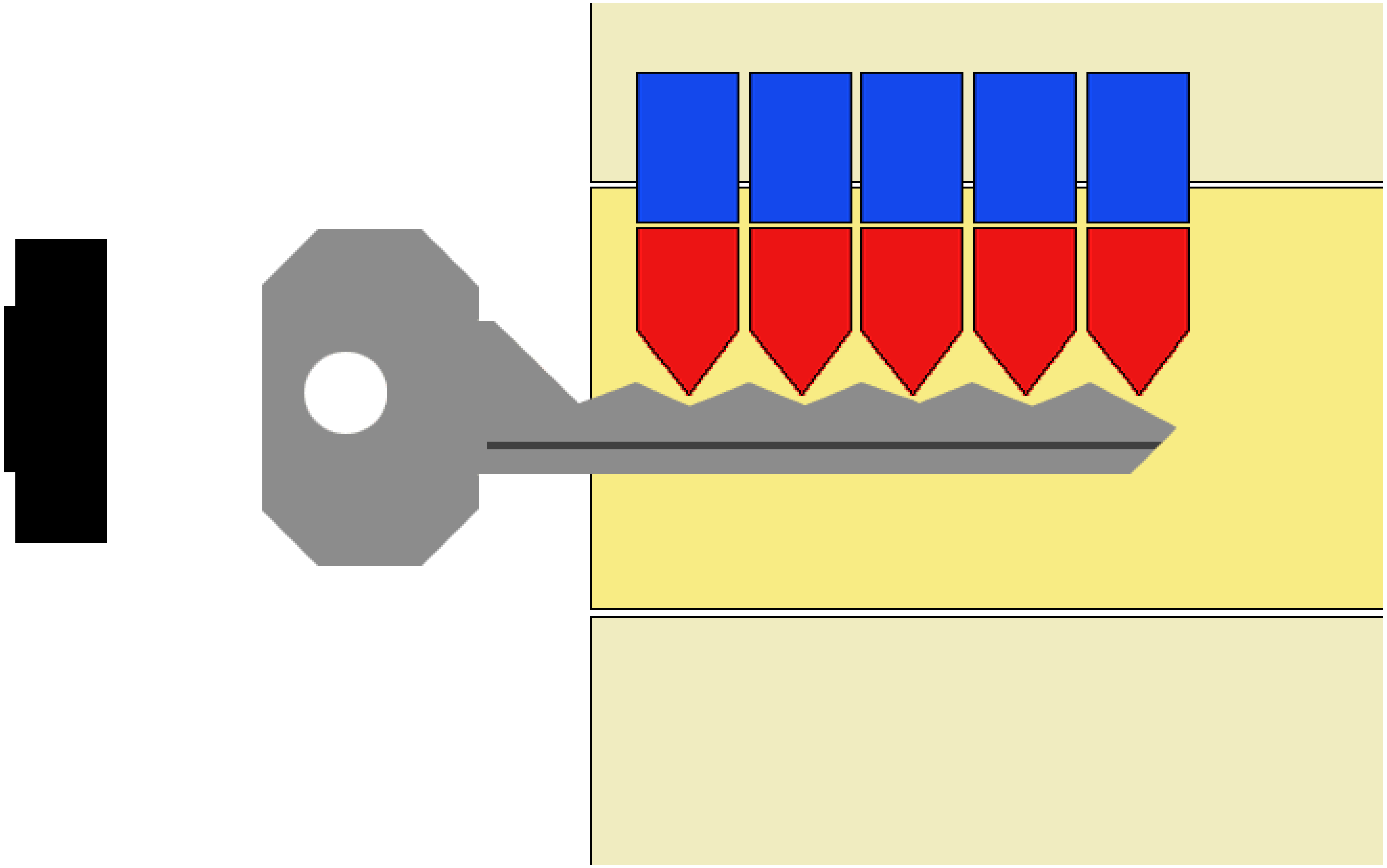
- Cut with
  - Hand file, dremel, key cutter

