Reverse Engineering Mechanical Locks:

Applied Theory

Babak Javadi and Shane Lawson

TakeDownCon Dallas 2011

Introductions: Babak Javadi

THE
CORE
GROUP

TOOOL

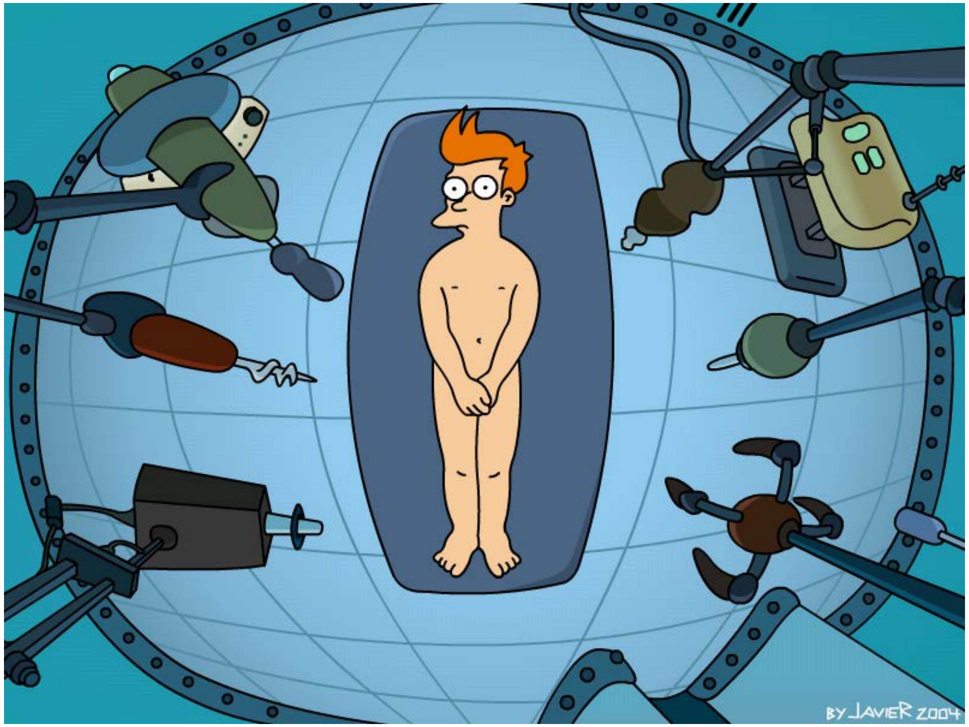
The Open Organisation Of Lockpickers

Introductions: Shane Lawson

What is Reverse Engineering in Physical Security?

Analysis of Locks Reveals…

- Conceptual Design Flaws
- Material Deficiencies
- Implementation Problems

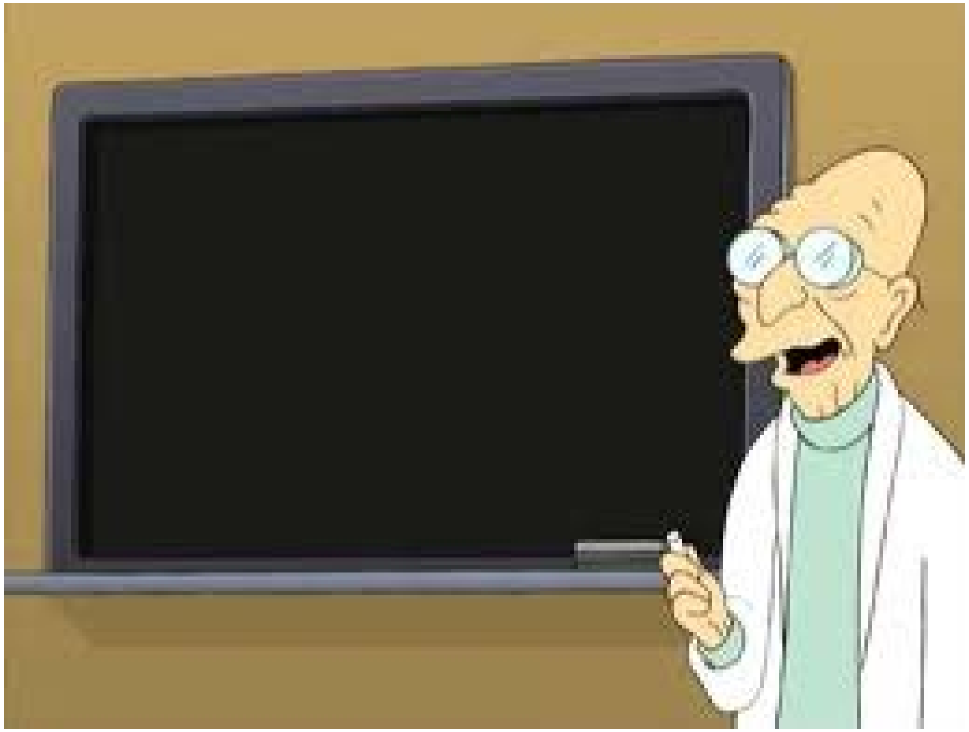


Getting Started: State Your Intentions

Is this a hobby?

For commercial gain?

Potentially dangerous?



Getting Started: Lab Basics

Have a Clean Workspace

Have a Clean Workspace

Lighting

Storage and Organization

Whiteboard

Seriously, Have a Clean Workspace

Getting Started: Tools of the Trade

Multiple Vises (note the spelling)

Clamps or "Helping Hands"

Tweezers

Jeweler's Loupe

Microscope

High Quality Digital Micrometer

© 2007 CuriousInventor.com

Getting Started: Tools of the Trade

Toolbox

Scrap Metal Stock

Key Blanks

Rotary Tool

Bench Grinder

Spare Lock Parts

Getting Started: Bonus Tools ($$$)

3-axis Mill

Metal Lathe

Laser Cutter

Band Saw

Drill Press

Getting Started: Sourcing Supplies

Get it New

GRAINGER®
FOR THE ONES WHO GET IT DONE

McMASTER-CARR®

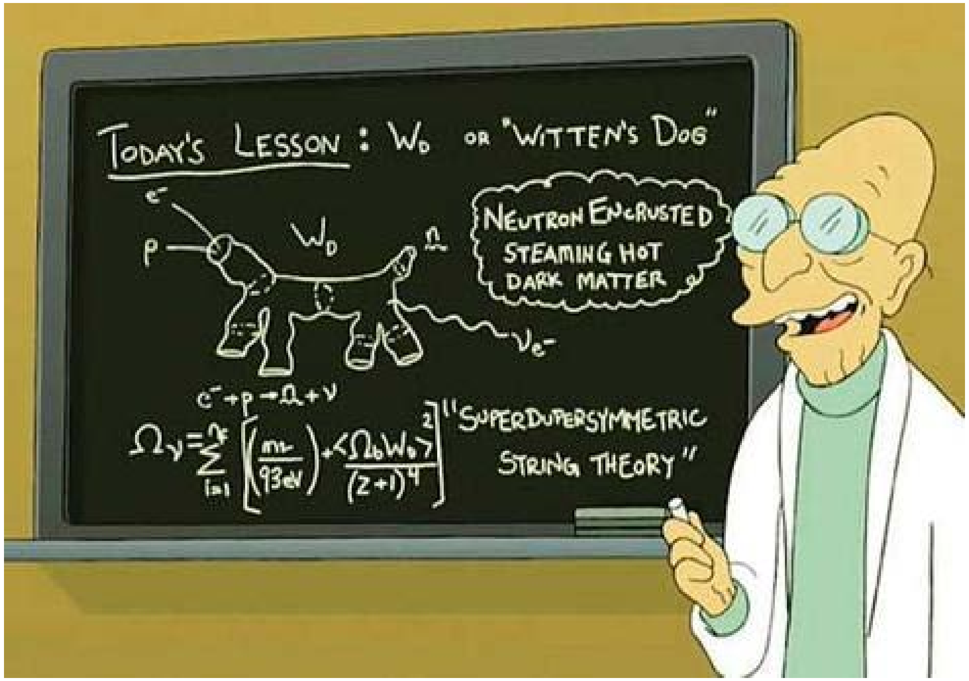
THE HOME DEPOT®

Get it Used

ebay®

Get Yourself Learned, Son

- Physics
- Metallurgy
- Masterkey Math
- Traditional Lock Mechanics
- Common Lock Traits


TODAY'S LESSON : W_D OR "WITTEN'S DOG"
e⁻
p
W_D
Ω
NEUTRON ENCRUSTED STEAMING HOT DARK MATTER
ν_e⁻
e⁻ + p → Ω + ν
"SUPERDUPERSYMMETRIC STRING THEORY"

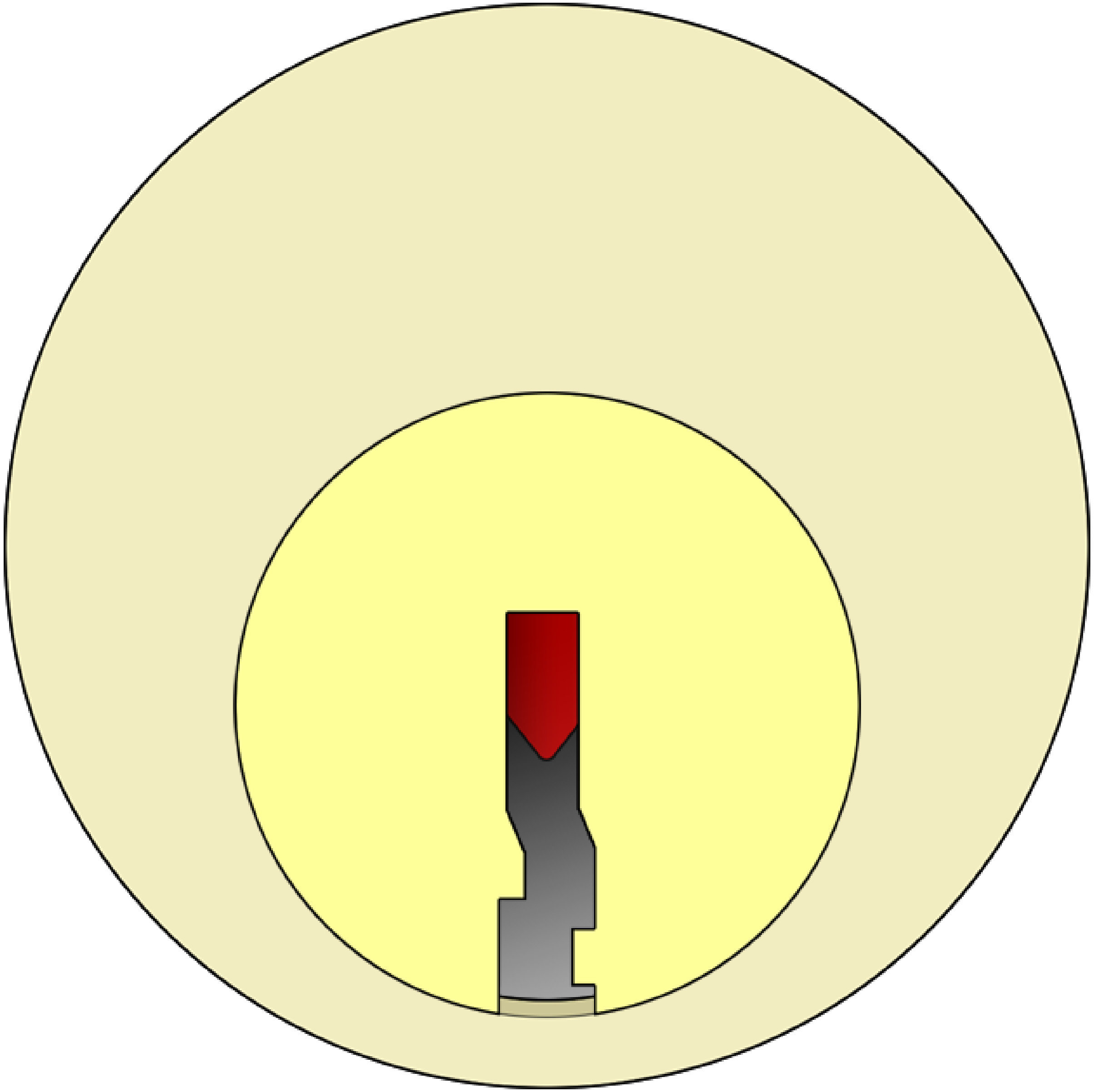
Common Attack Vectors

- Non-Destructive
  - Picking
  - Decoding
  - Impressioning
  - Bypass

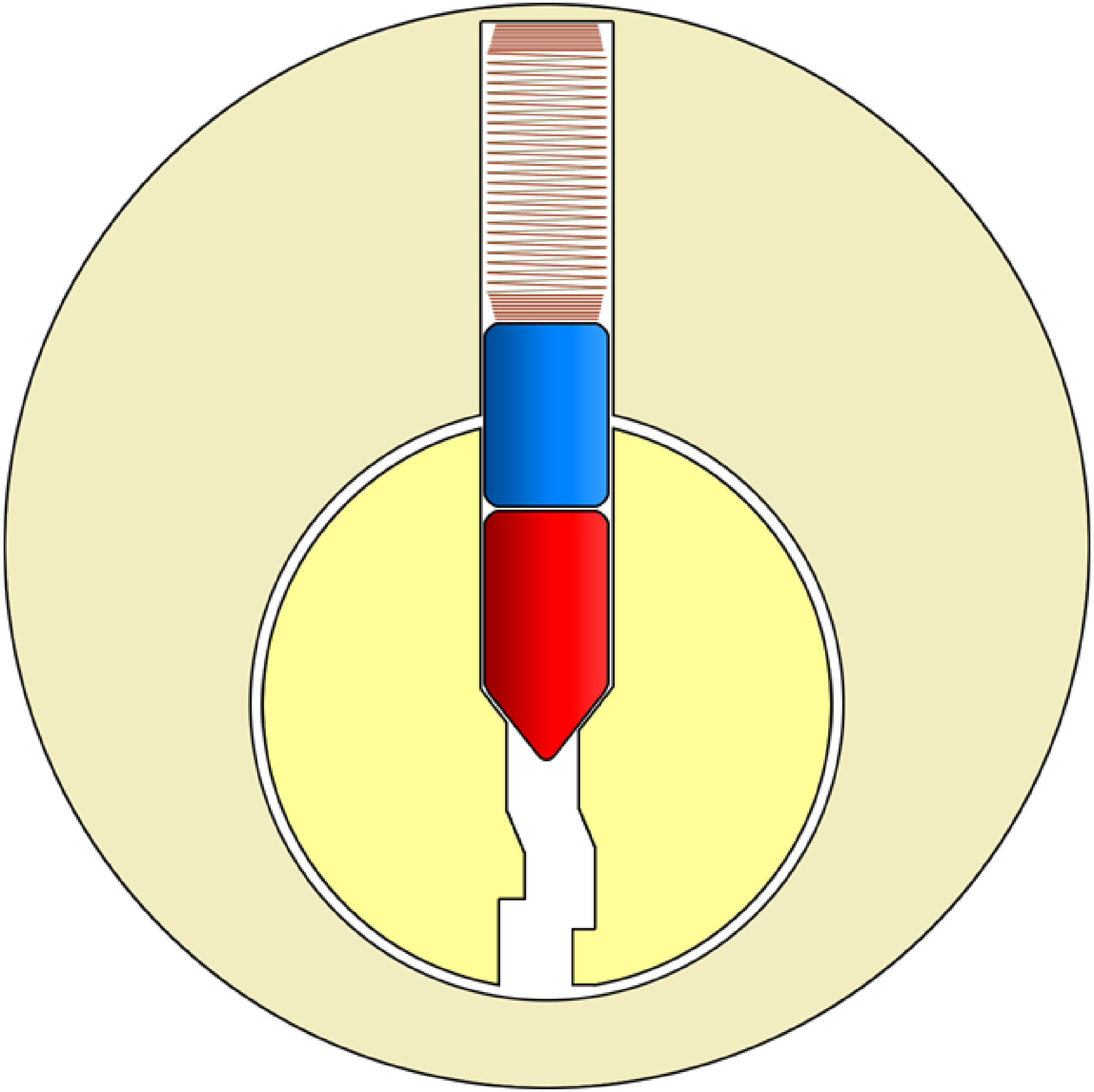
- Destructive
  - Drilling
  - Cutting
  - Brute Force

Pin Tumbler Locks

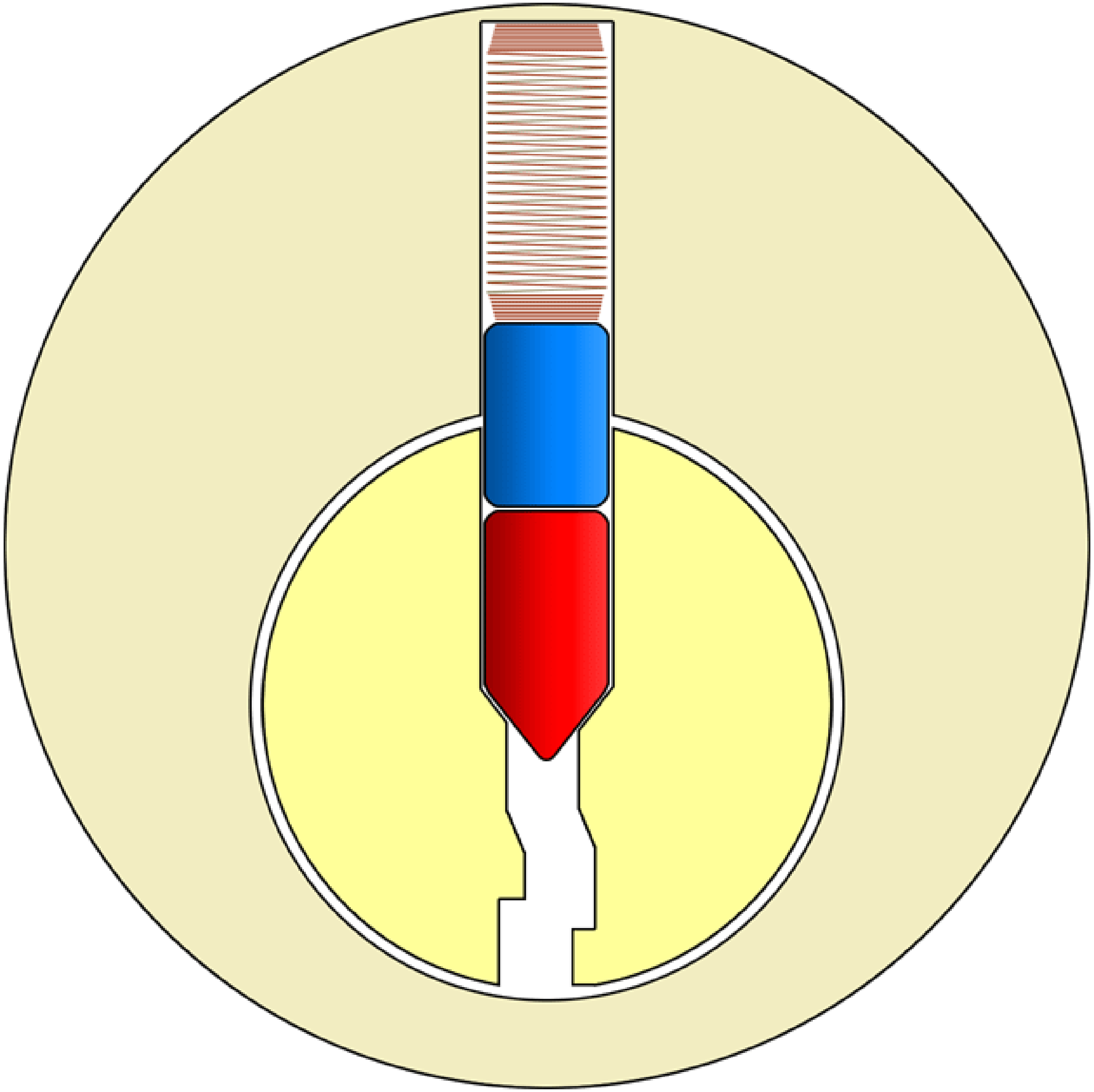
Outer View



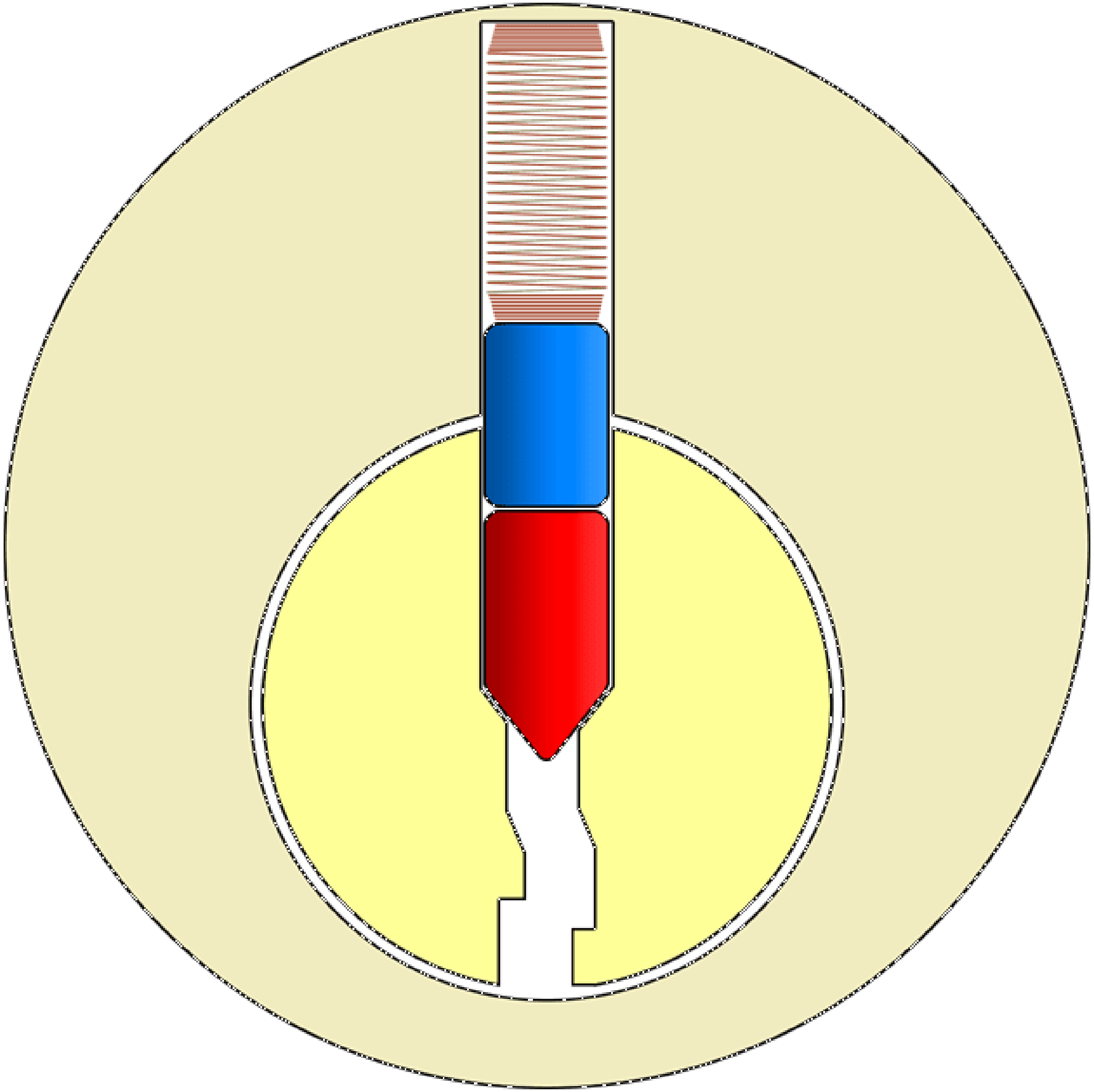
Inner View



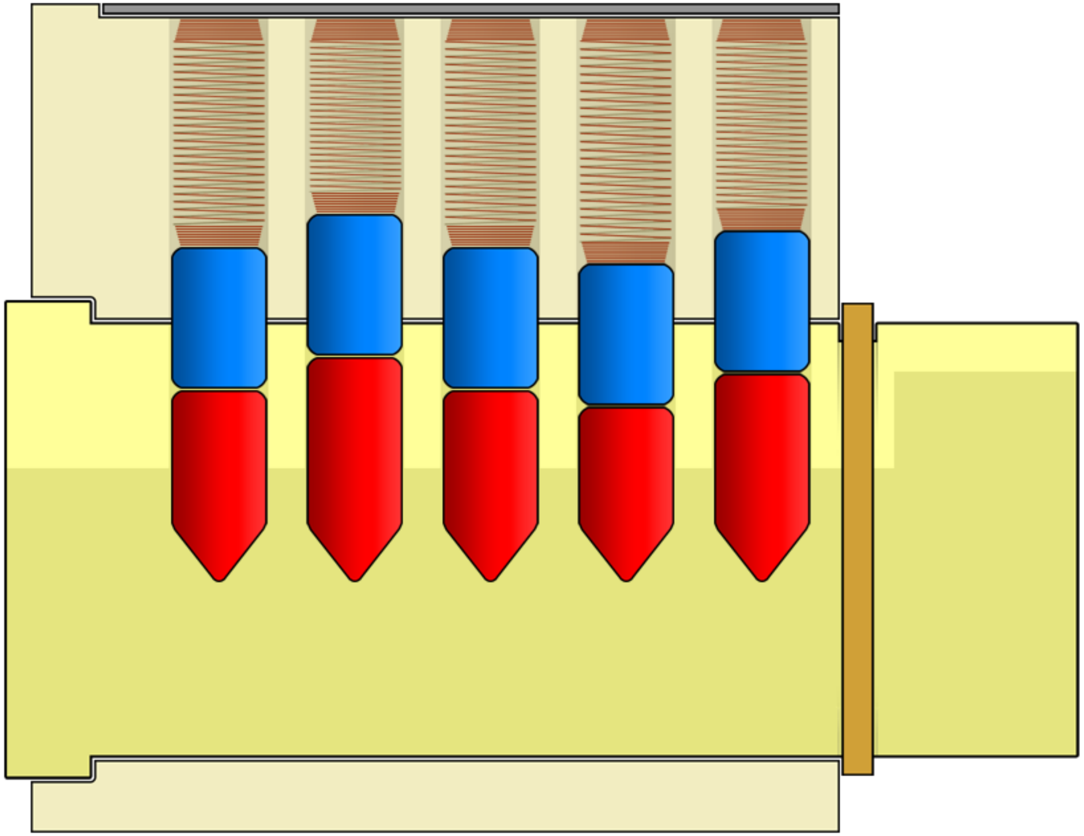
Attempt Without a Key



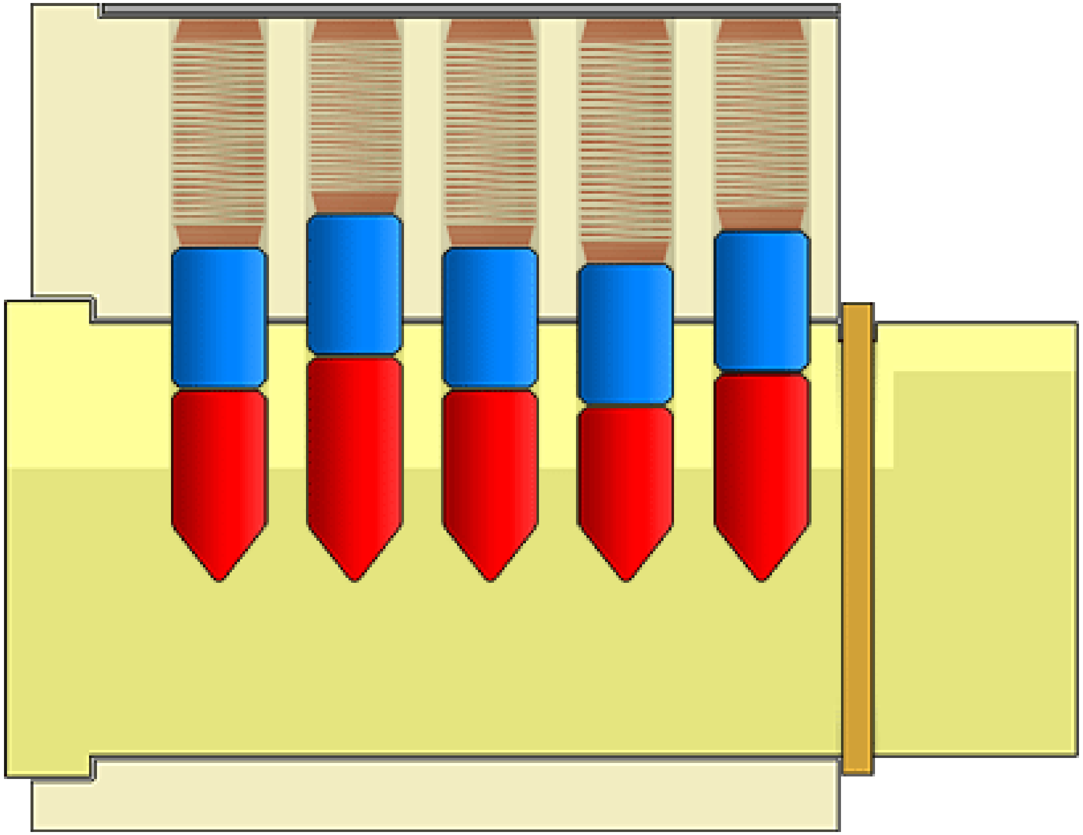
Operating With a Key



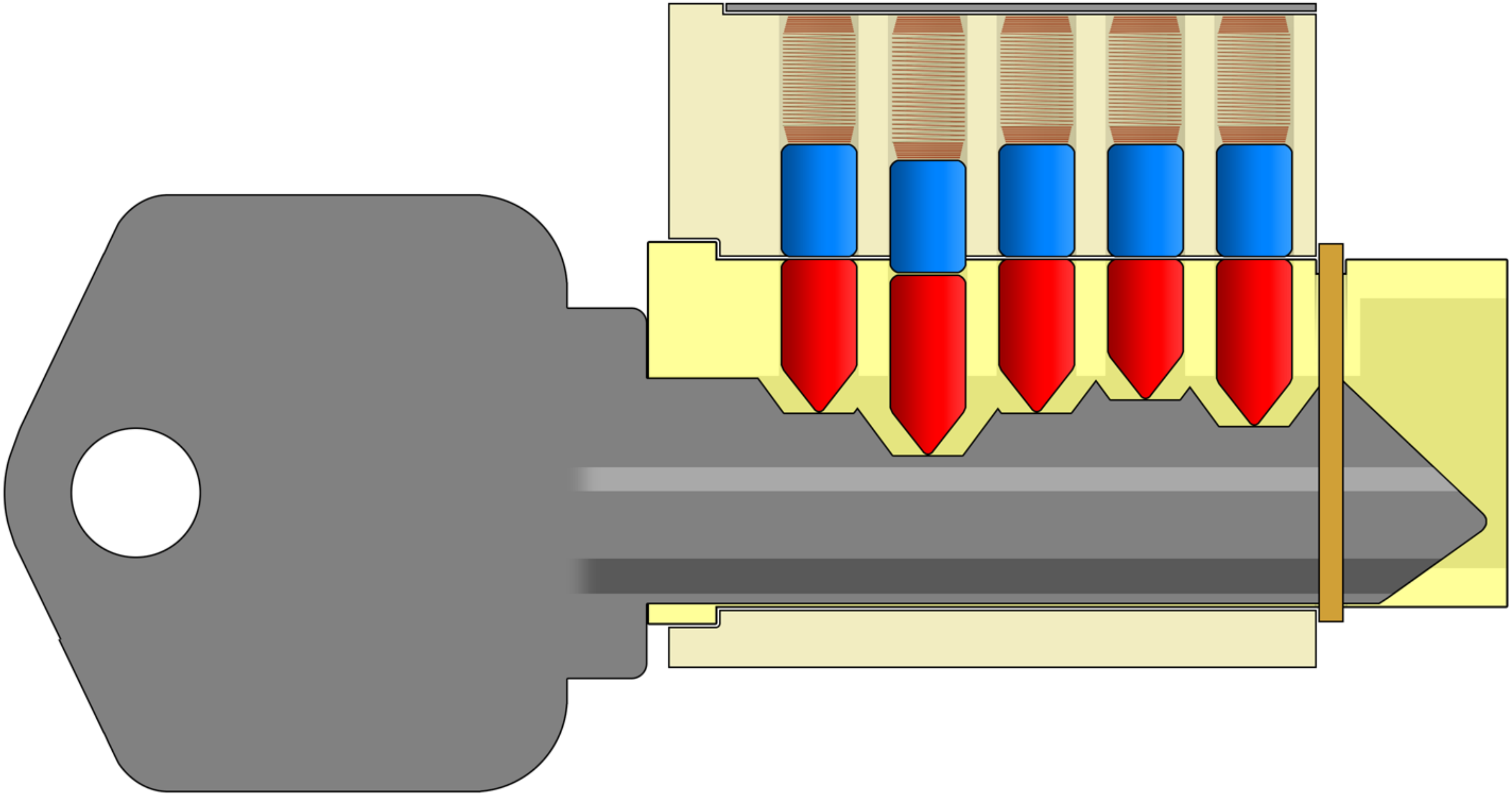
Pin Stacks



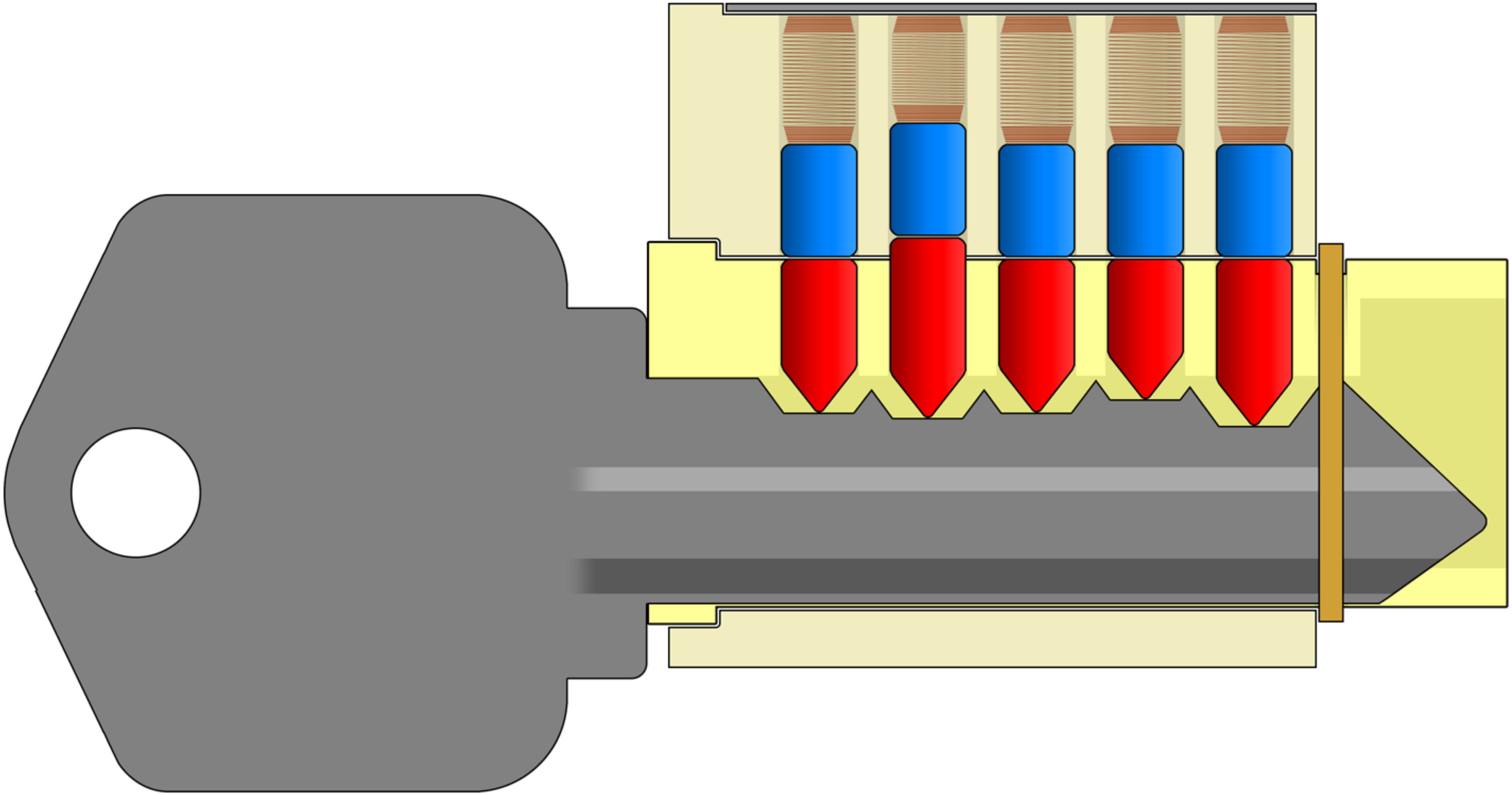
Key Operation



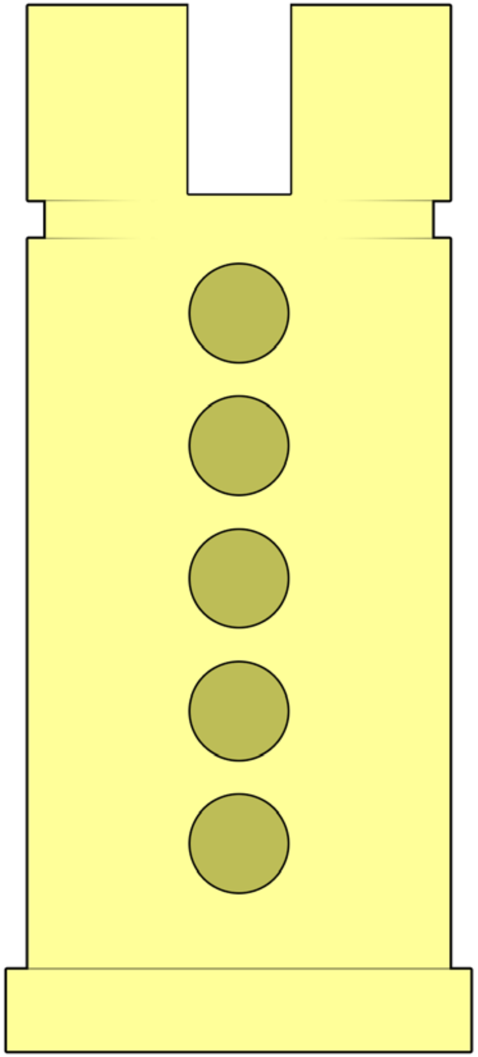
One Bitting Too Low

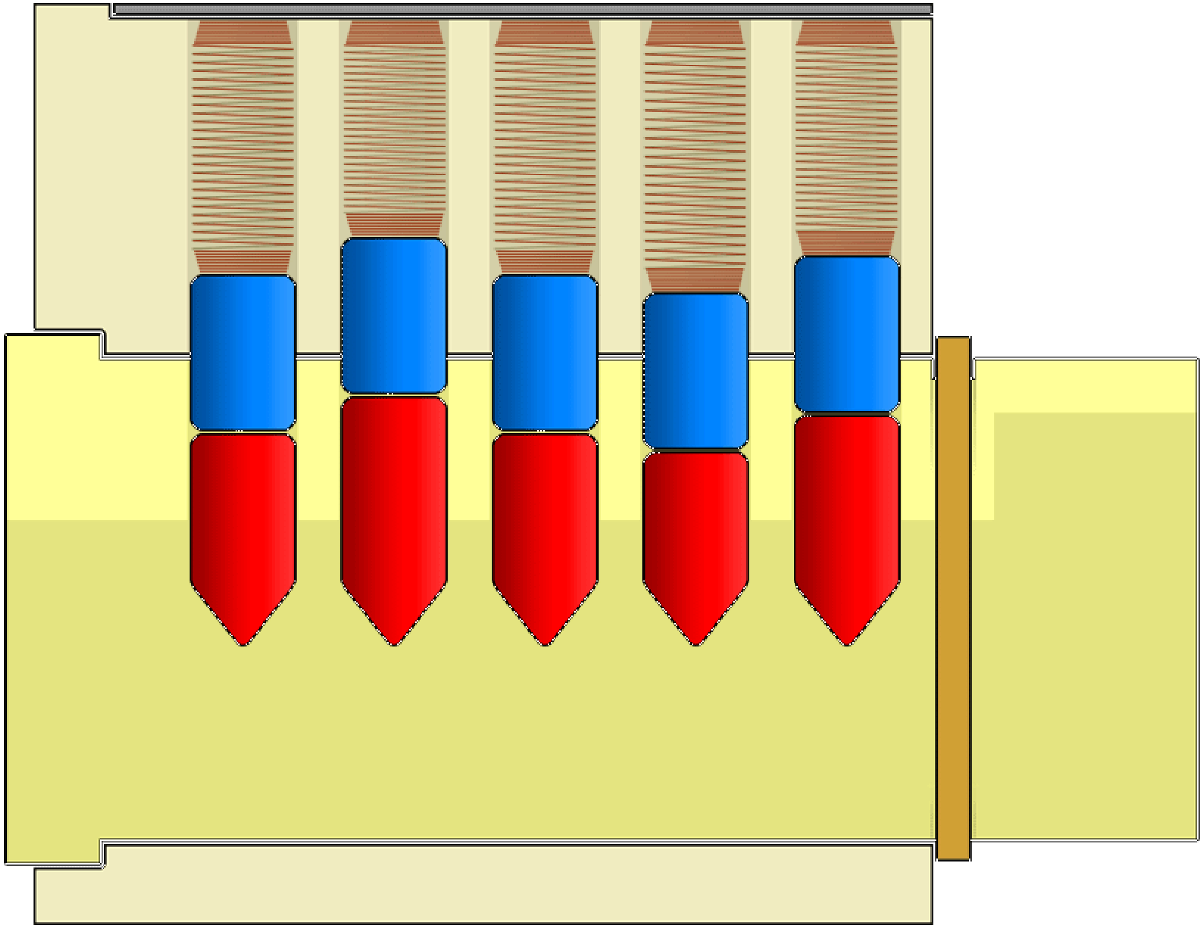


One Bitting Too High

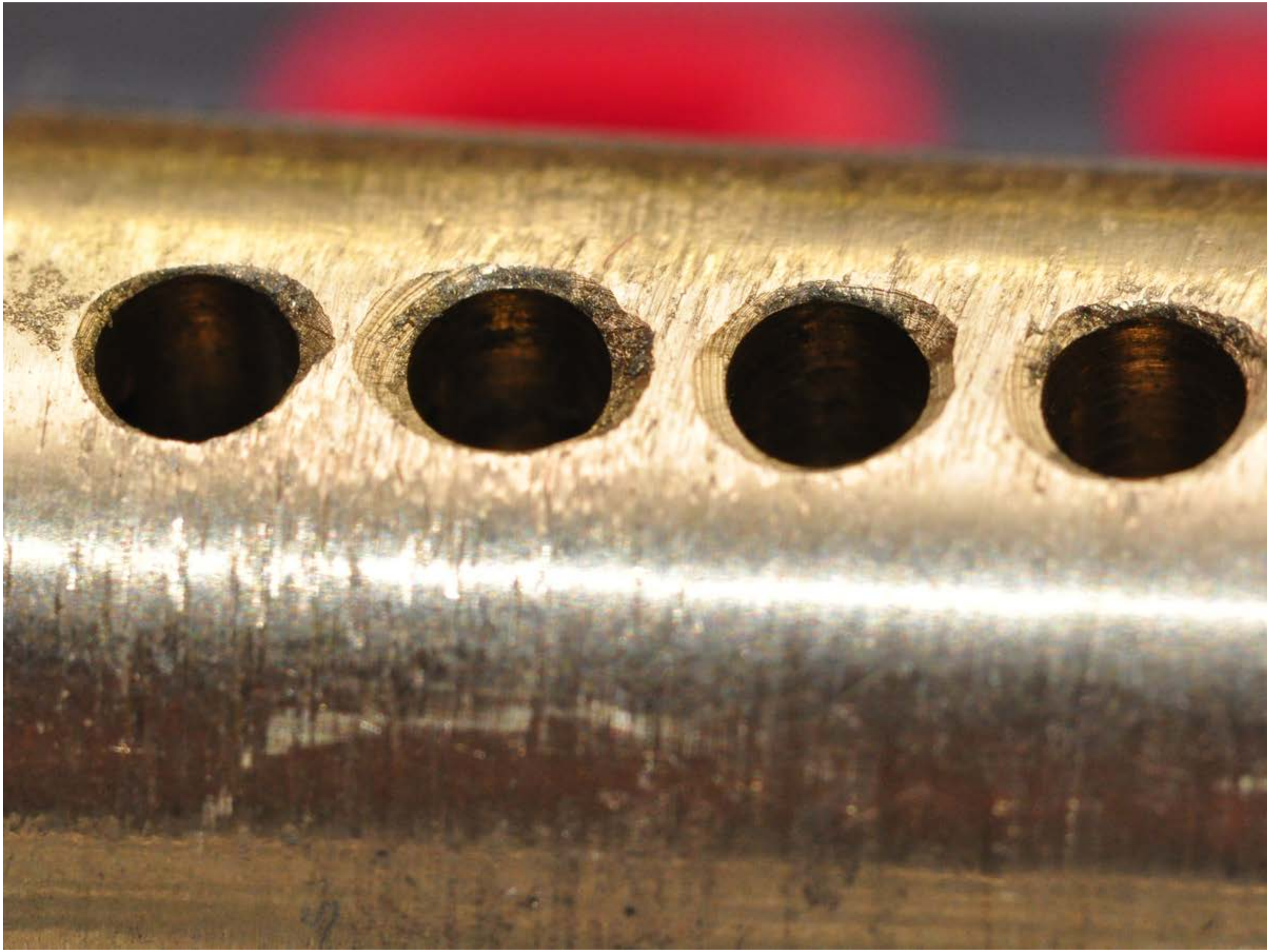


In a Perfect World



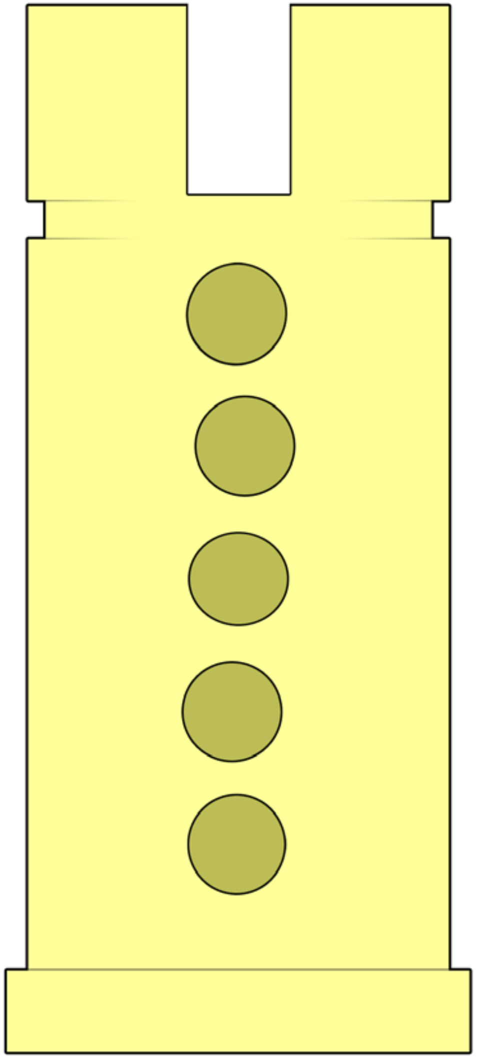