Bump Keys

Key Bumping



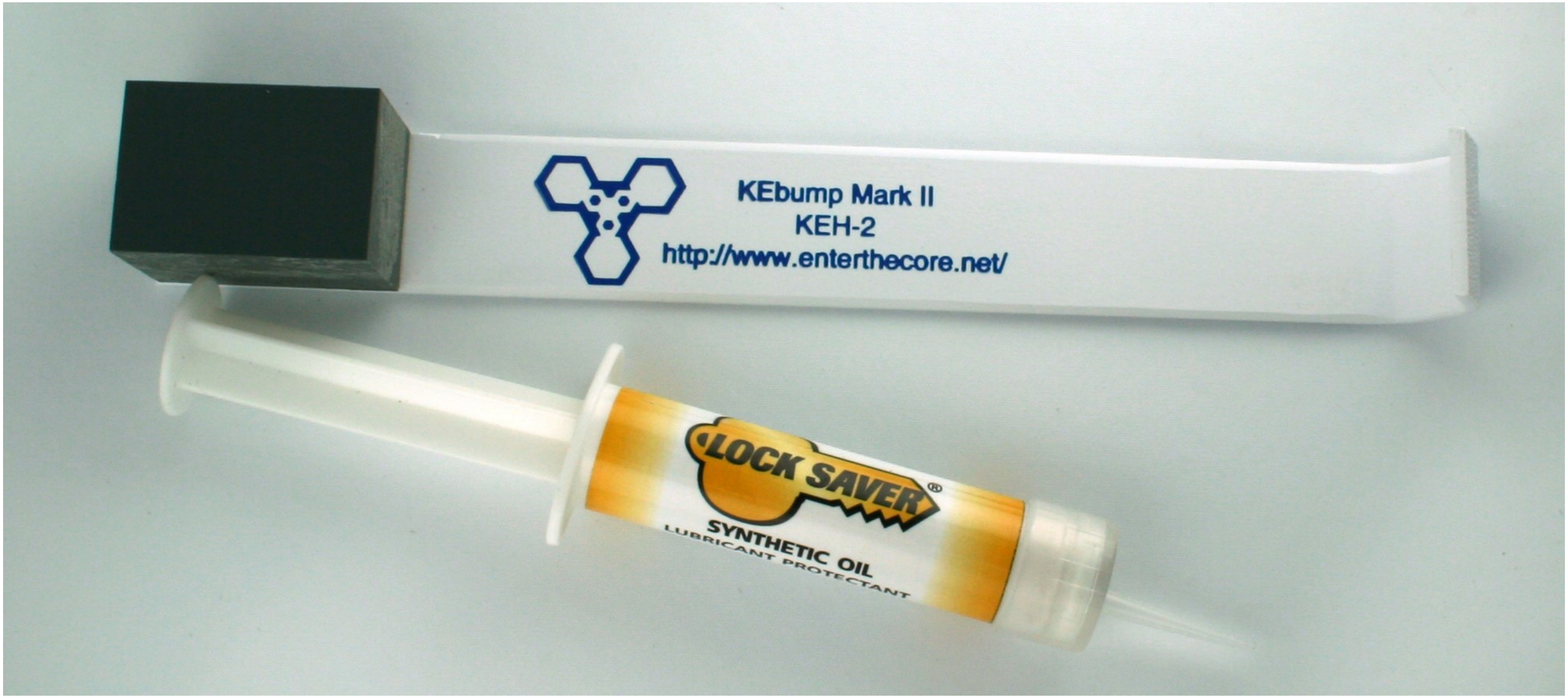
Key Bumping