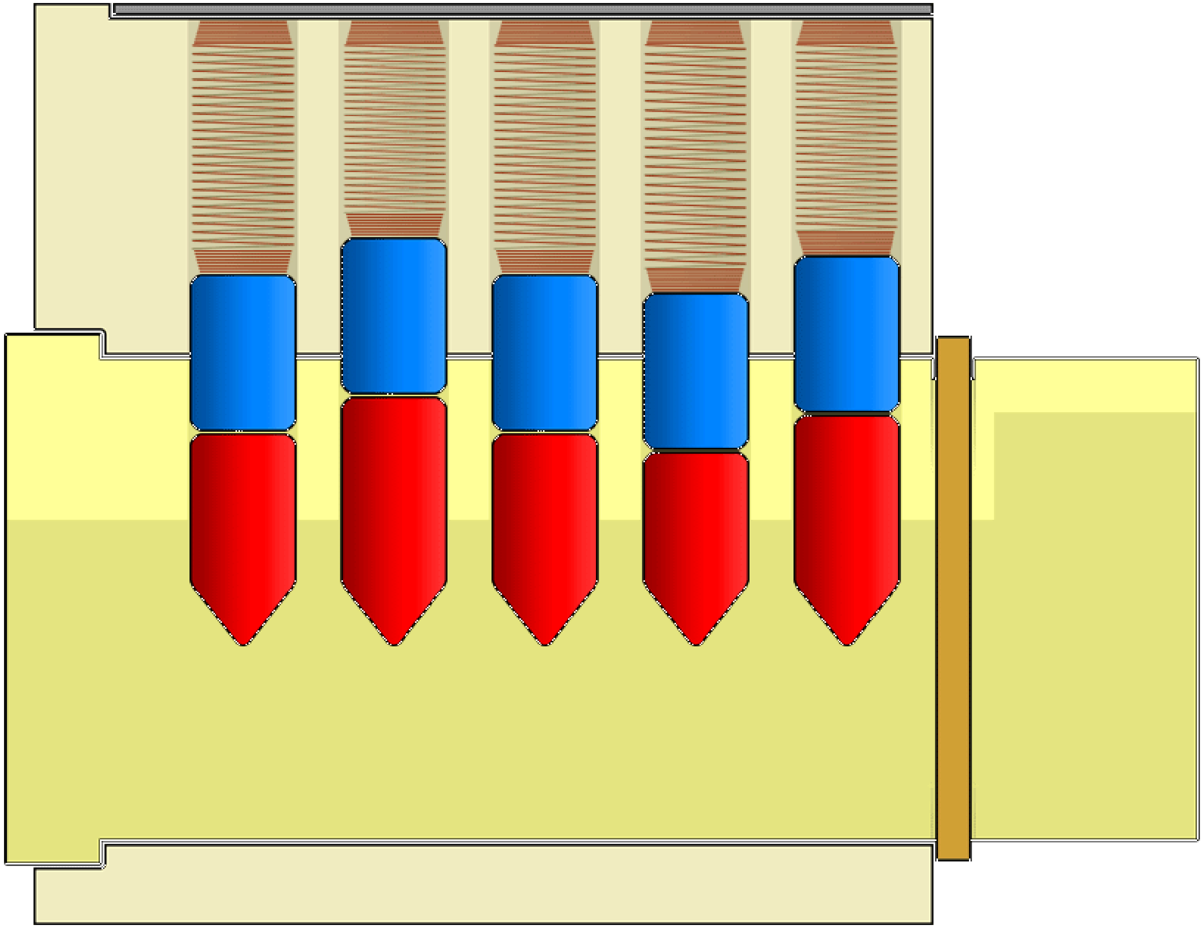
In the Real World



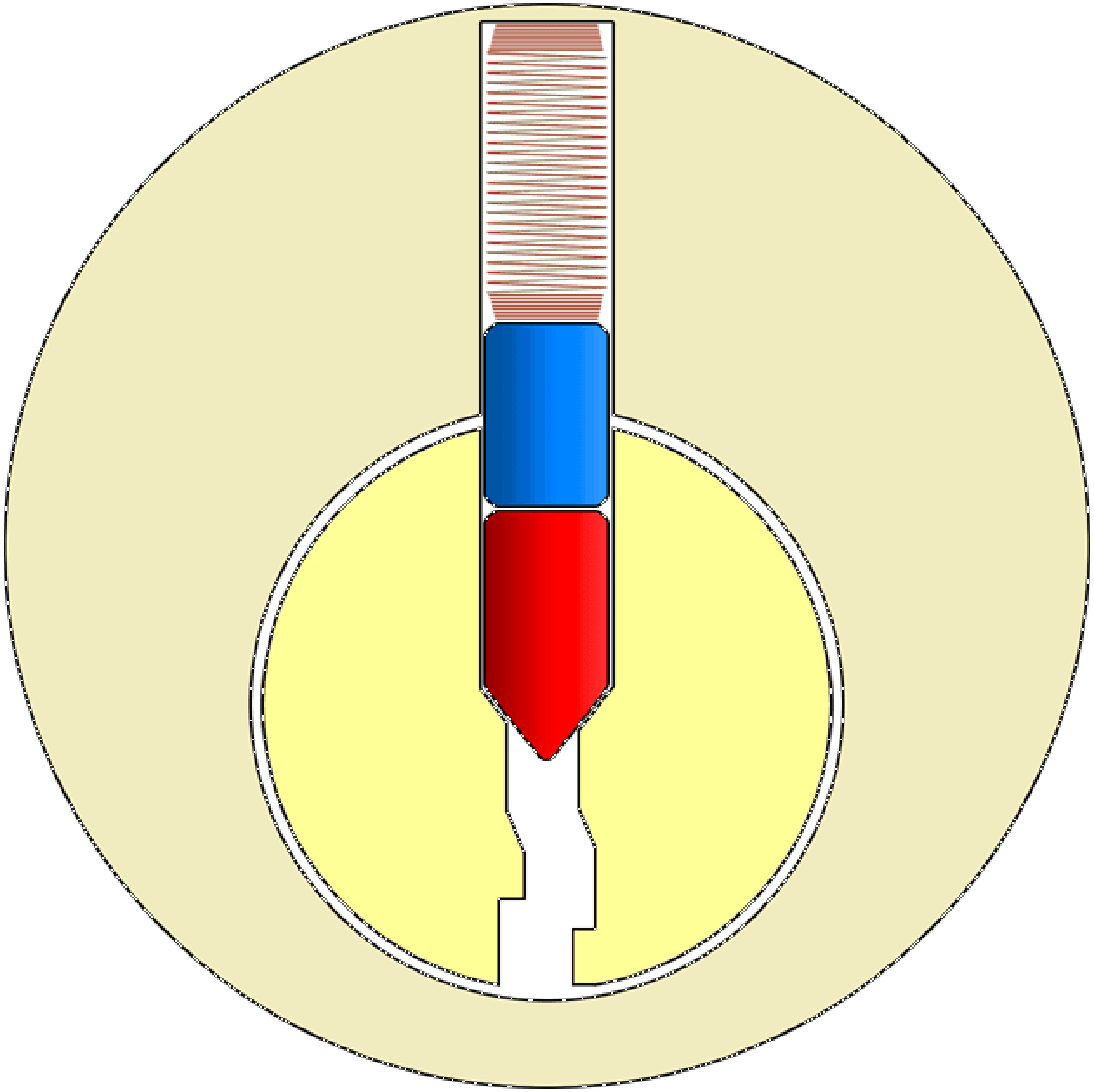
In the Real World

In the Real World

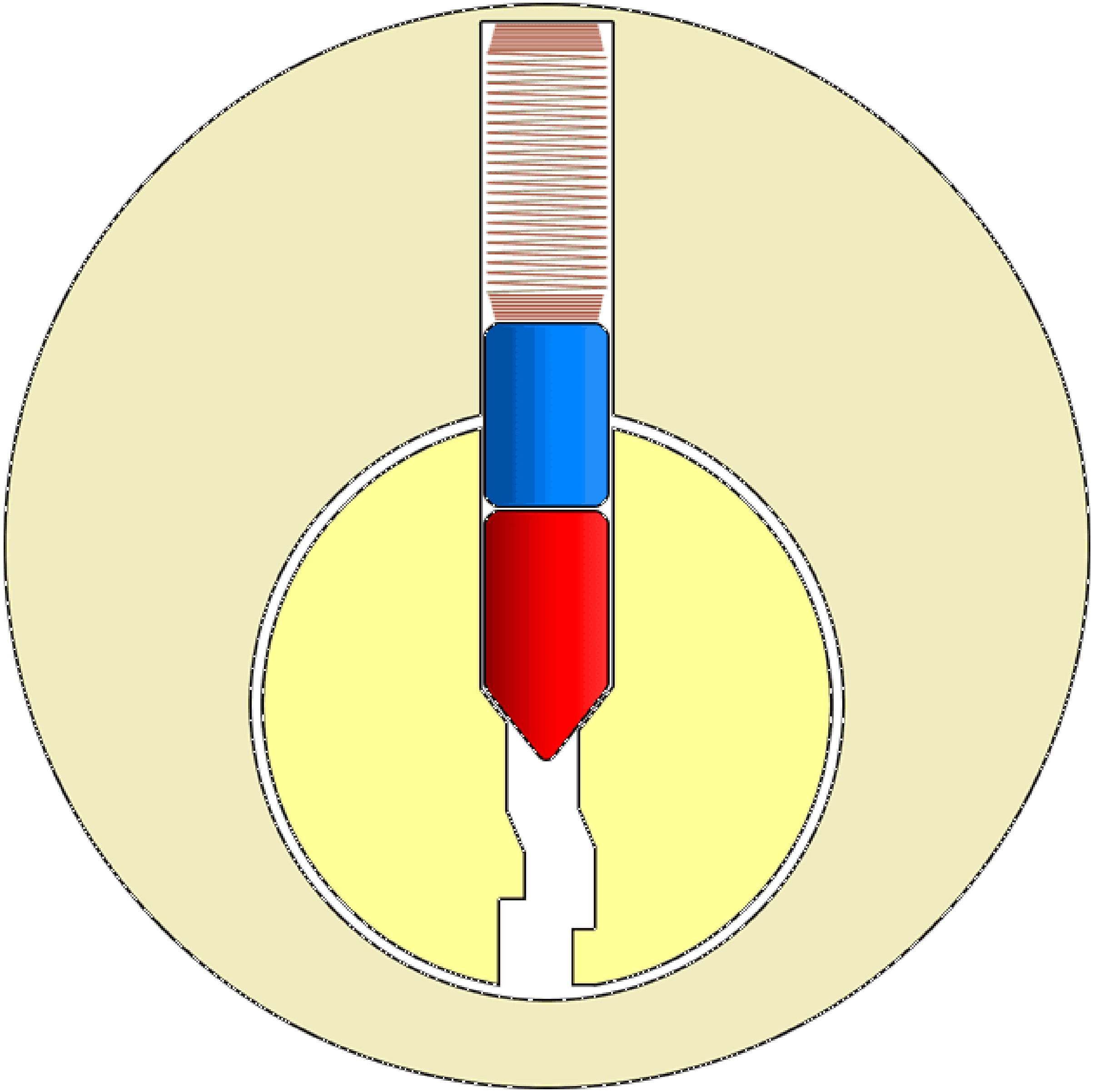




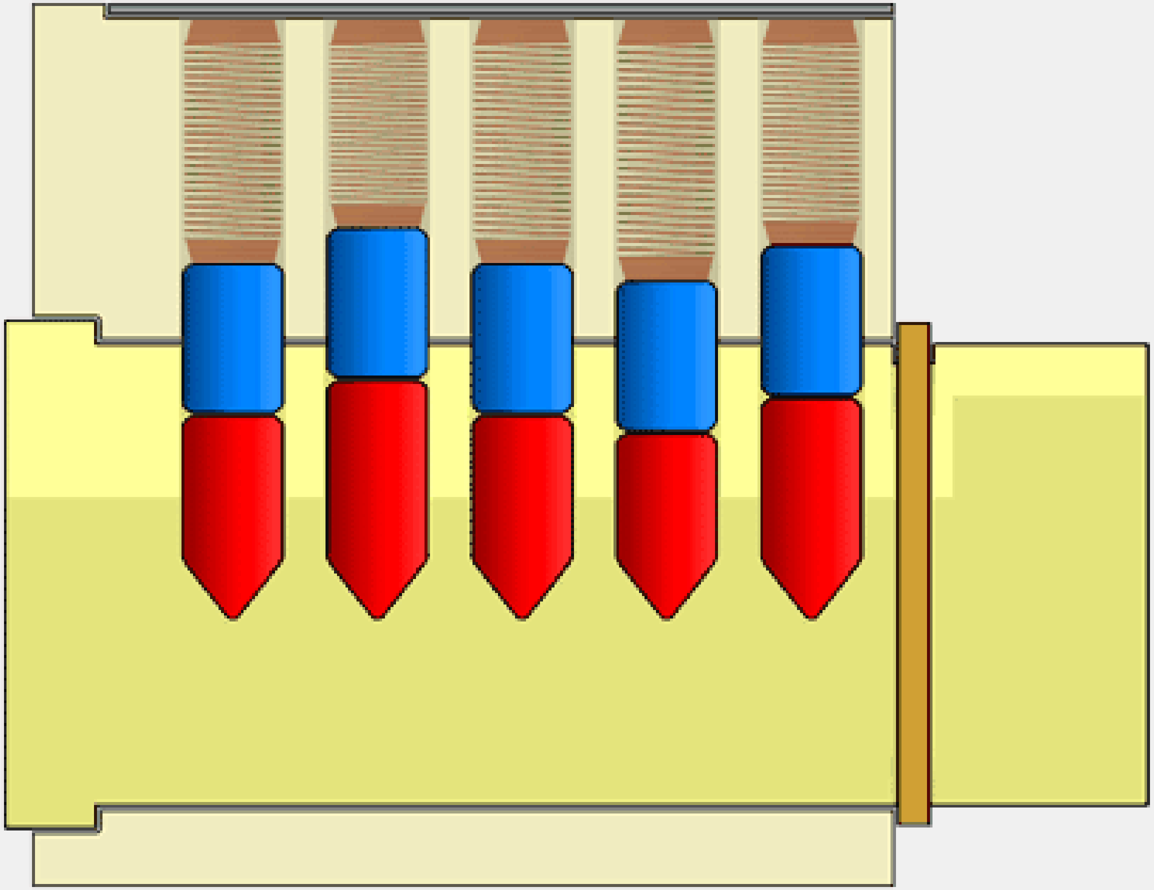
"Setting" a Binding Pin



The Key Pin Can Still Move Freely



Setting Multiple Pins



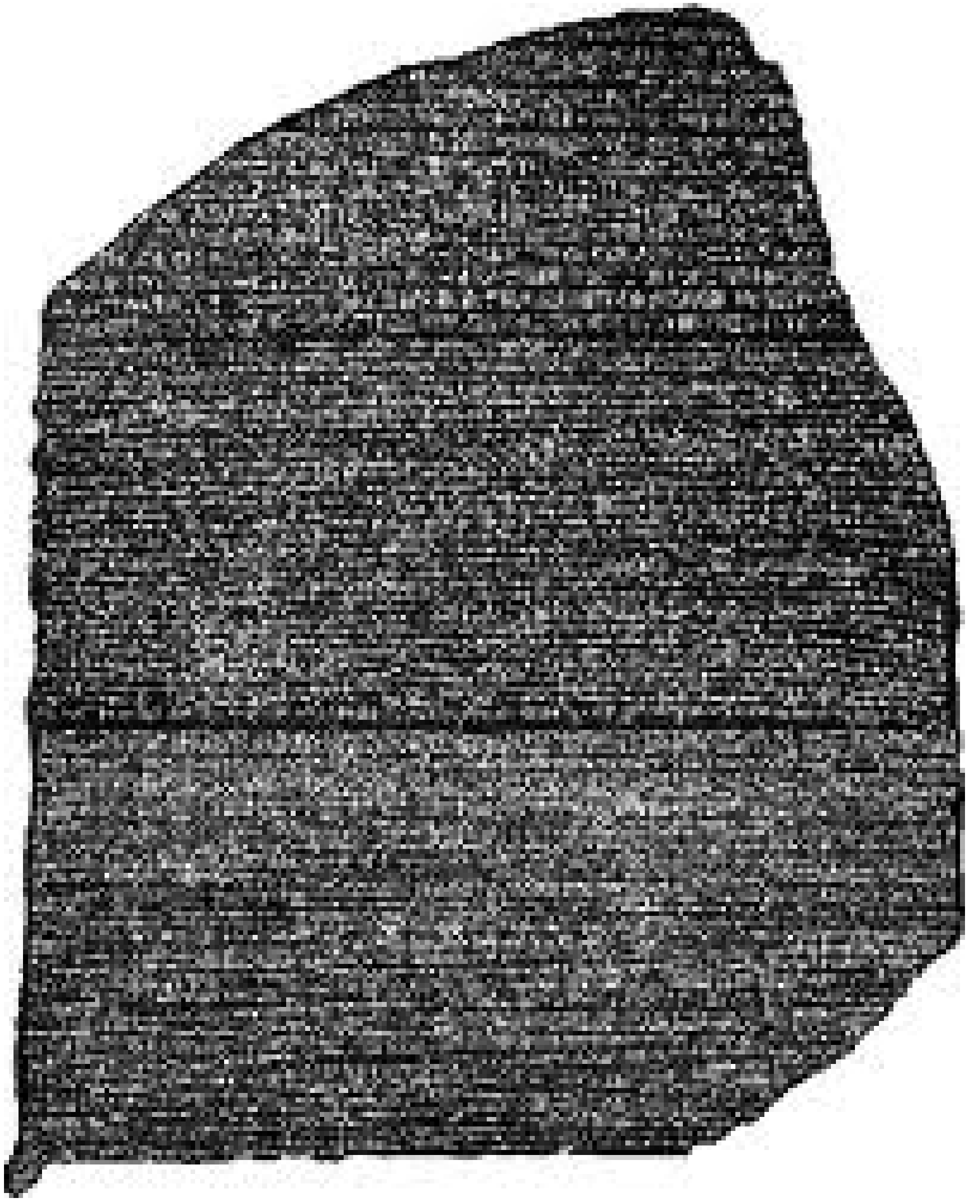
Decoding

Clandestine Method of Entry

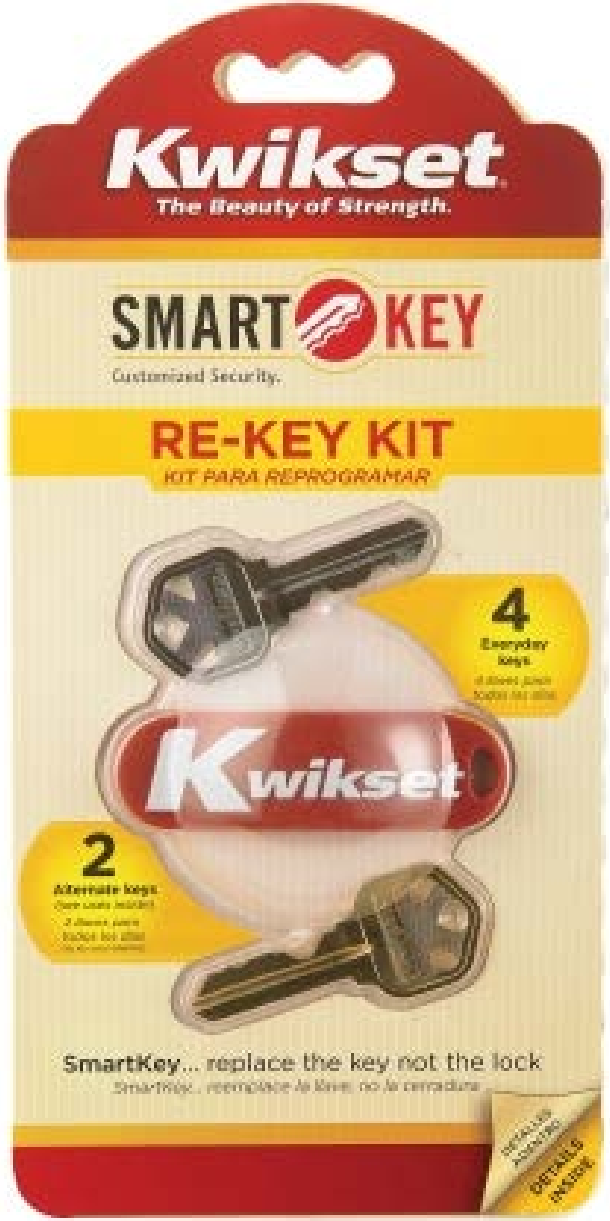
Primary Target is the Key Code

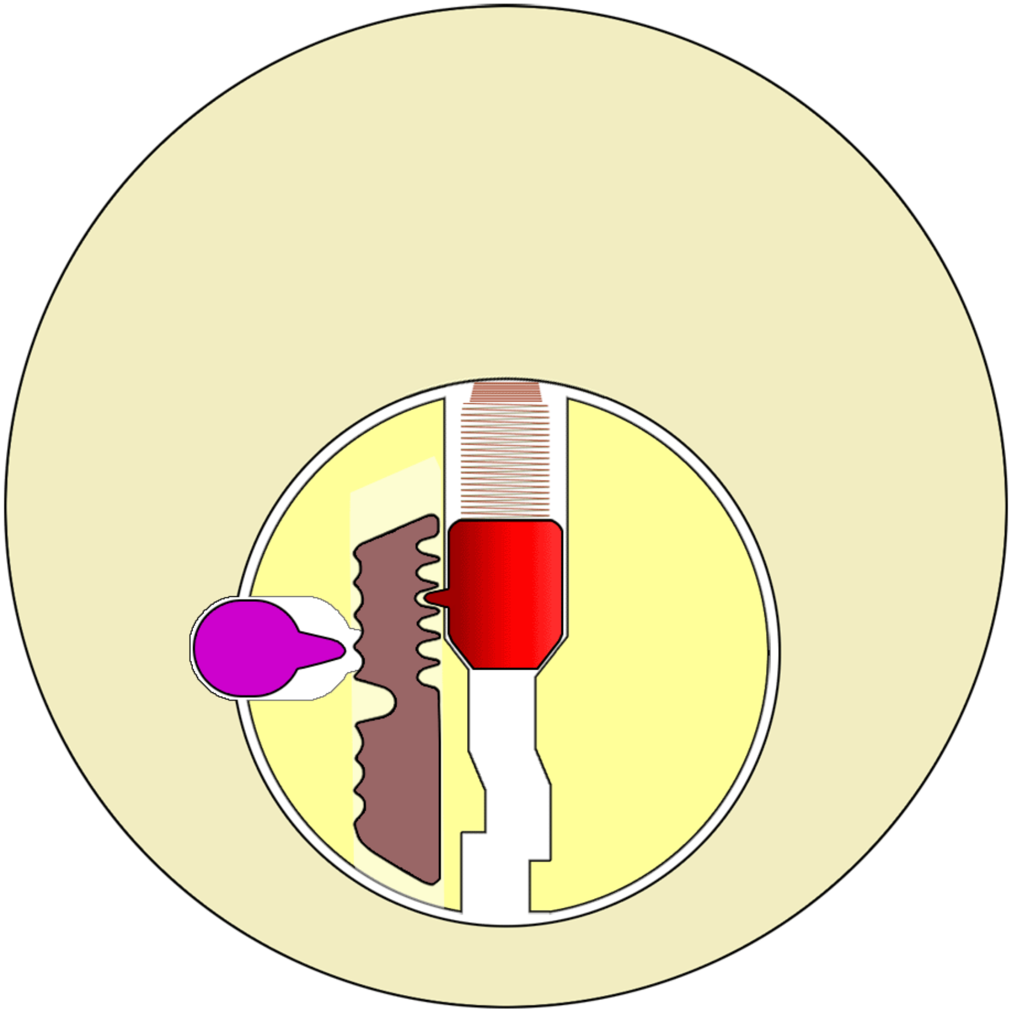
Key Origination

Calculating Master Keys