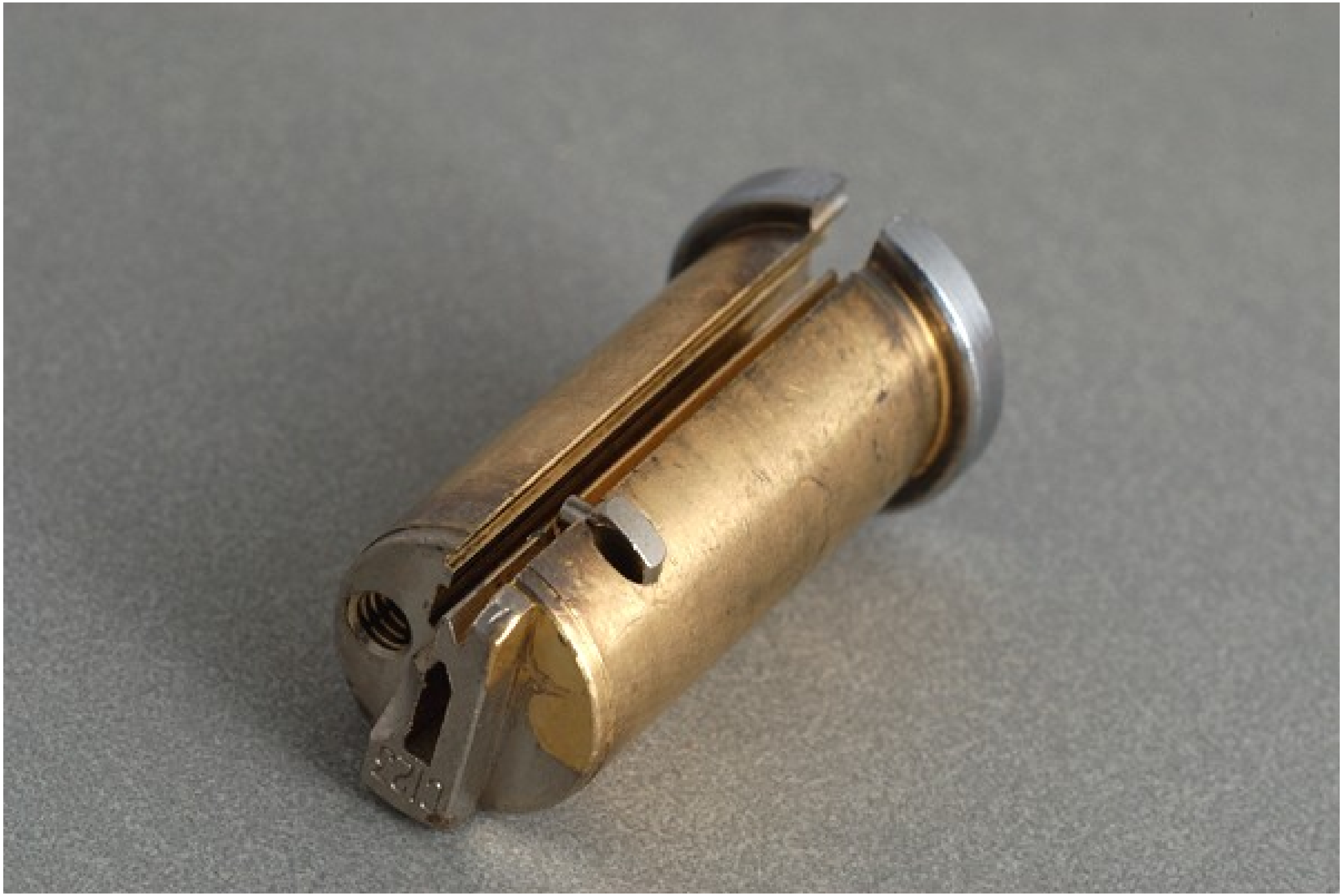
100% Efficiency…?

Don't underestimate attackers...