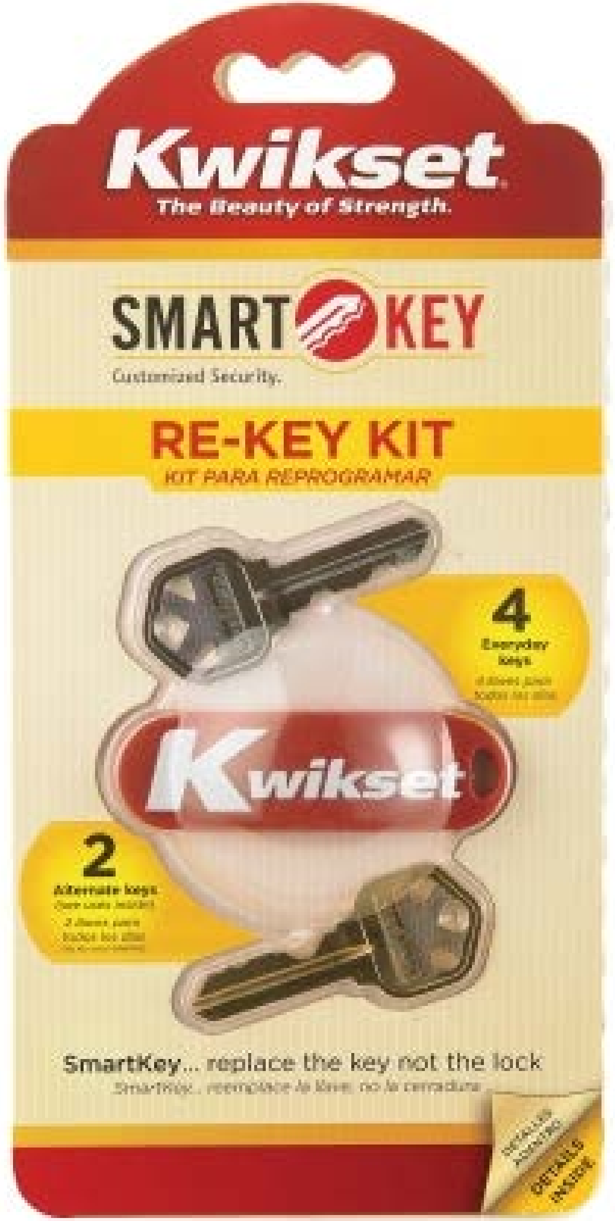


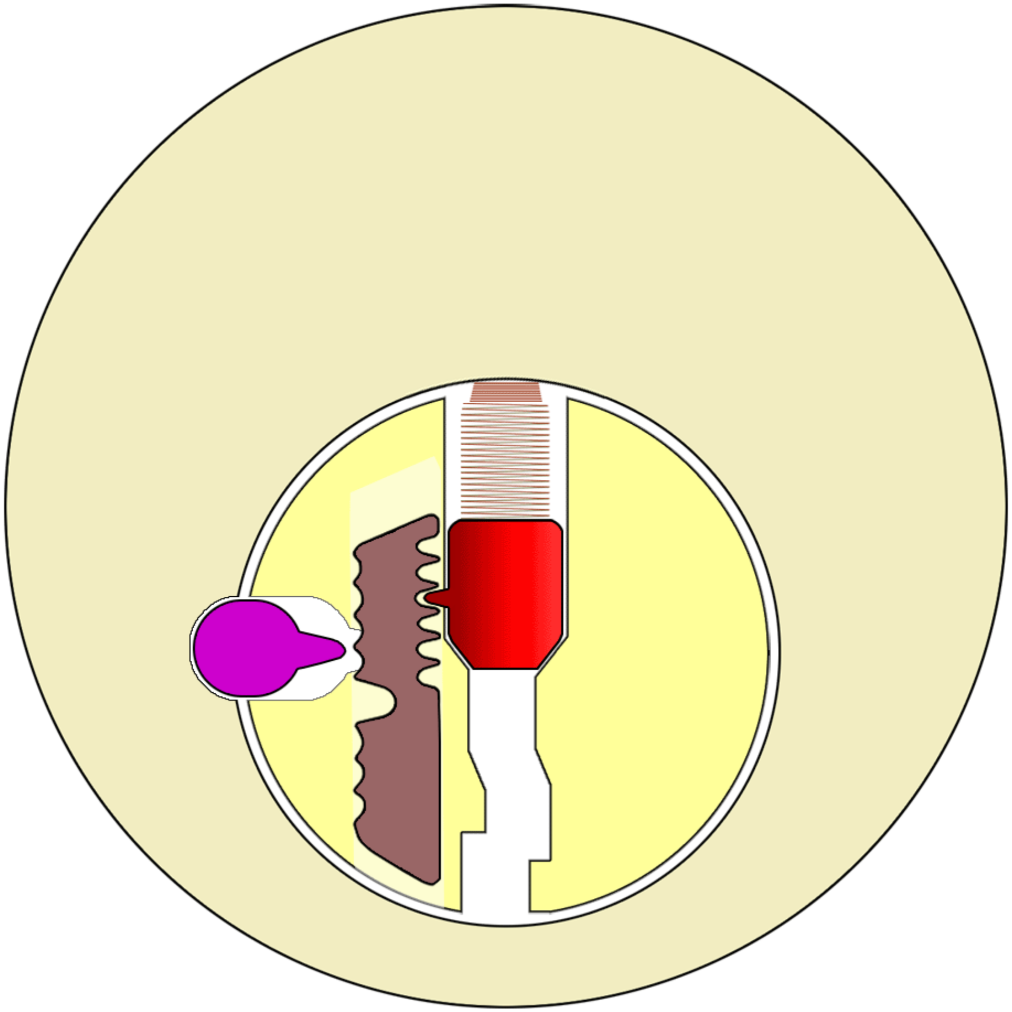
Kwikset Smart Series



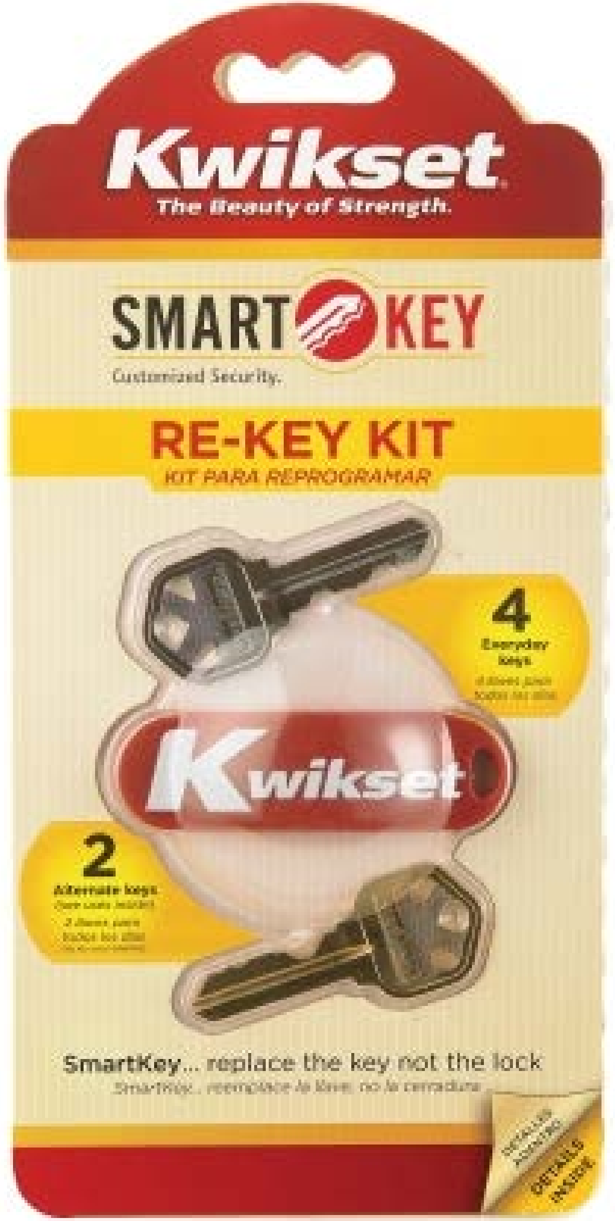


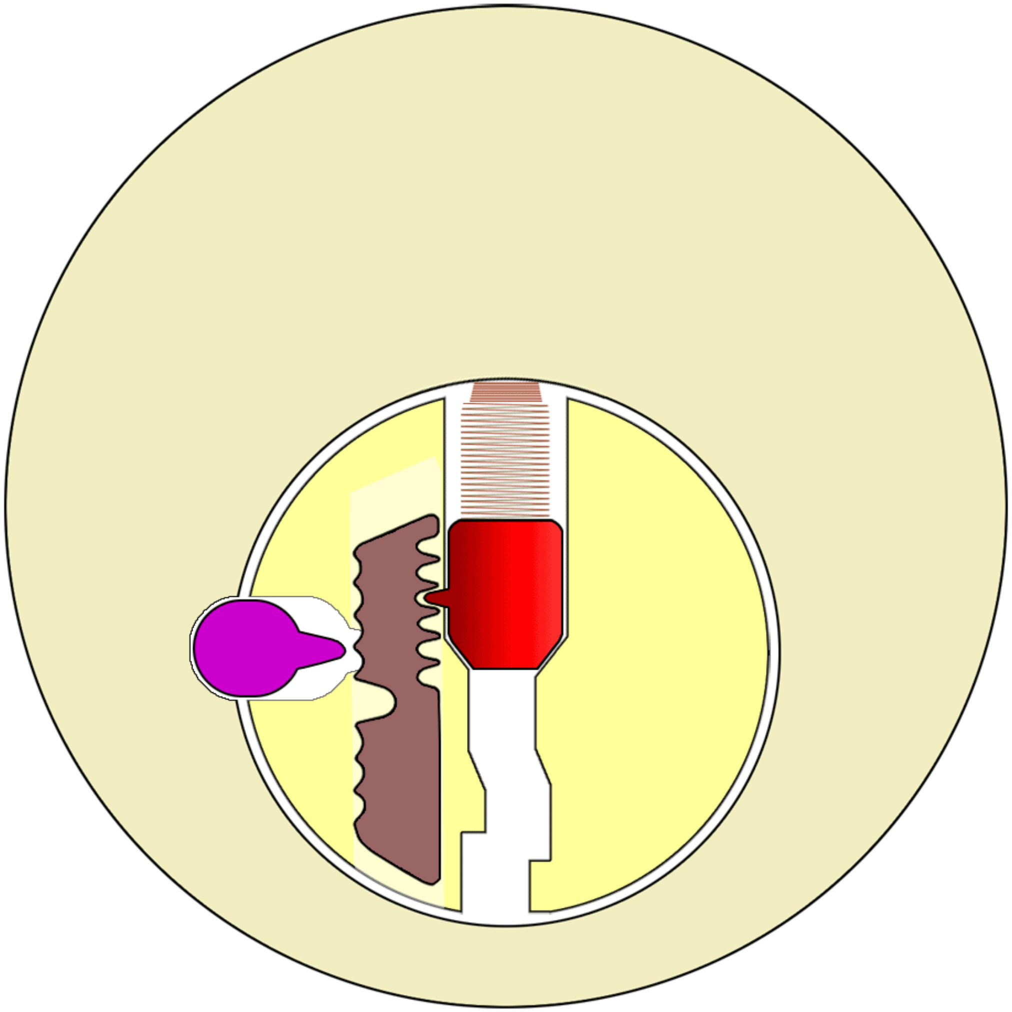
Kwikset Smart Series



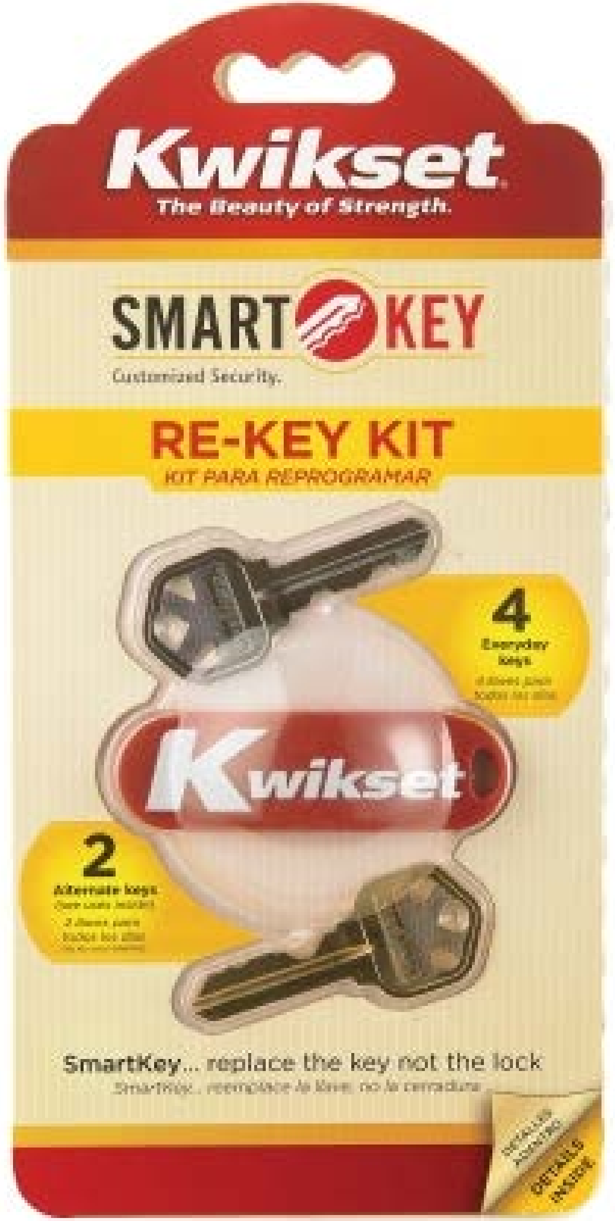


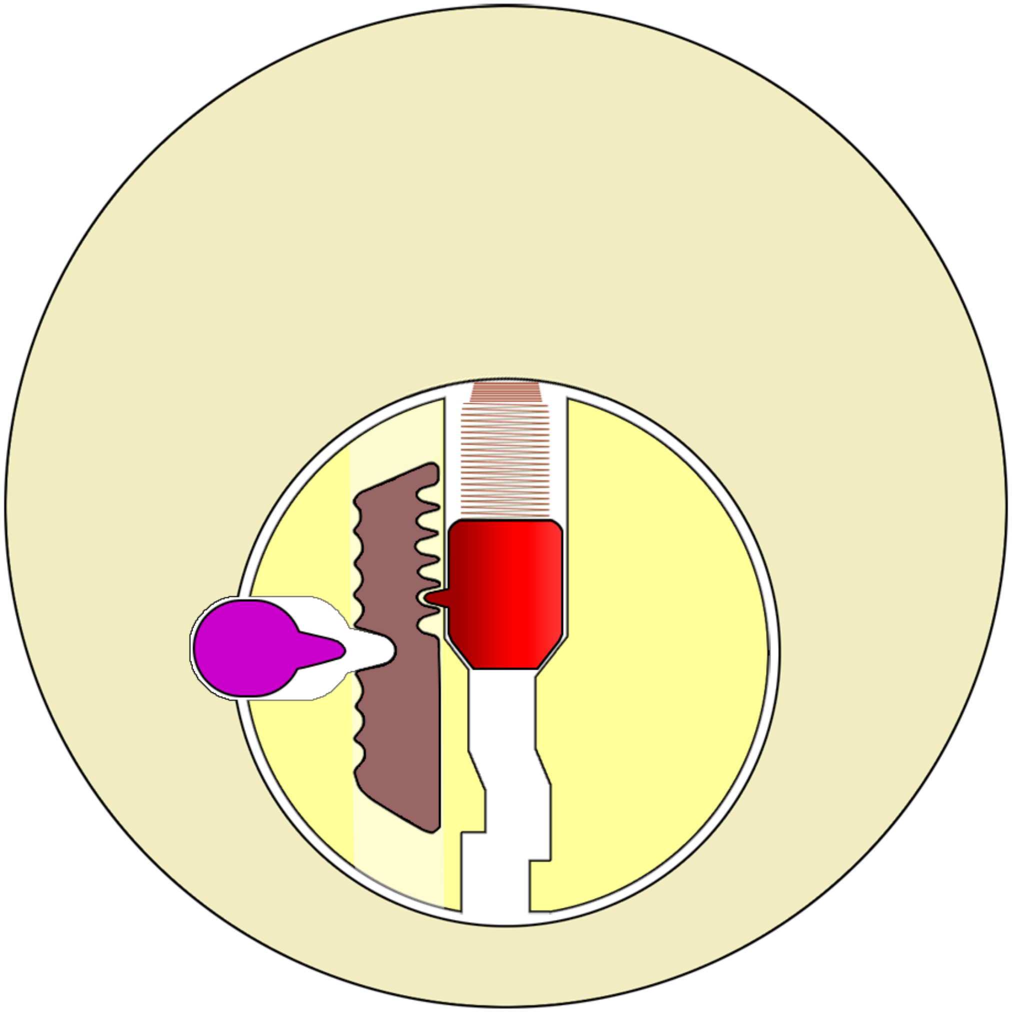
Kwikset Smart Series



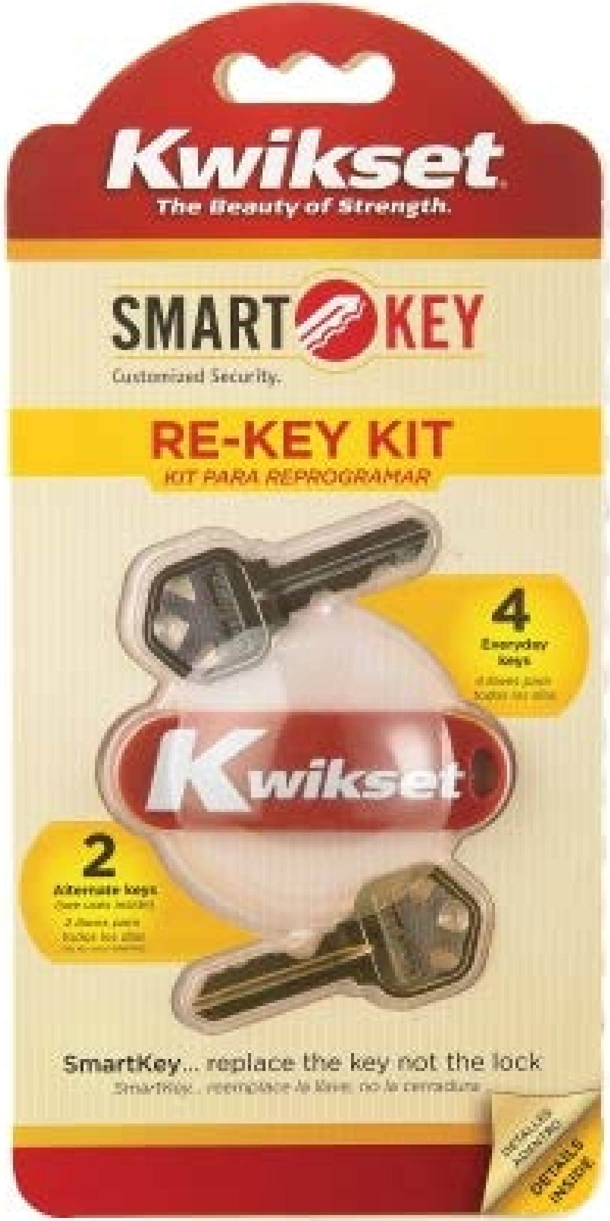


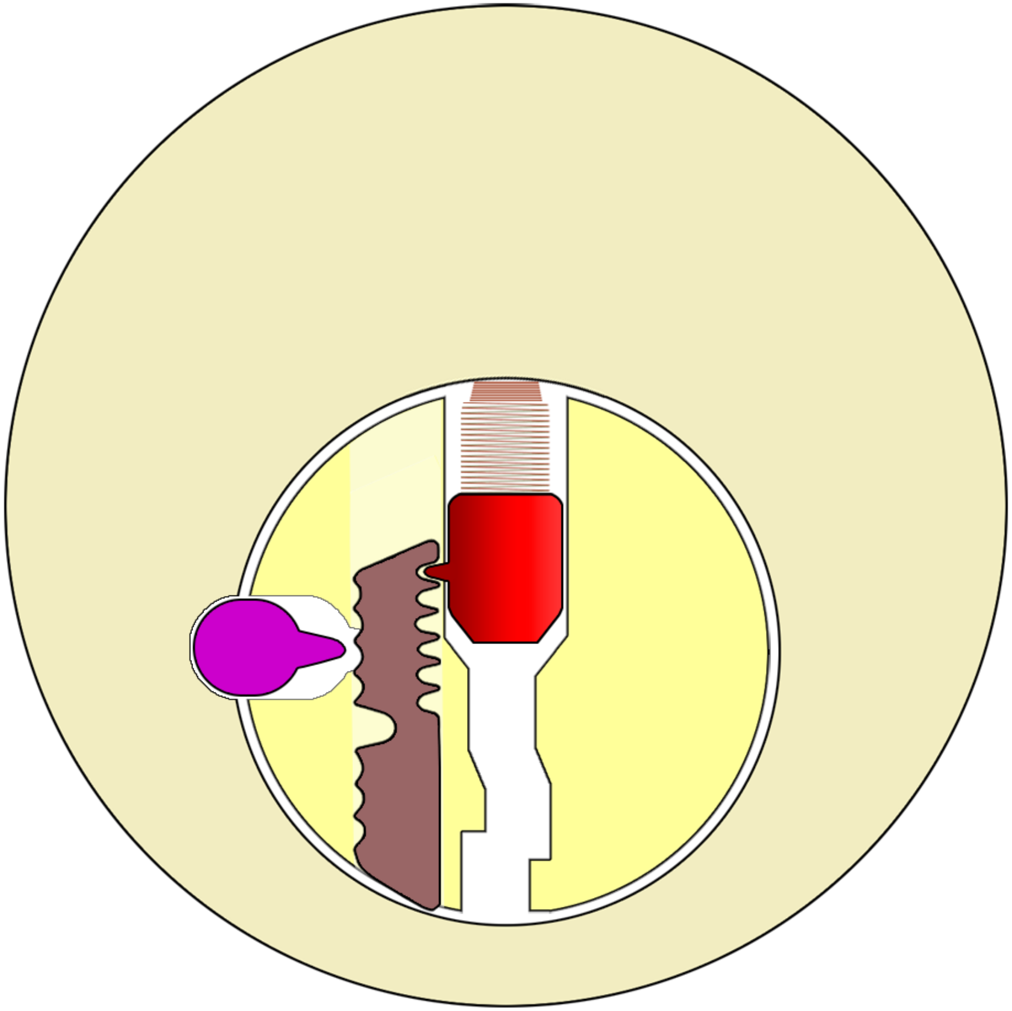
Kwikset Smart Series



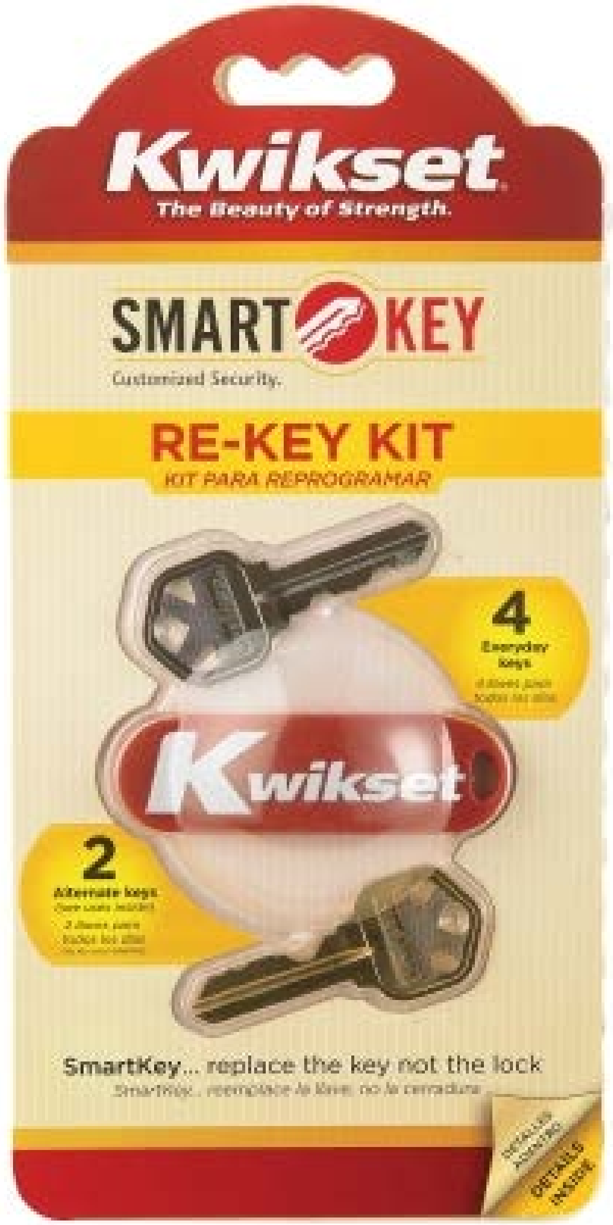


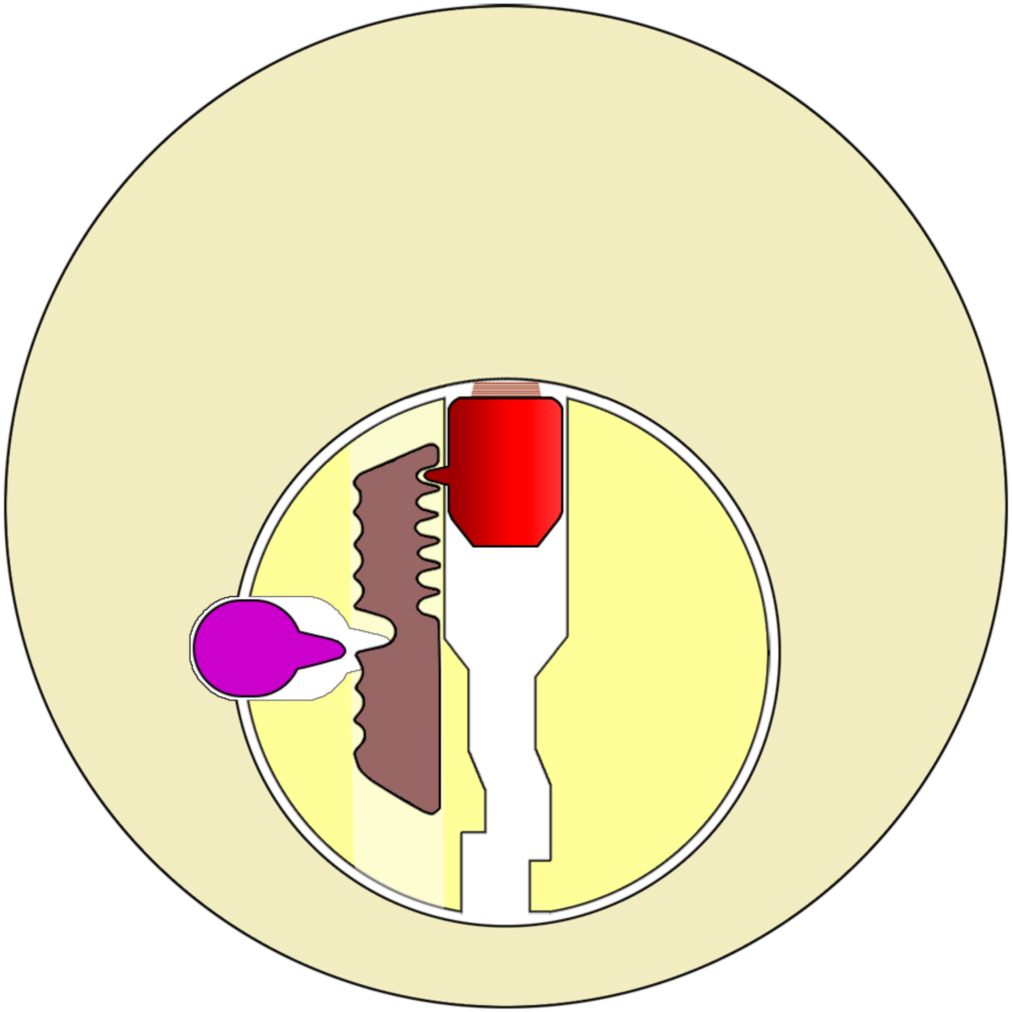
Kwikset Smart Series



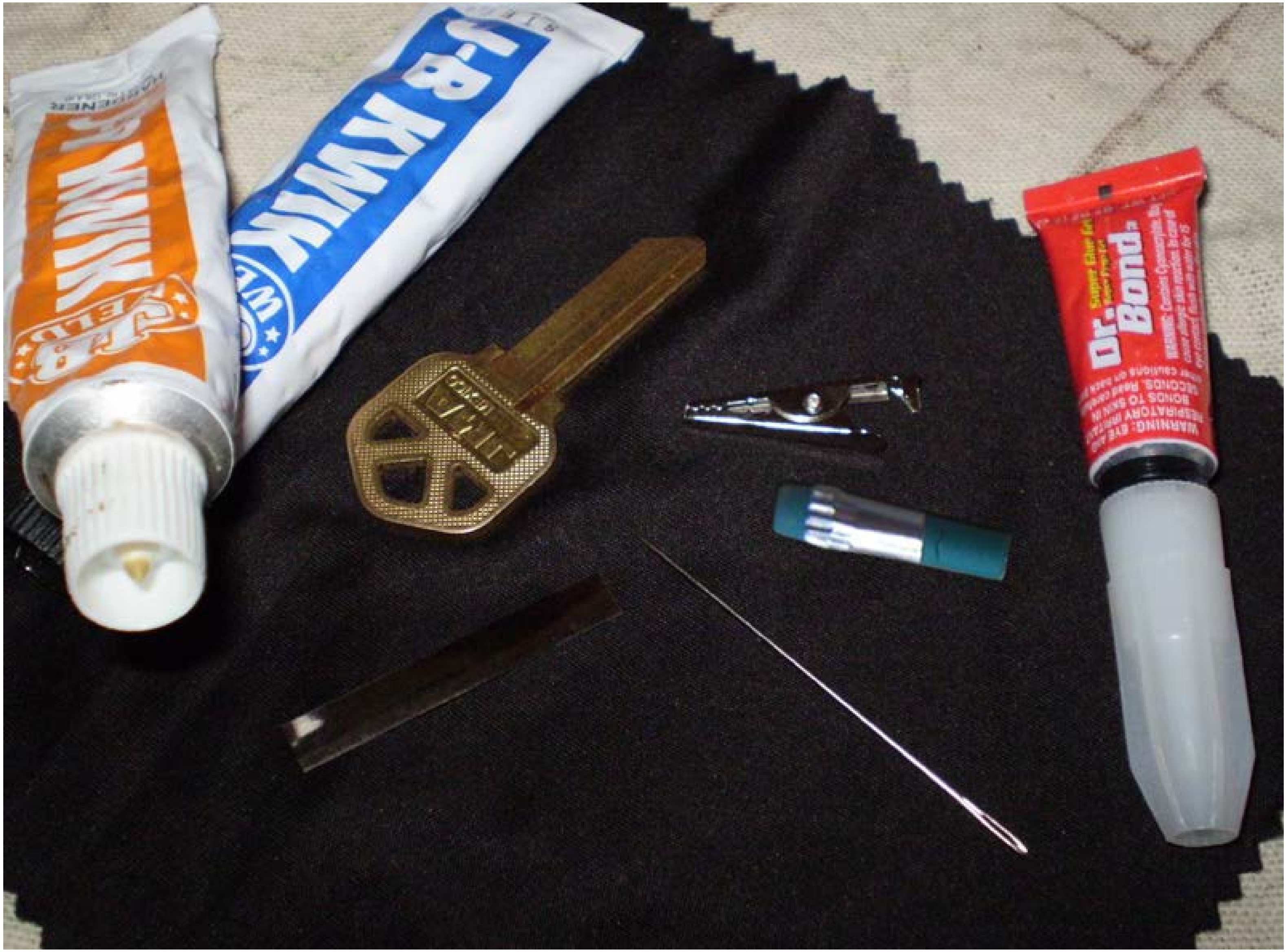


Kwikset Smart Series

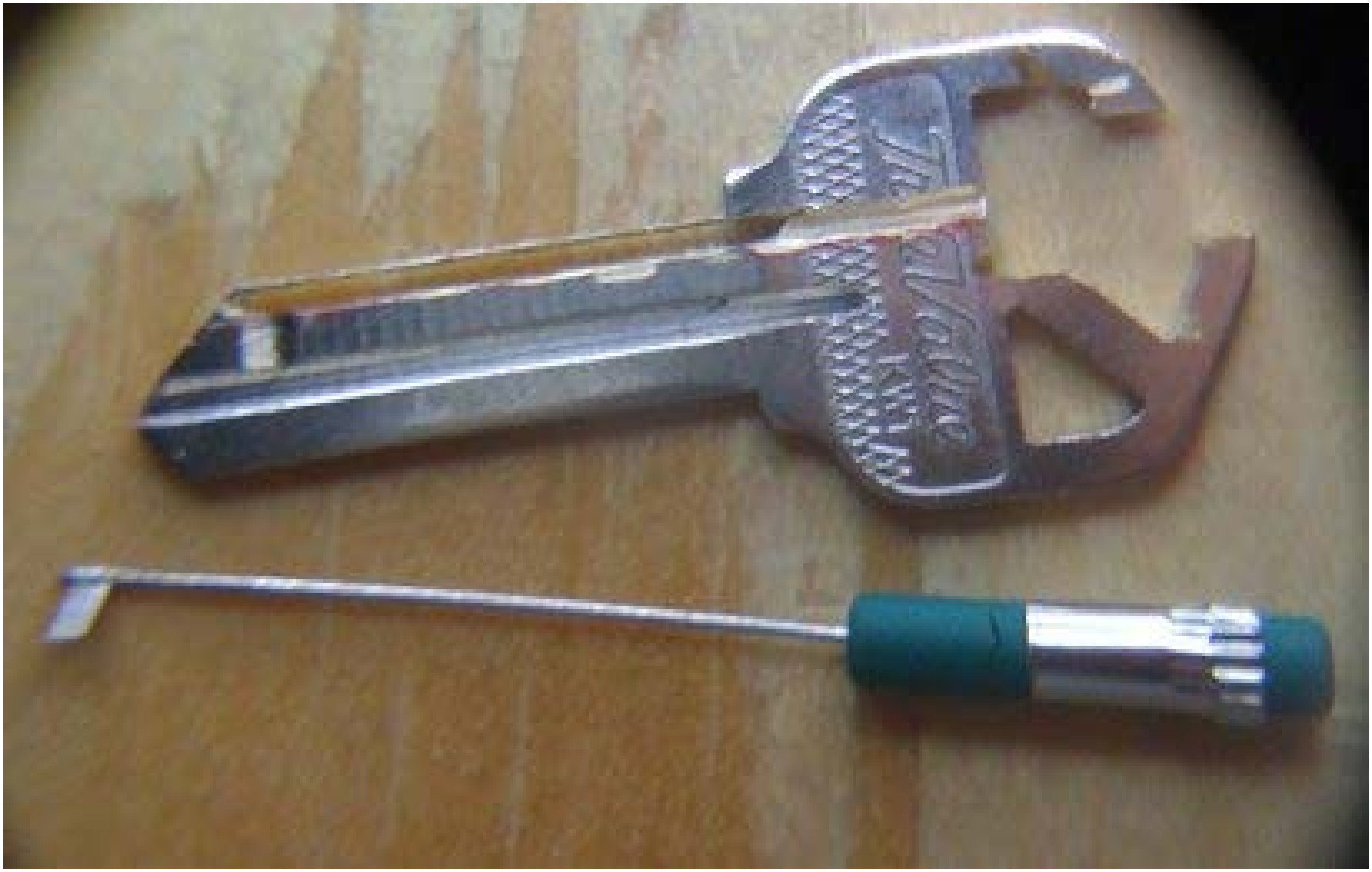




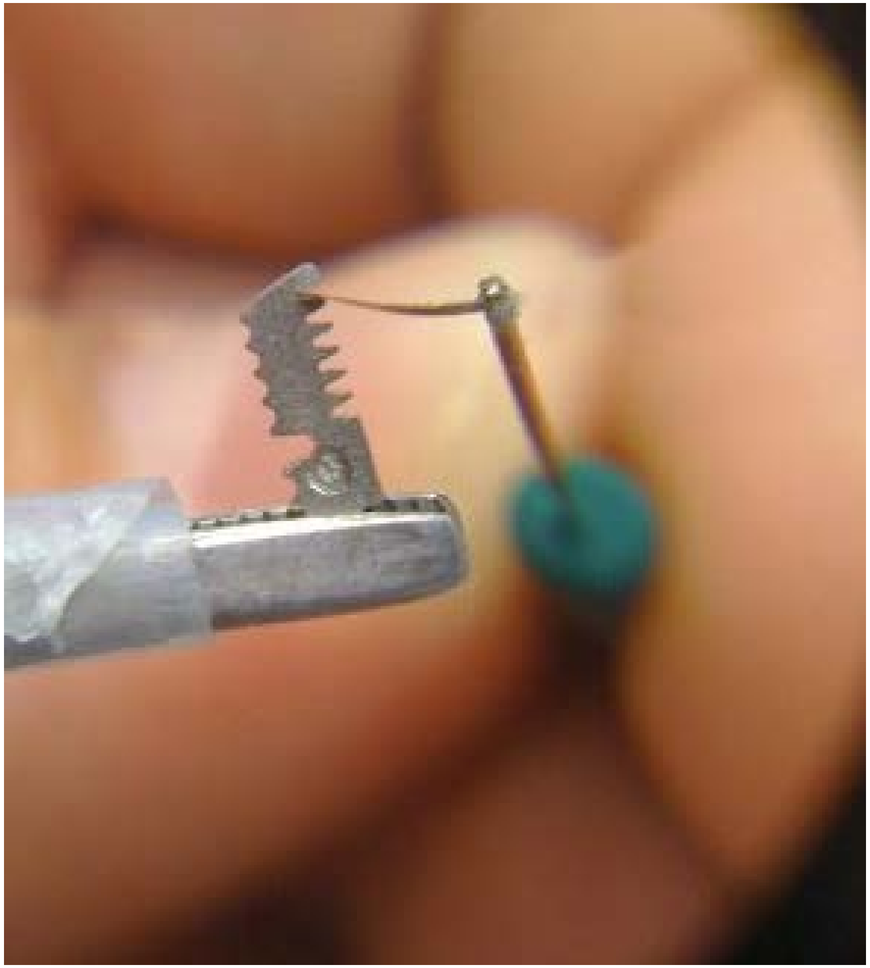
Kwikset Smart Series: Making Decoder

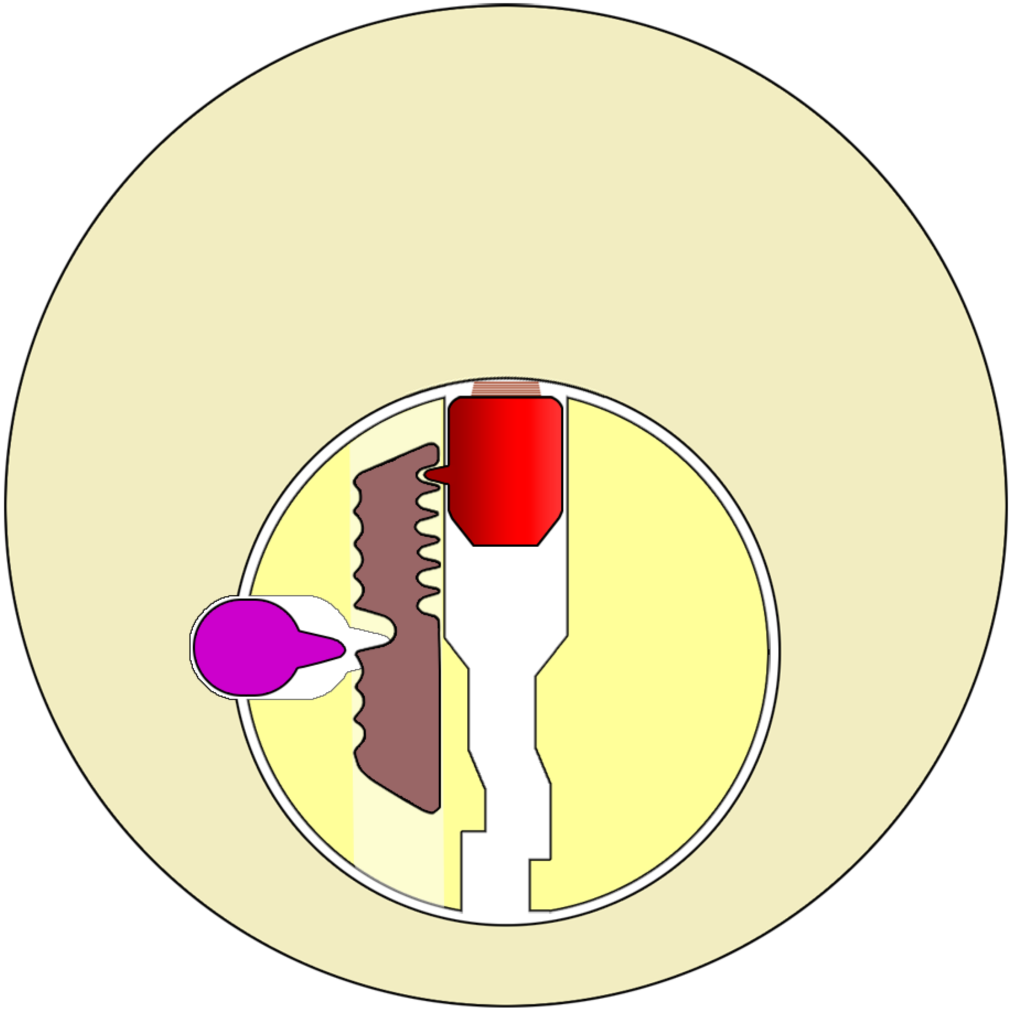


Kwikset Smart Series: The First Decoder

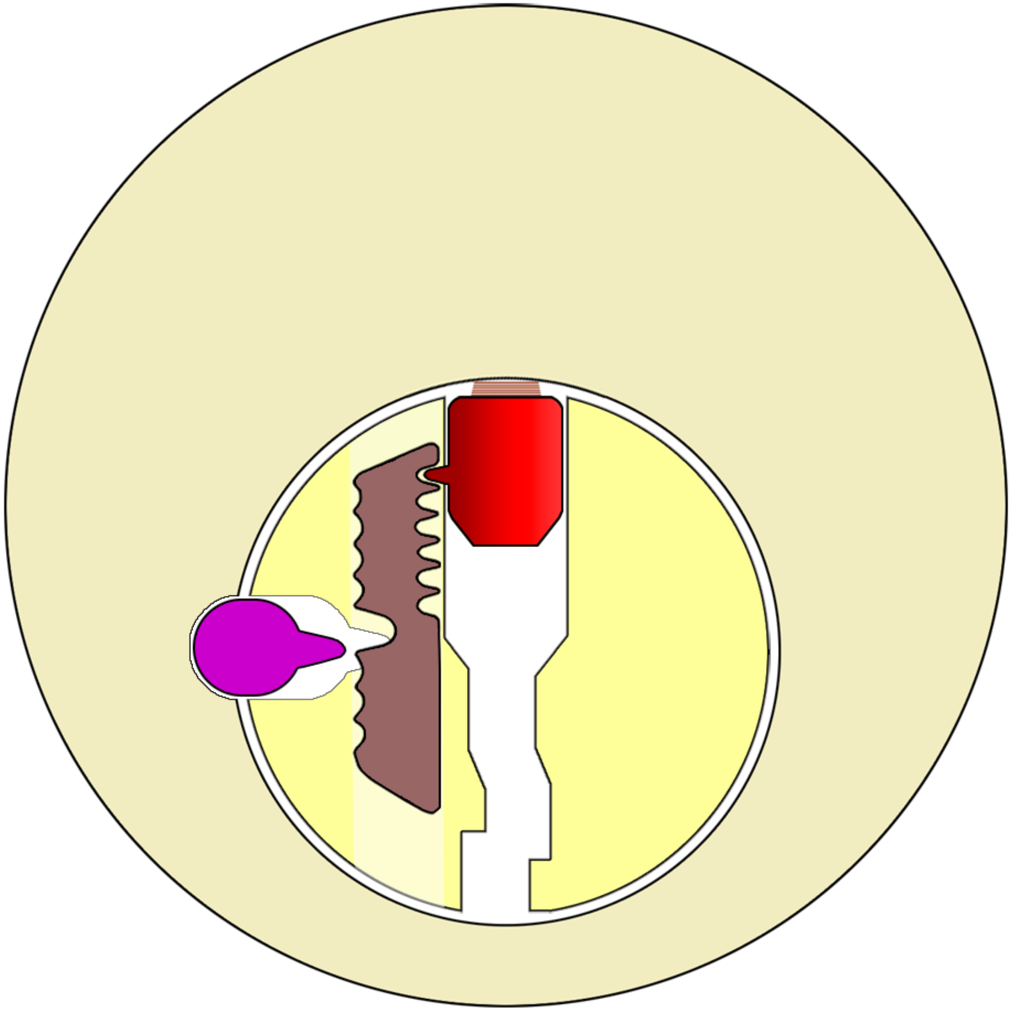


Kwikset Smart Series: Decoder Operation

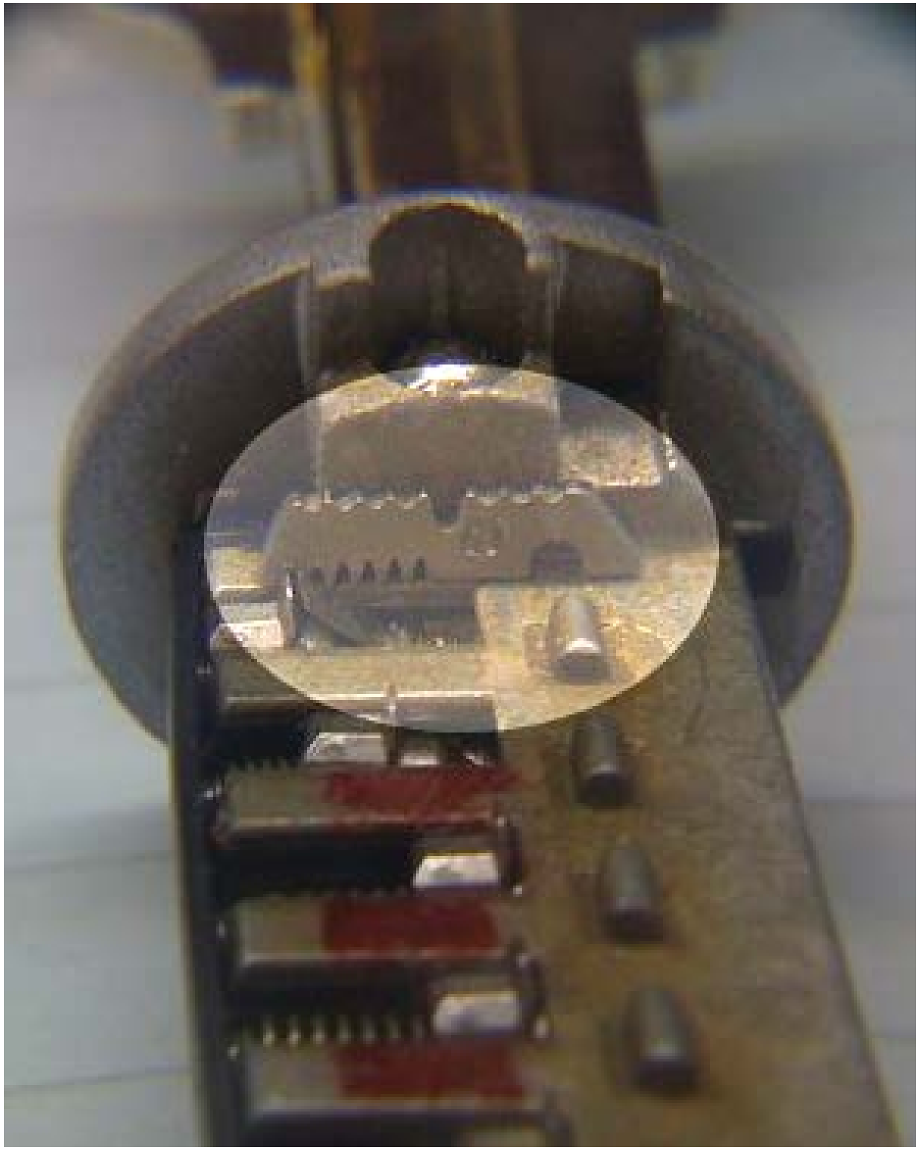


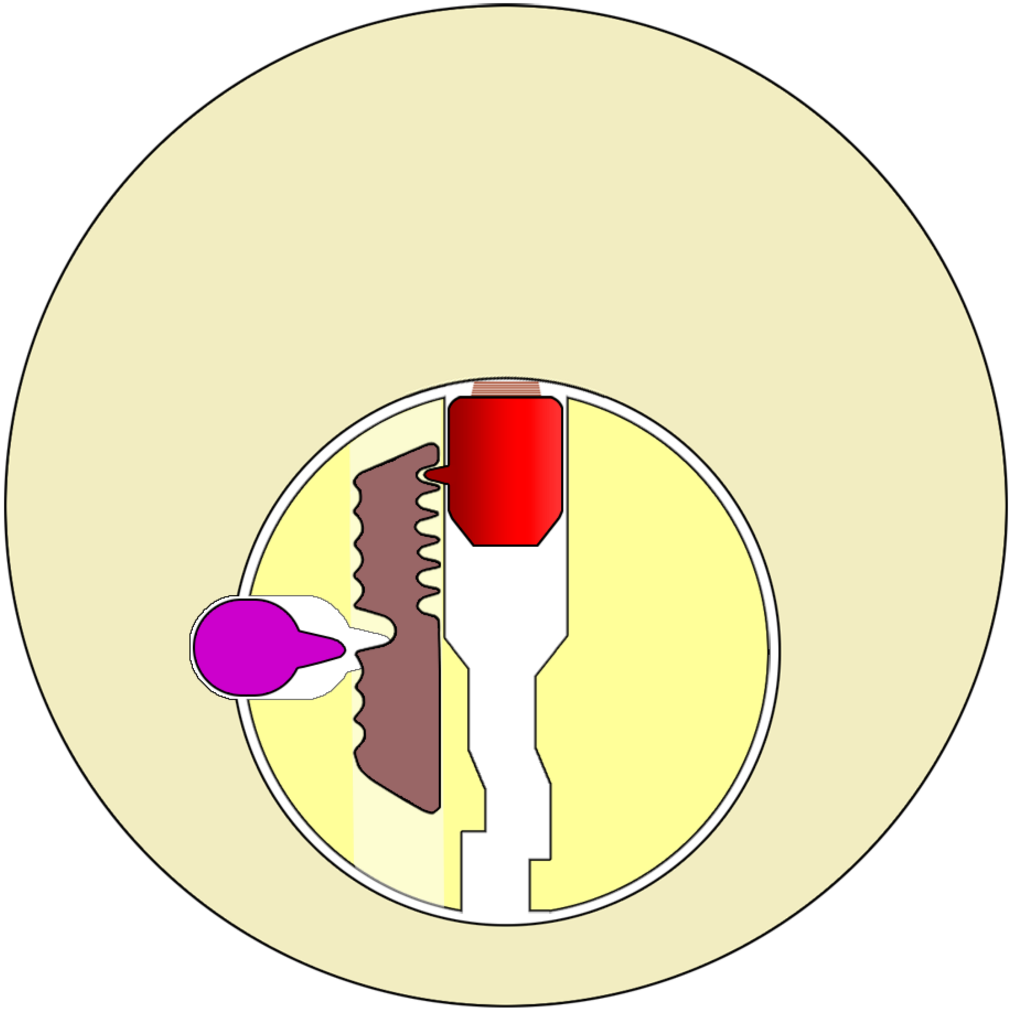


Kwikset Smart Series: Decoder Operation



Kwikset Smart Series: Decoder Operation





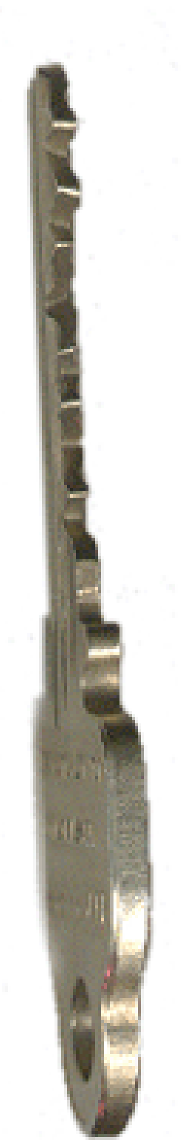
Informing Kwikset

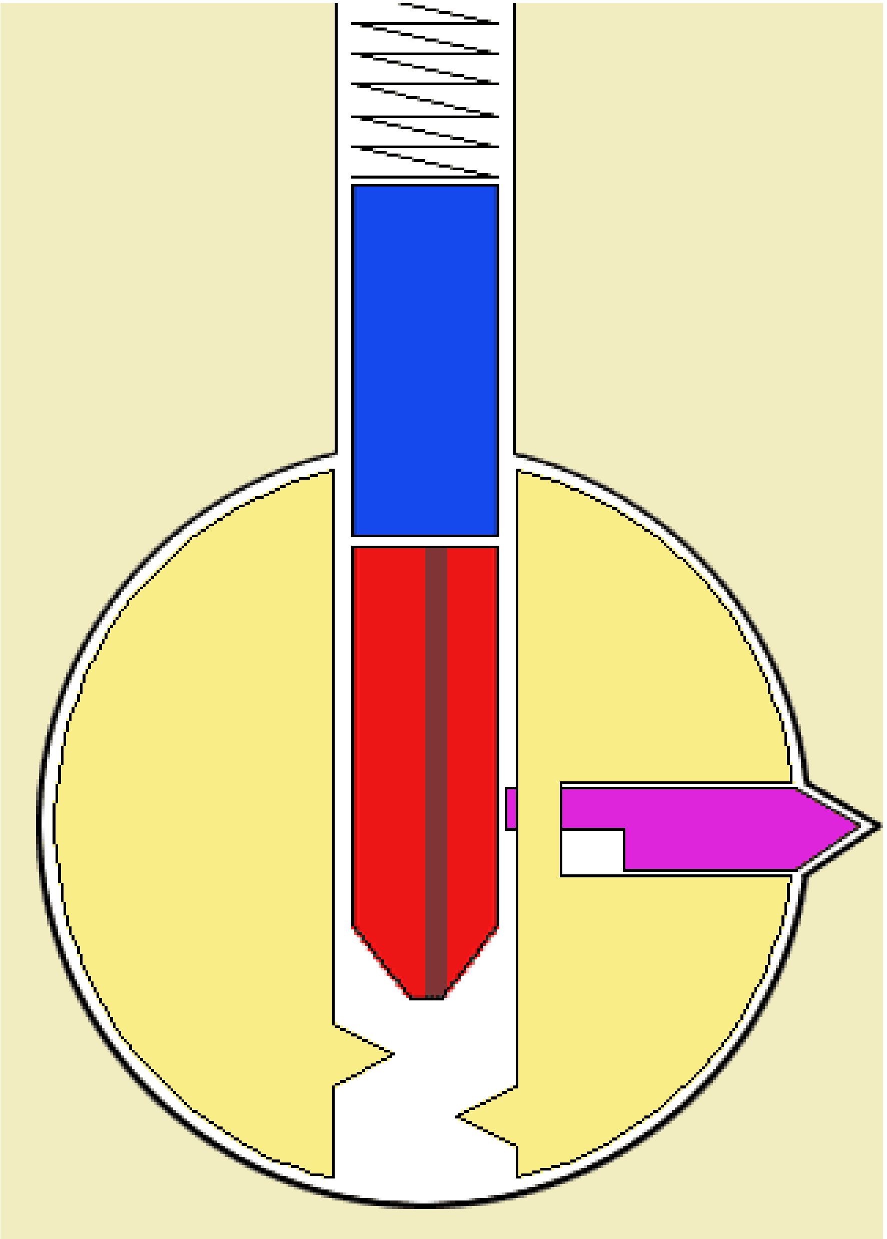
Kwikset Smart Series: Metallurgy Failure