Bumping Hammers

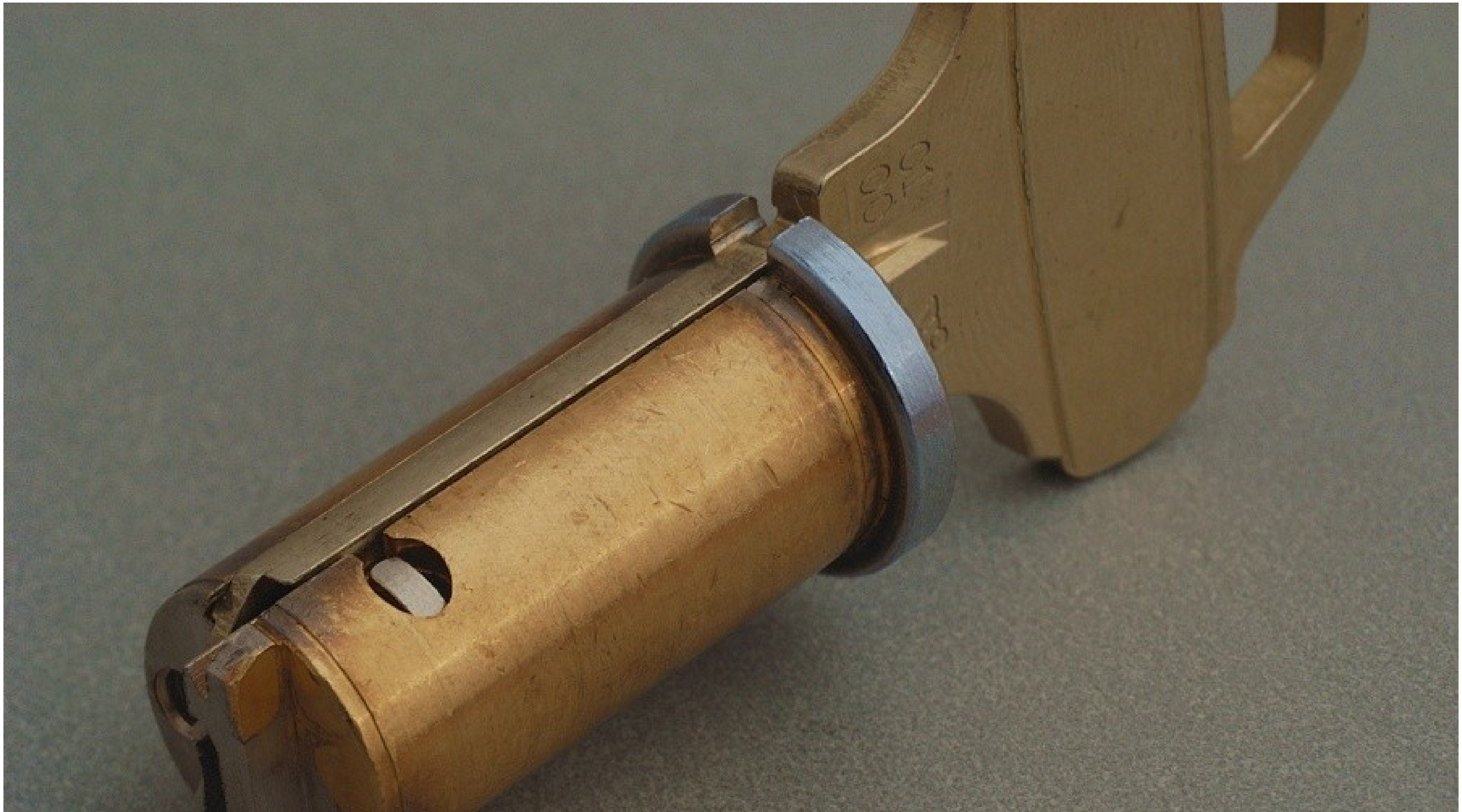


Side Pins

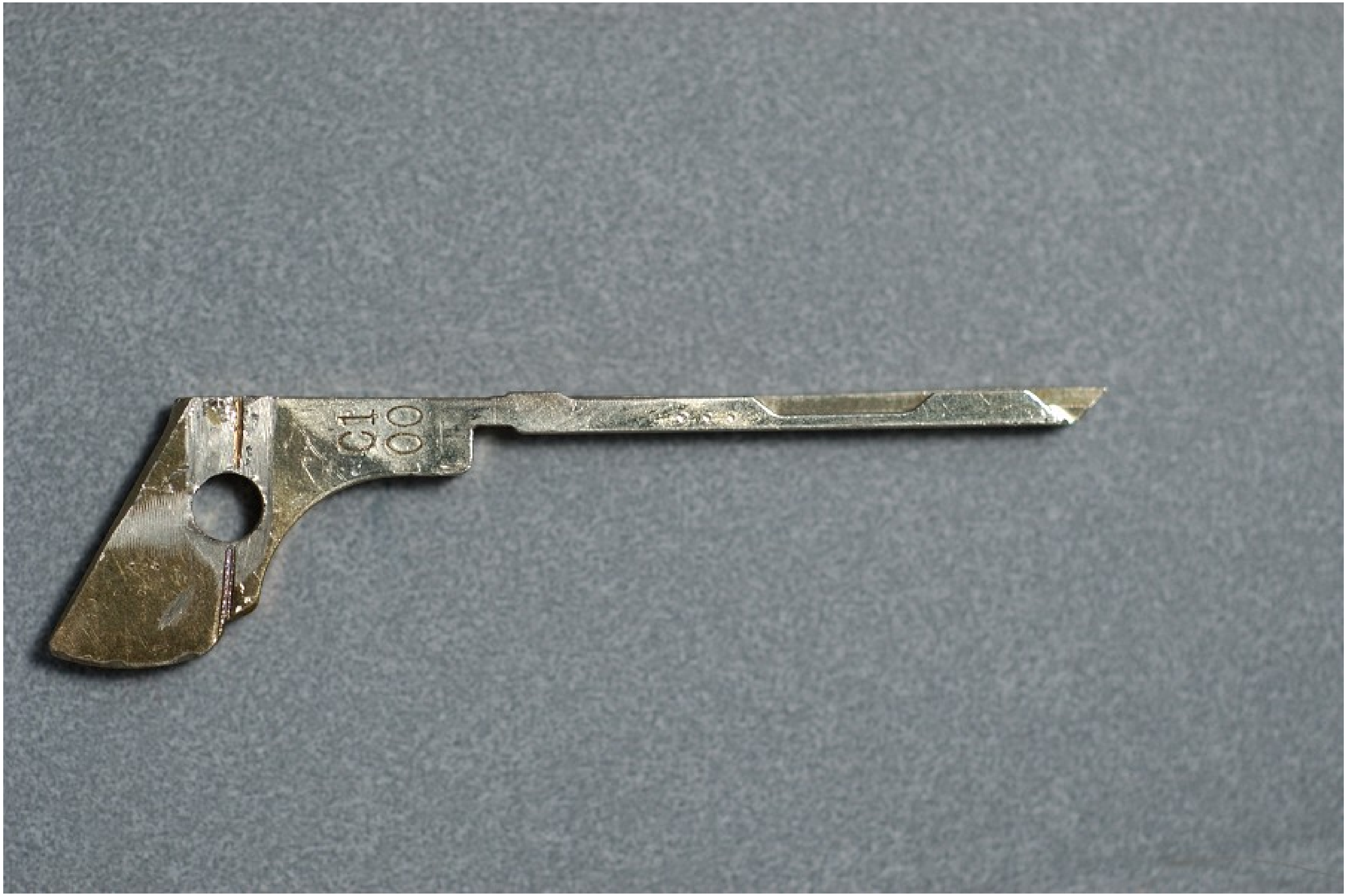


Side Pins

Side Pins



Side Pins



Side Pins

Regional Sidebar Attacks

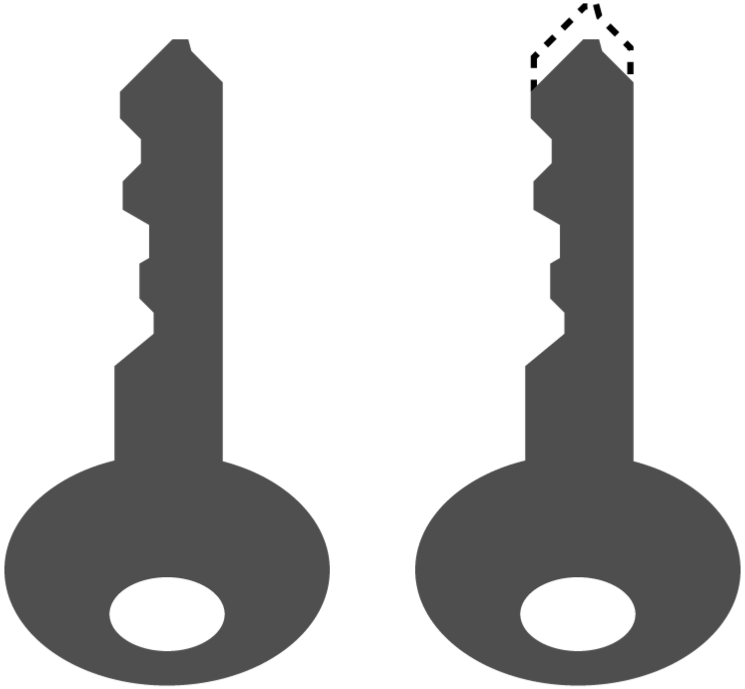
- ASSA Twin Combi
- Schlage Primus
- Fichet 480
- The list goes on...

- Schlage is doing it wrong.

One Last Way Schlage Is Doing It Wrong: LFIC

- BEST SFIC
- Small Format Interchangable Core

- Schlage LFIC
- 6.5 Control Key



Passive Components

What have we learned?

Resources

- openlocksport.com
- lockwiki.com
- lockpickingforensics.com
- ndemag.com

Meet us at Q&A!