There's also this little problem...

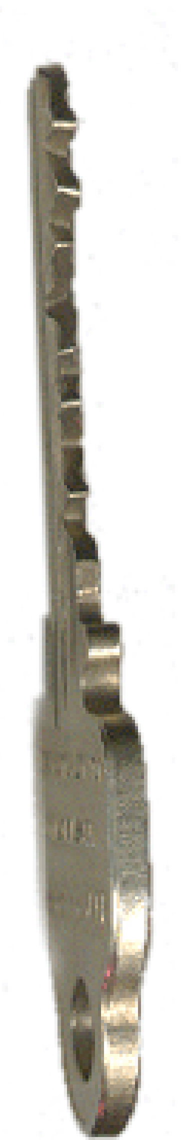
Kwikset Smasher Tool

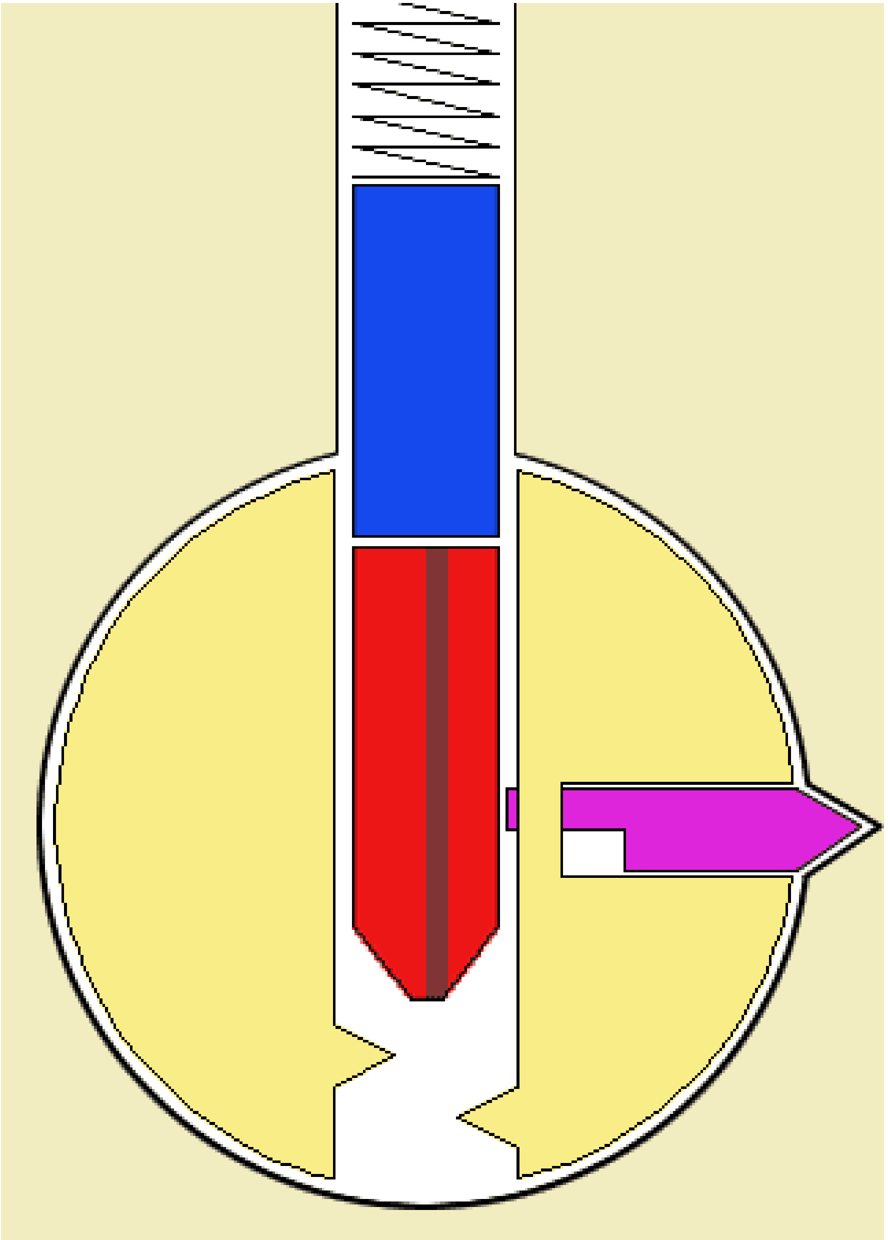
Decoding: Medeco Sidebar



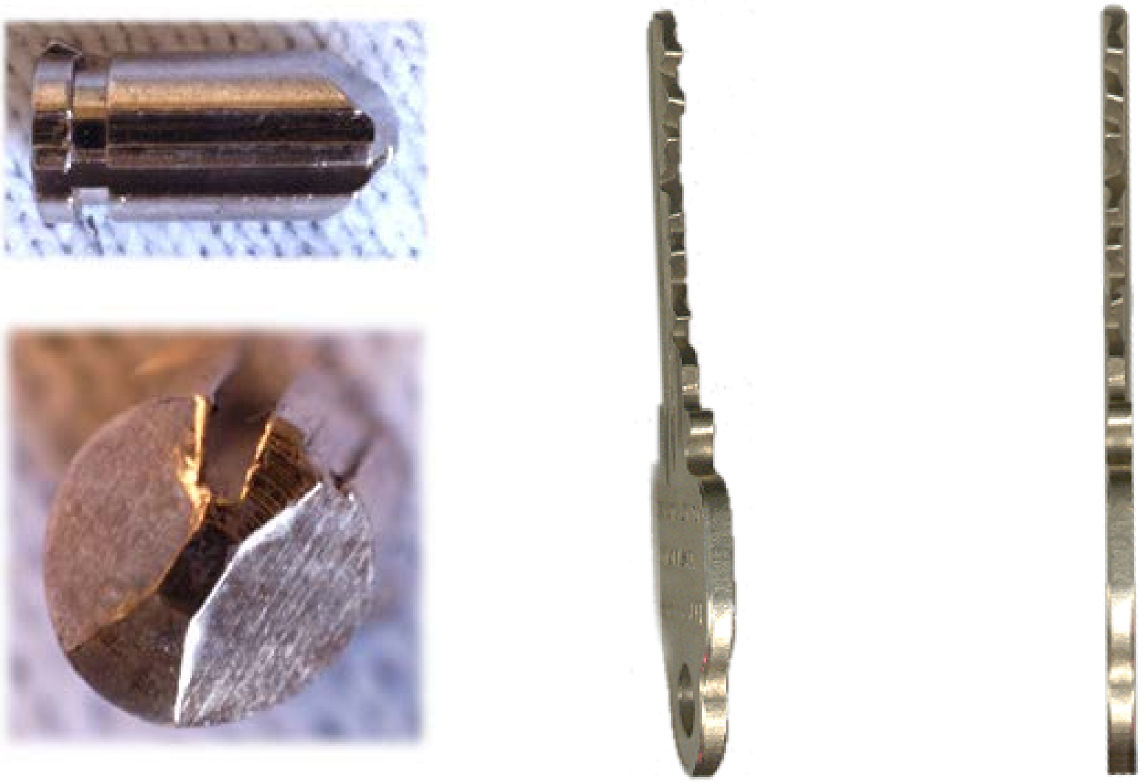


Decoding: Medeco Sidebar





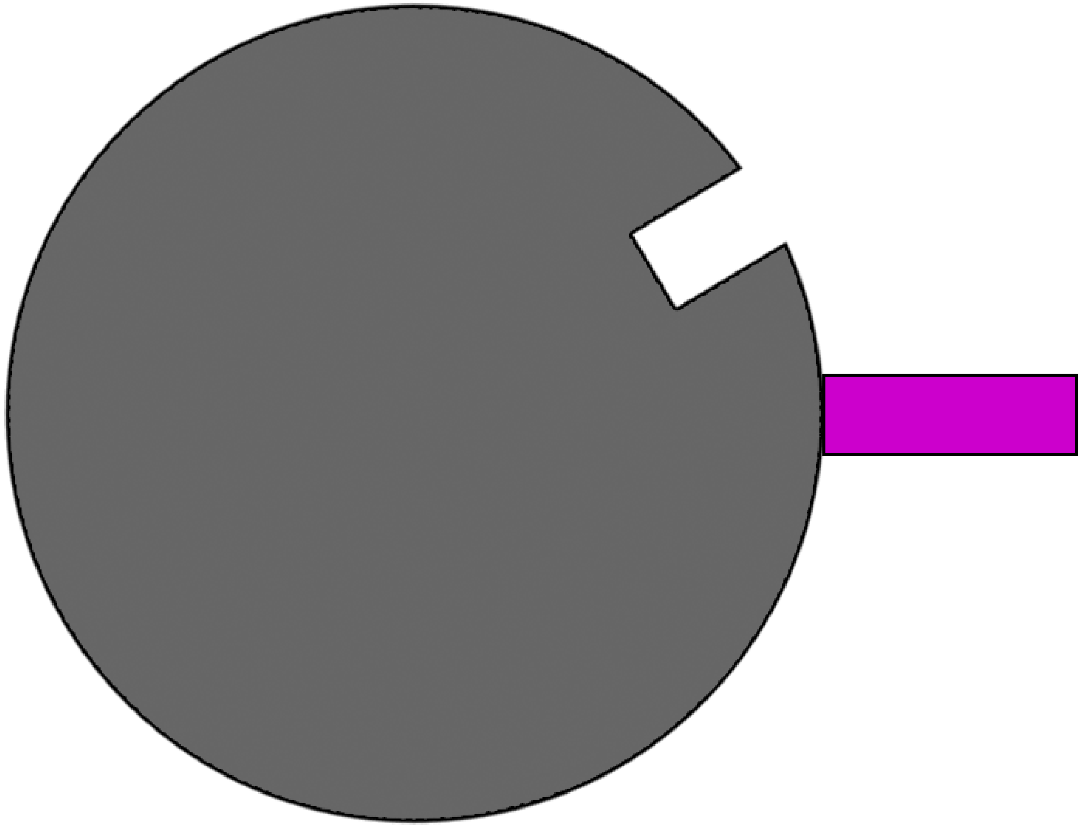
Decoding: Medeco Sidebar

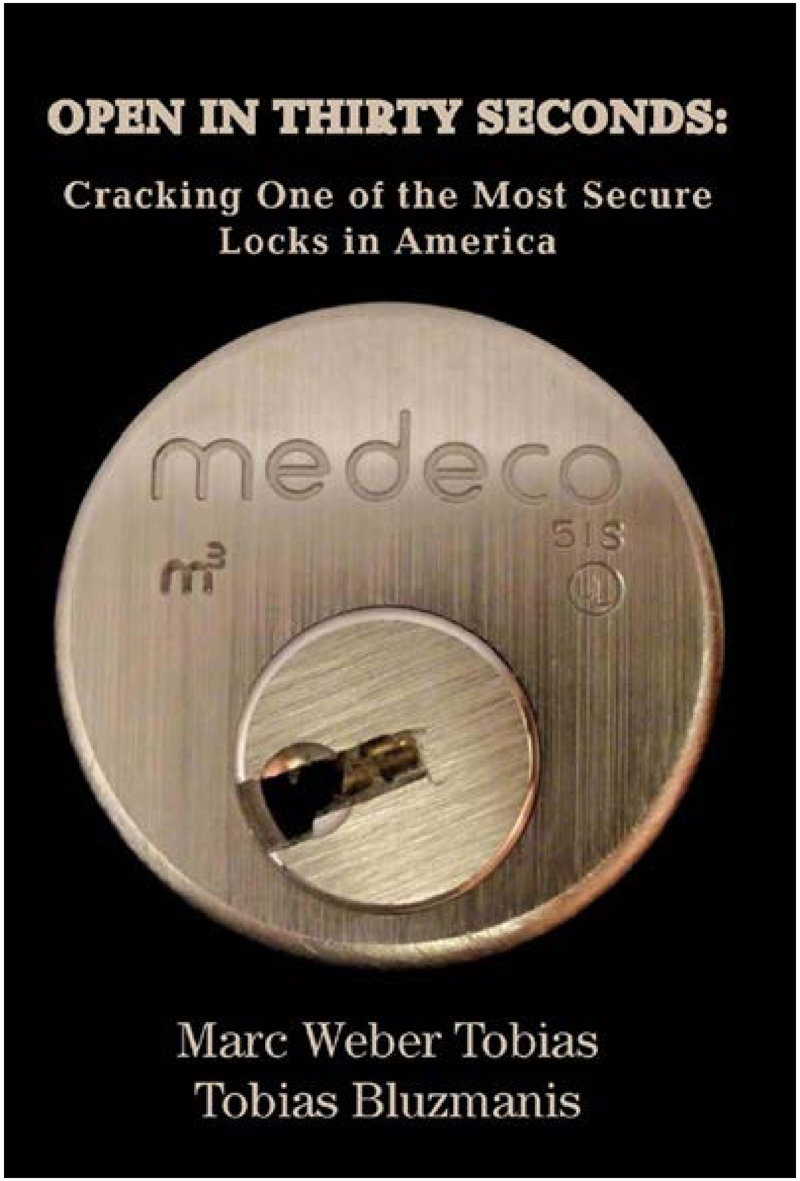


Medeco plug exposed, key pins rotating to align sidebar cuts

Top View   Side View

Decoding: Medeco Sidebar



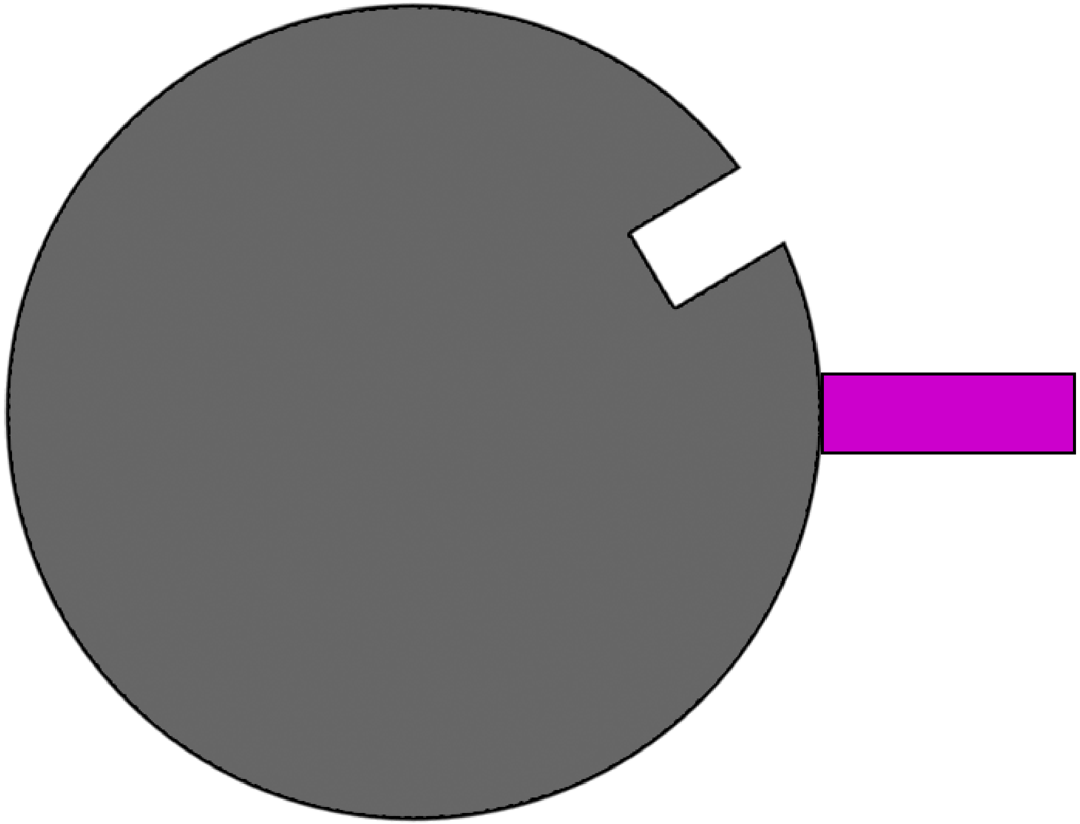


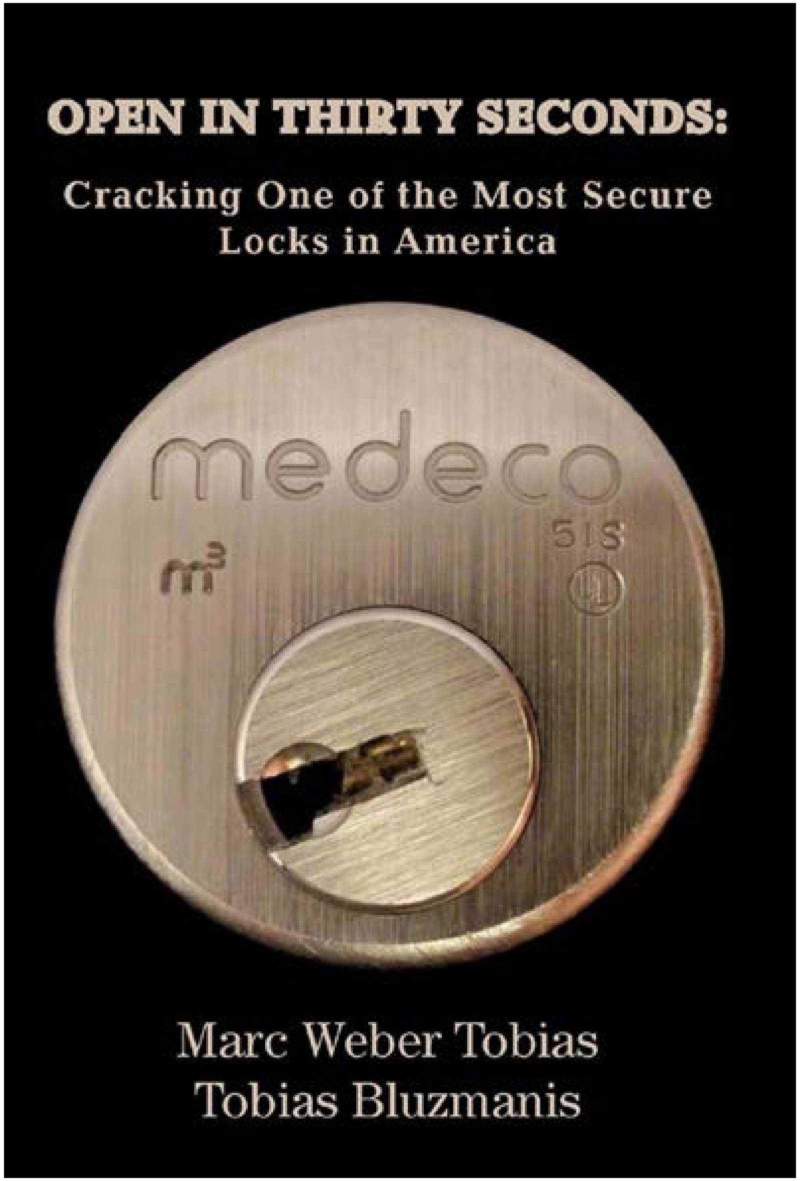
OPEN IN THIRTY SECONDS:

Cracking One of the Most Secure Locks in America

Marc Weber Tobias
Tobias Bluzmanis

Decoding: Medeco Sidebar



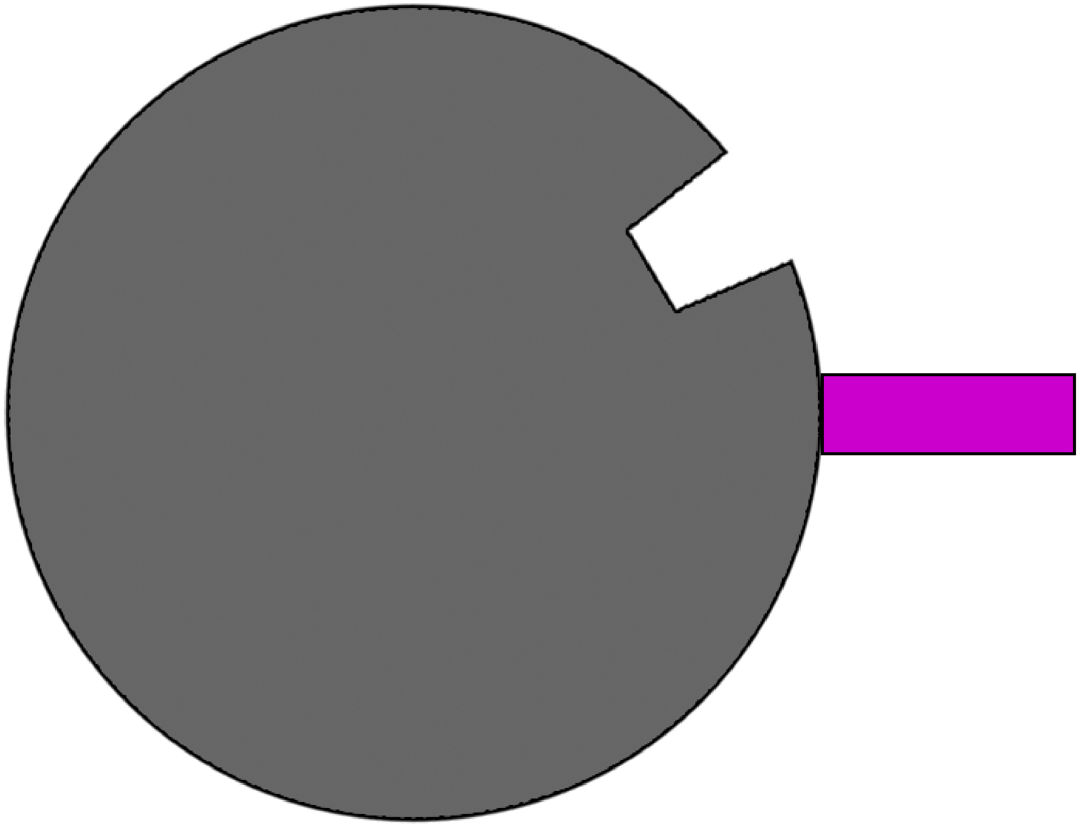


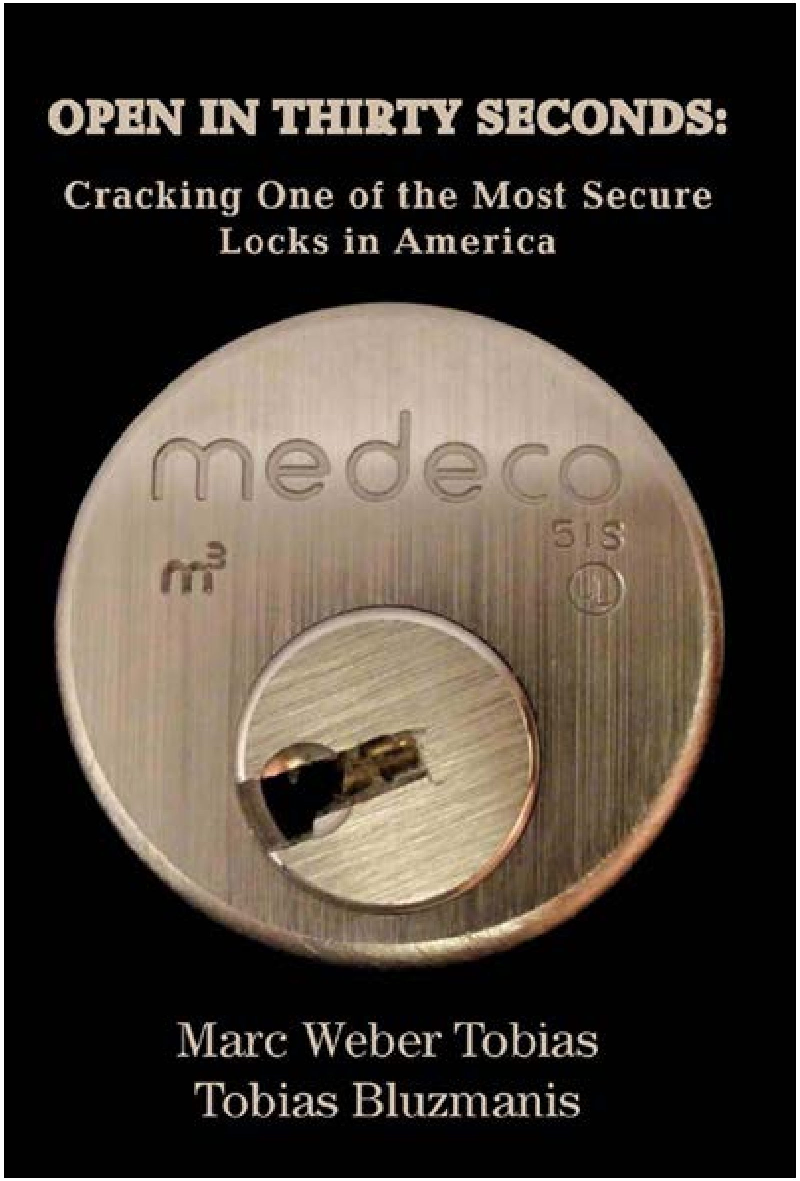
OPEN IN THIRTY SECONDS:

Cracking One of the Most Secure Locks in America

Marc Weber Tobias
Tobias Bluzmanis

Decoding: Medeco Sidebar



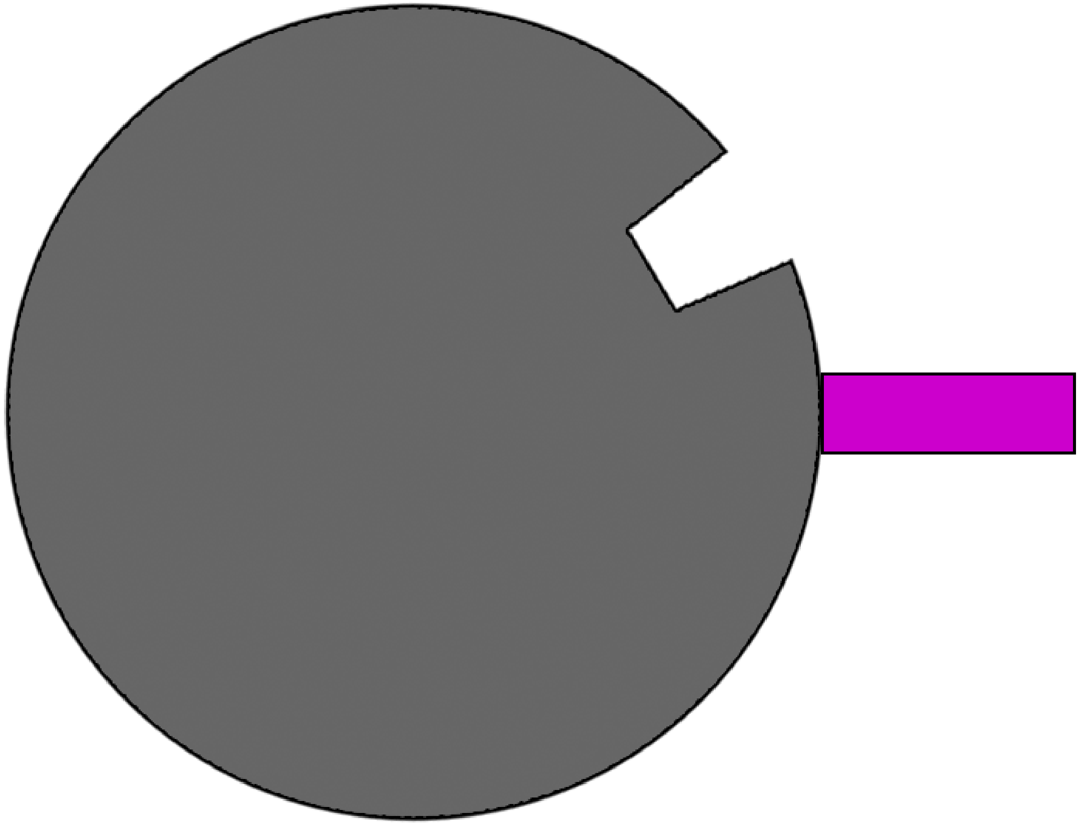


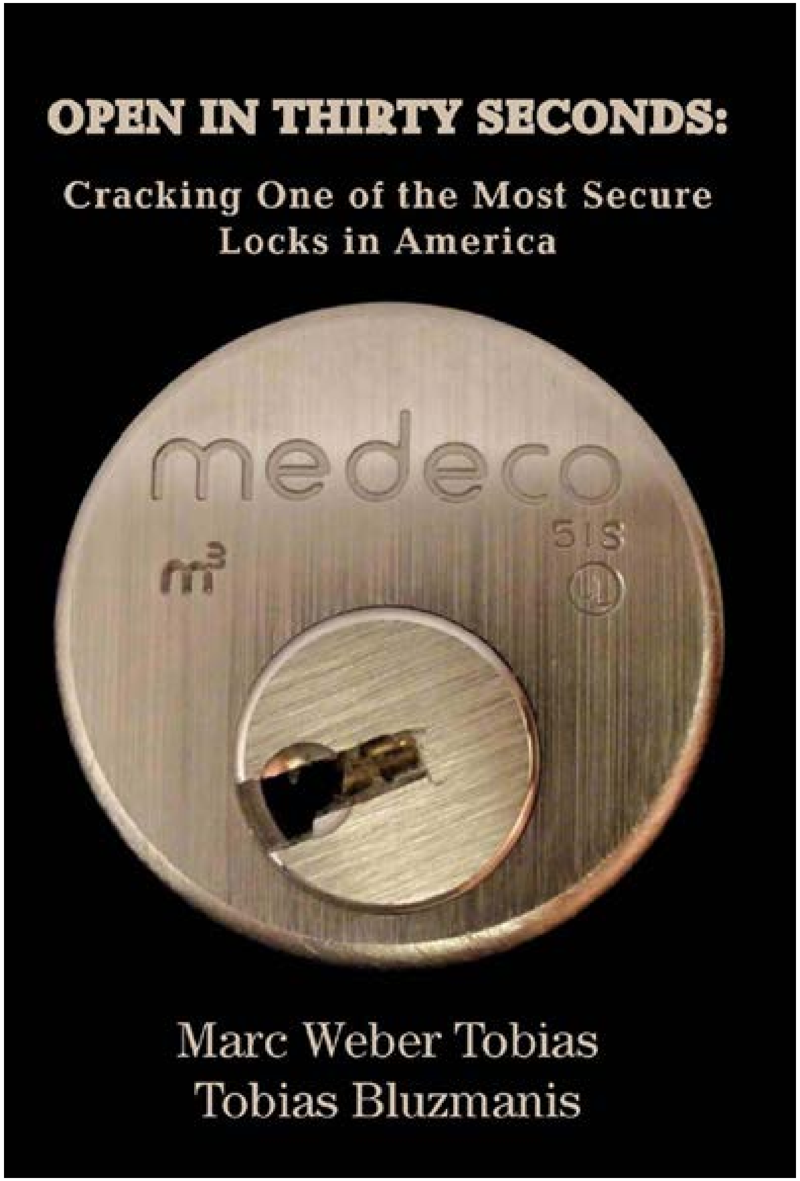
OPEN IN THIRTY SECONDS:

Cracking One of the Most Secure Locks in America

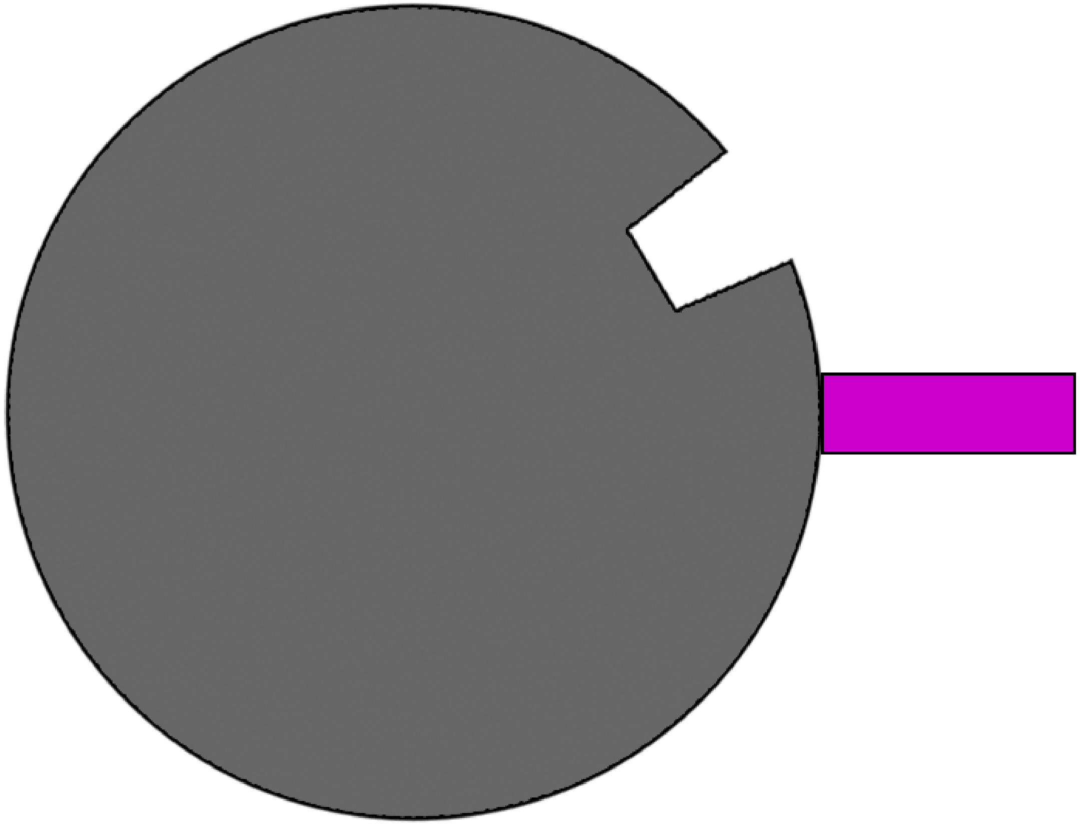
Marc Weber Tobias
Tobias Bluzmanis

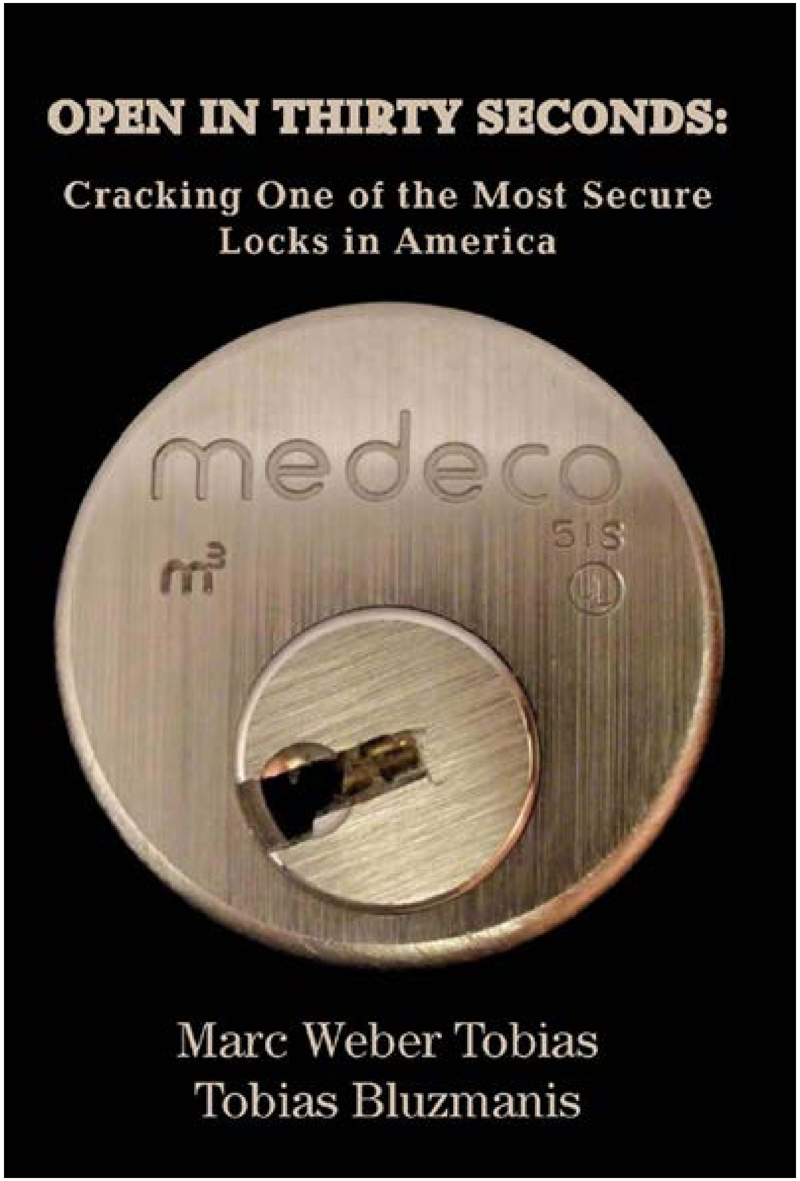
Decoding: Medeco Sidebar





Decoding: Medeco Sidebar



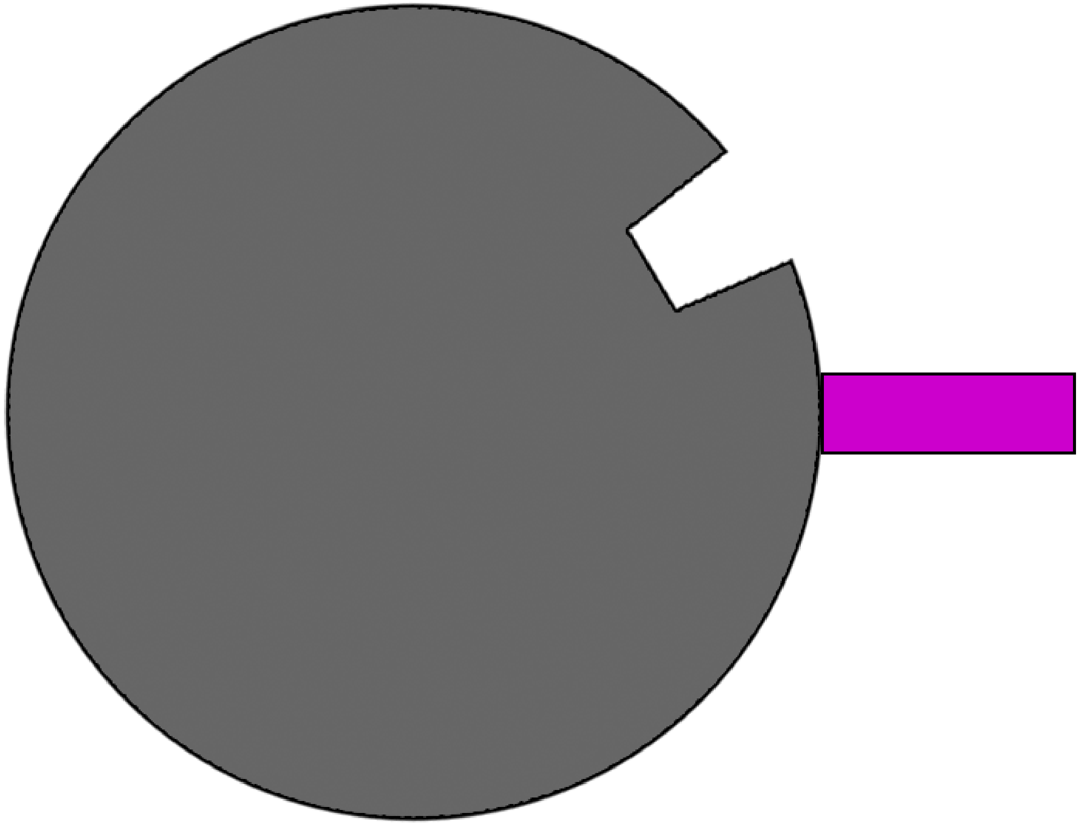


OPEN IN THIRTY SECONDS:

Cracking One of the Most Secure Locks in America

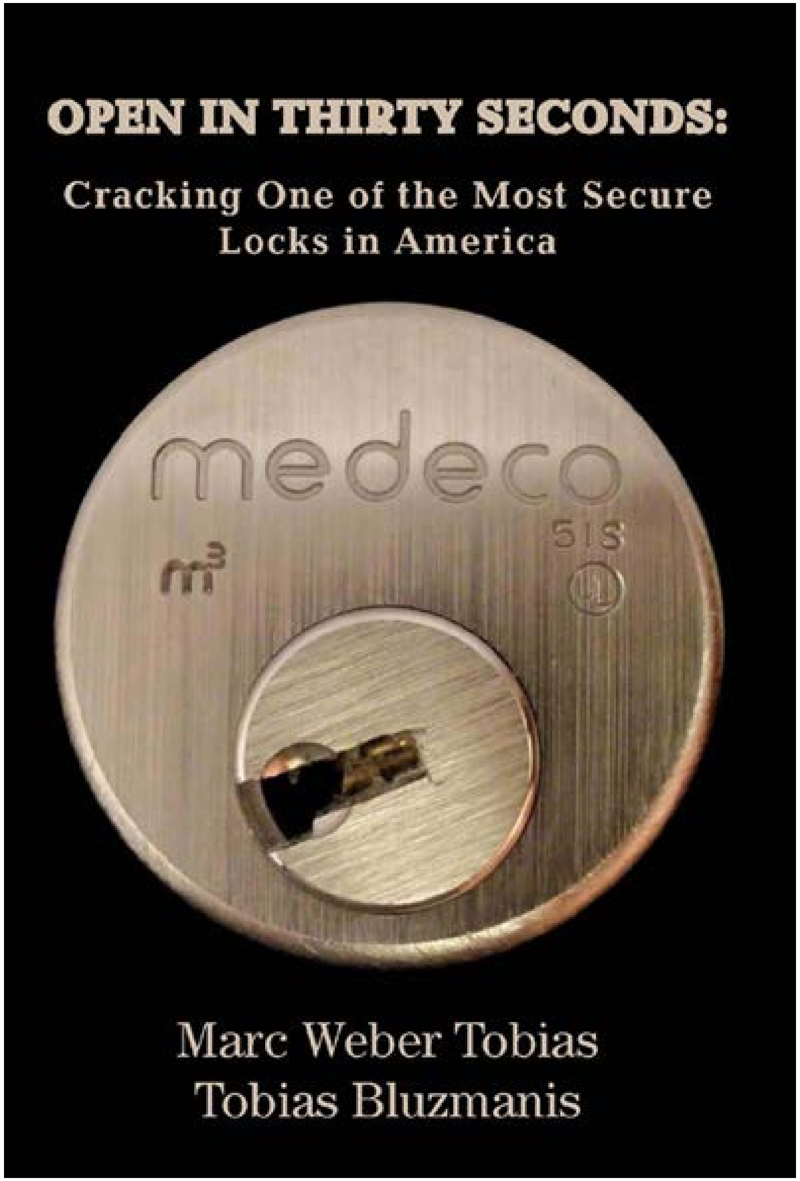
Marc Weber Tobias
Tobias Bluzmanis

Decoding: Medeco Sidebar



Successful Medeco Attacks

Marc Tobias LockCon

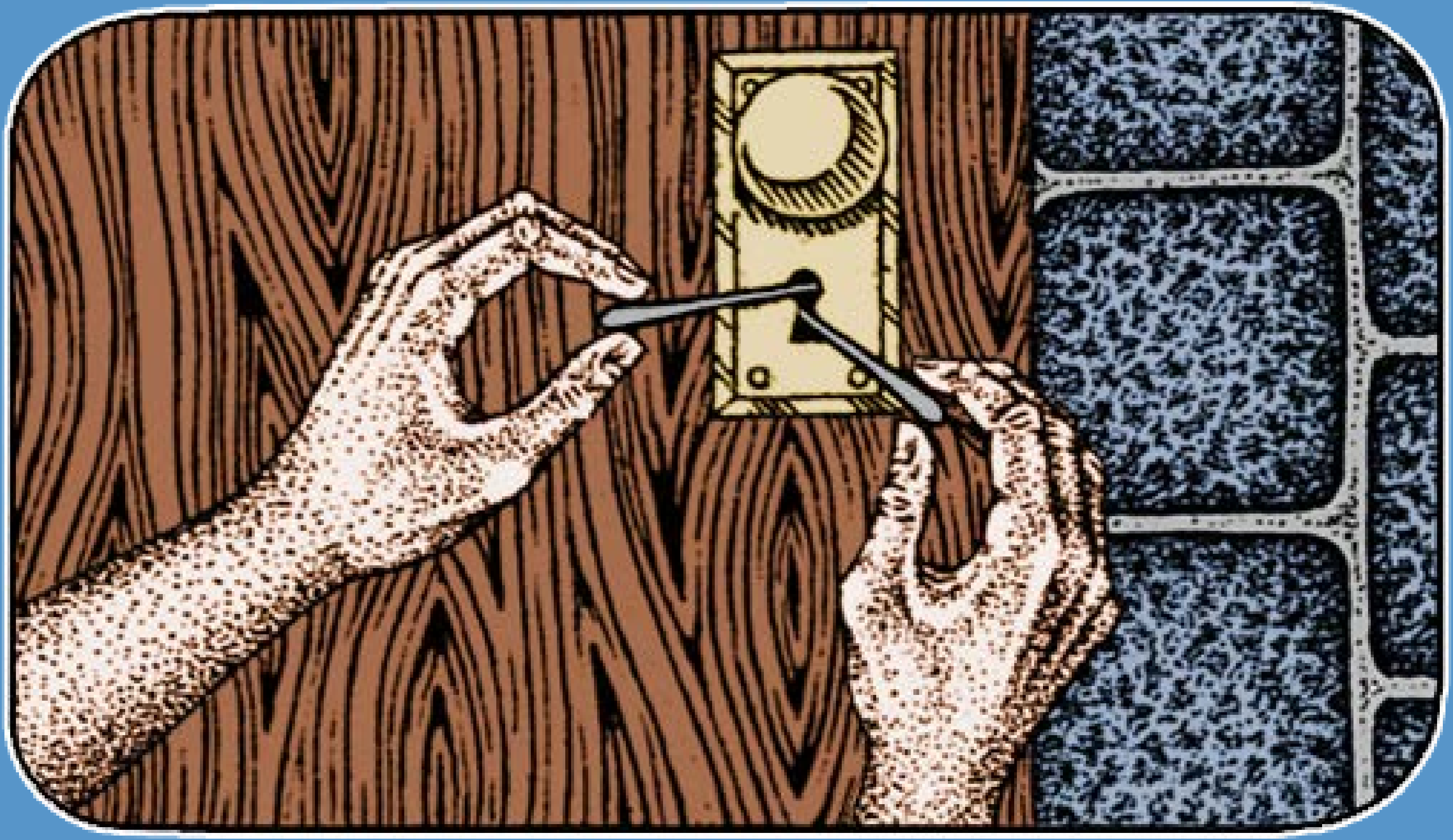


OPEN IN THIRTY SECONDS:

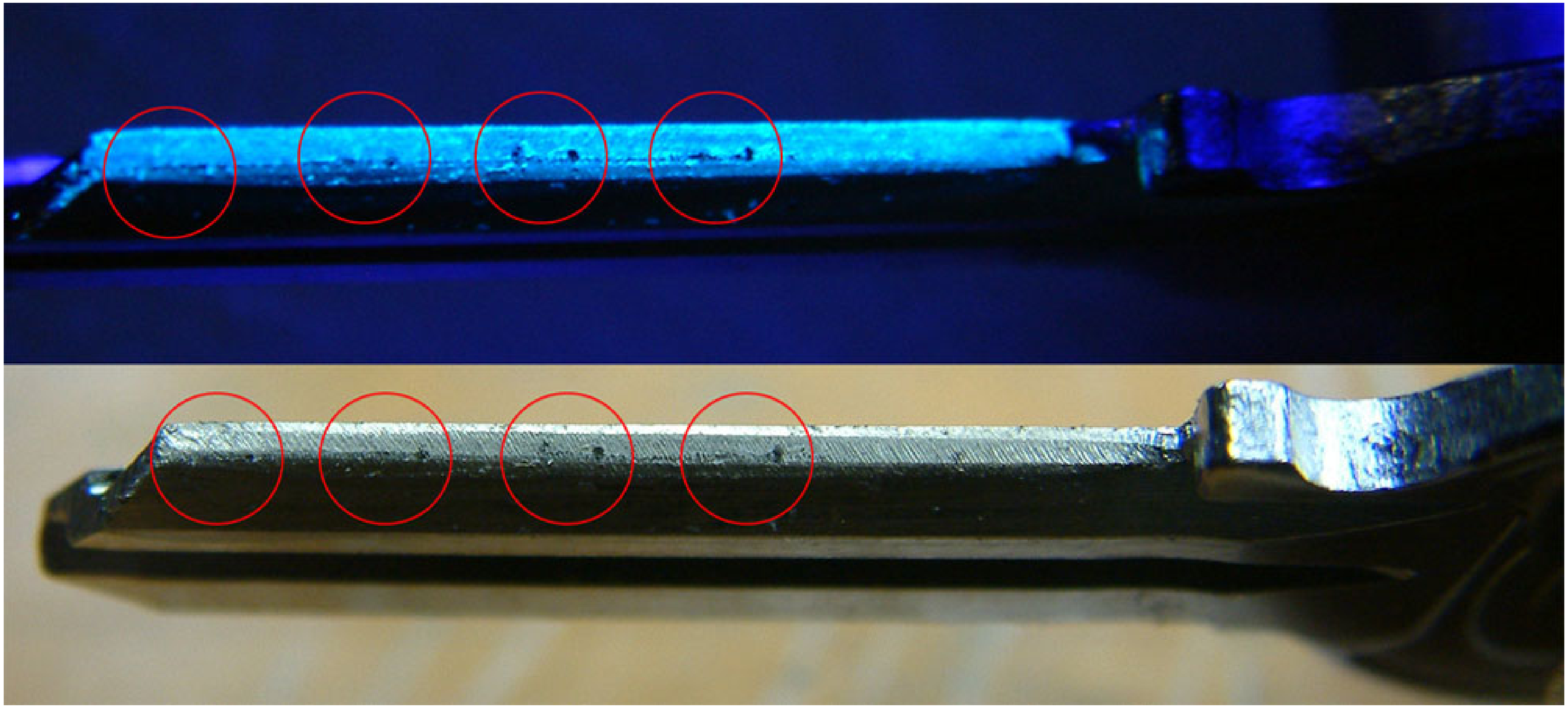
Cracking One of the Most Secure Locks in America

Marc Weber Tobias
Tobias Bluzmanis

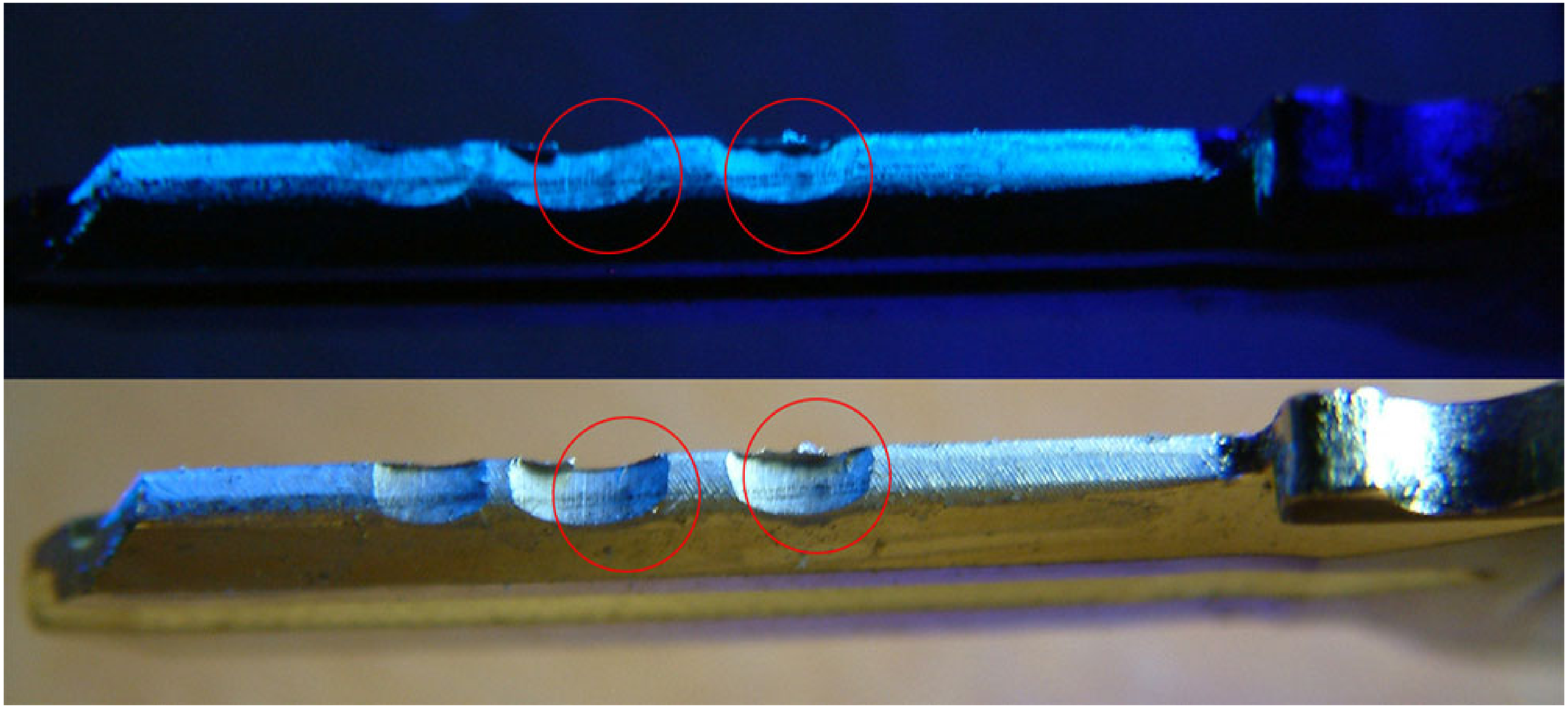
Impressioning



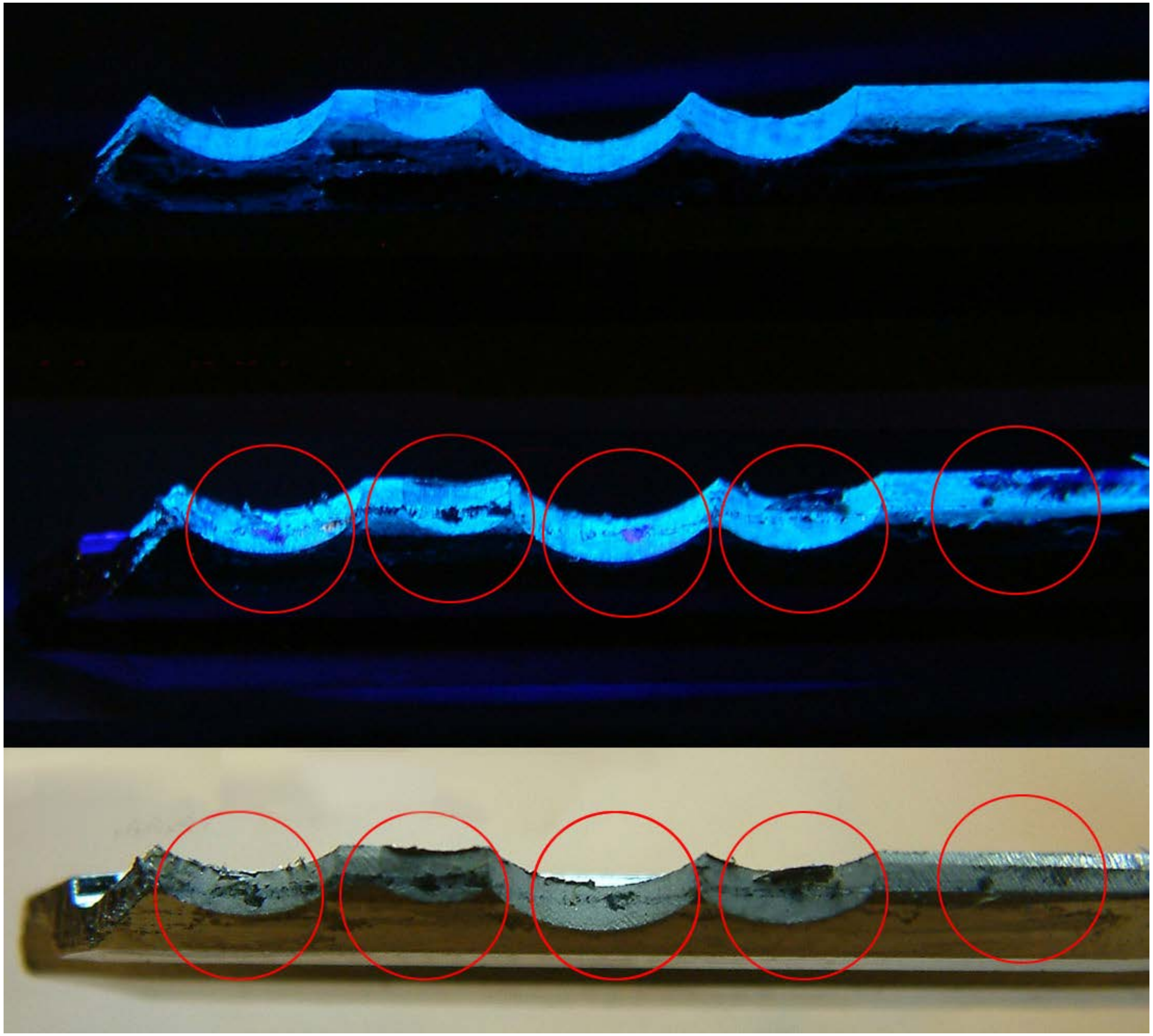
Impressioning



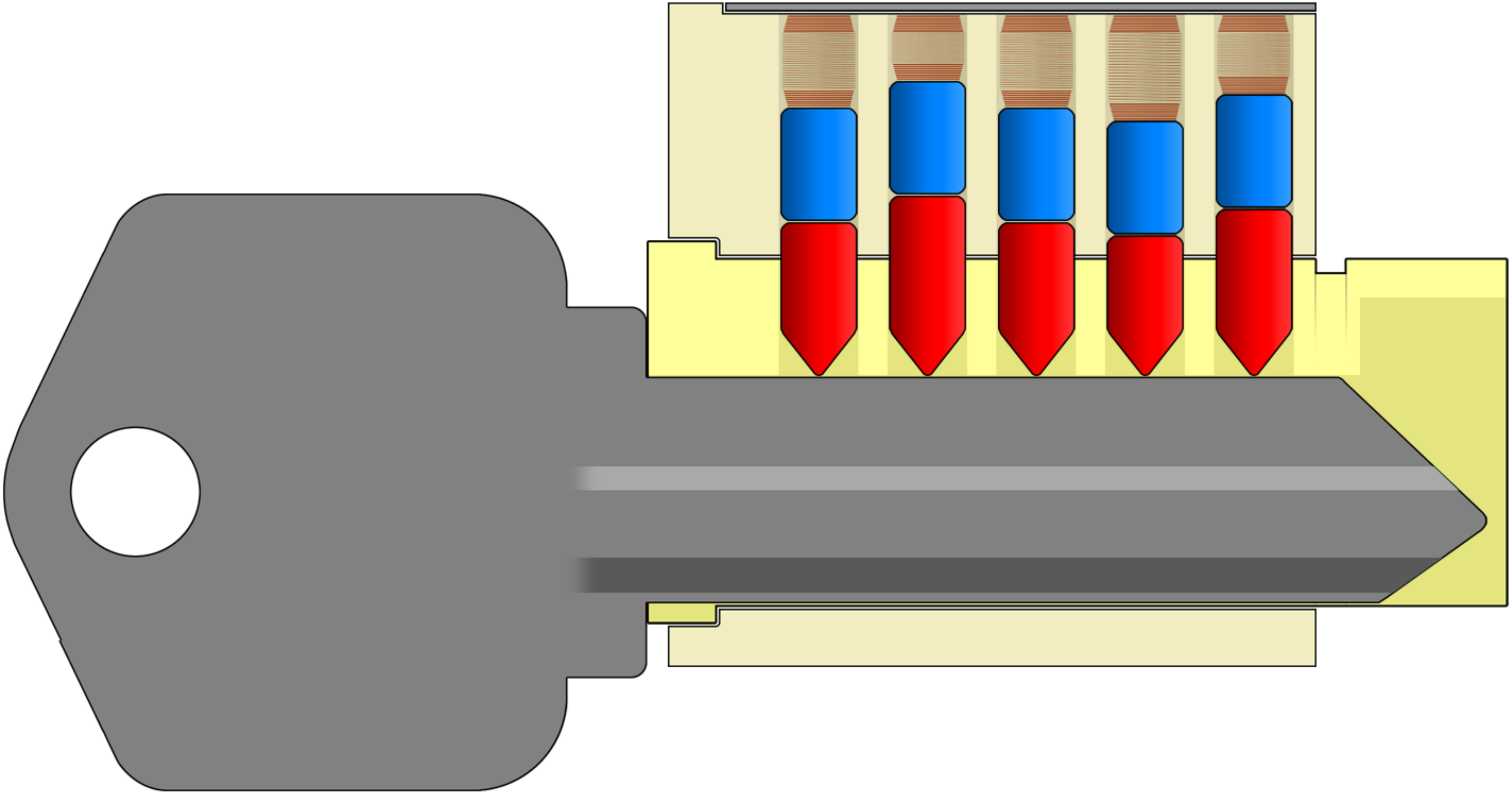
Impressioning



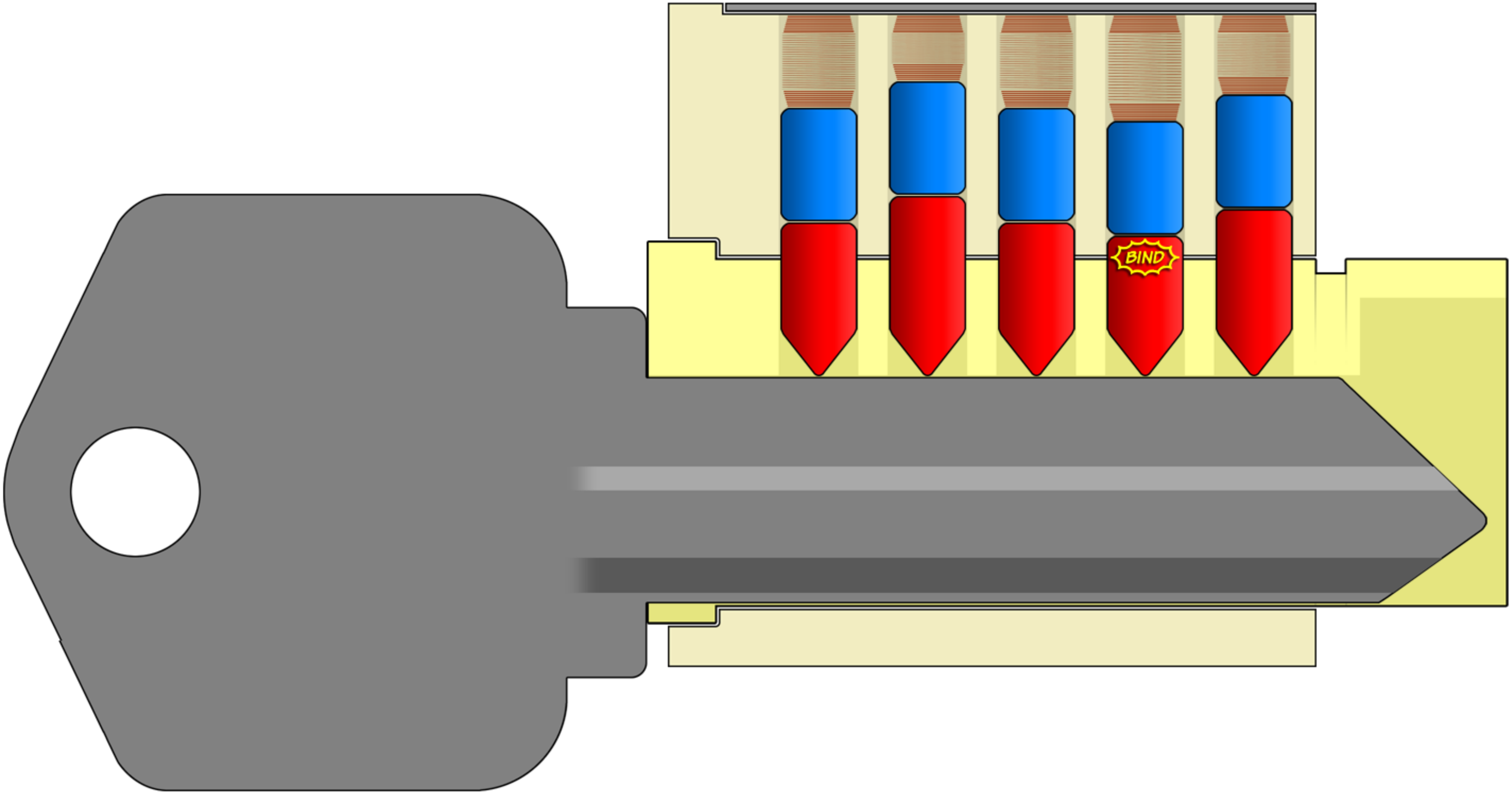
Impressioning



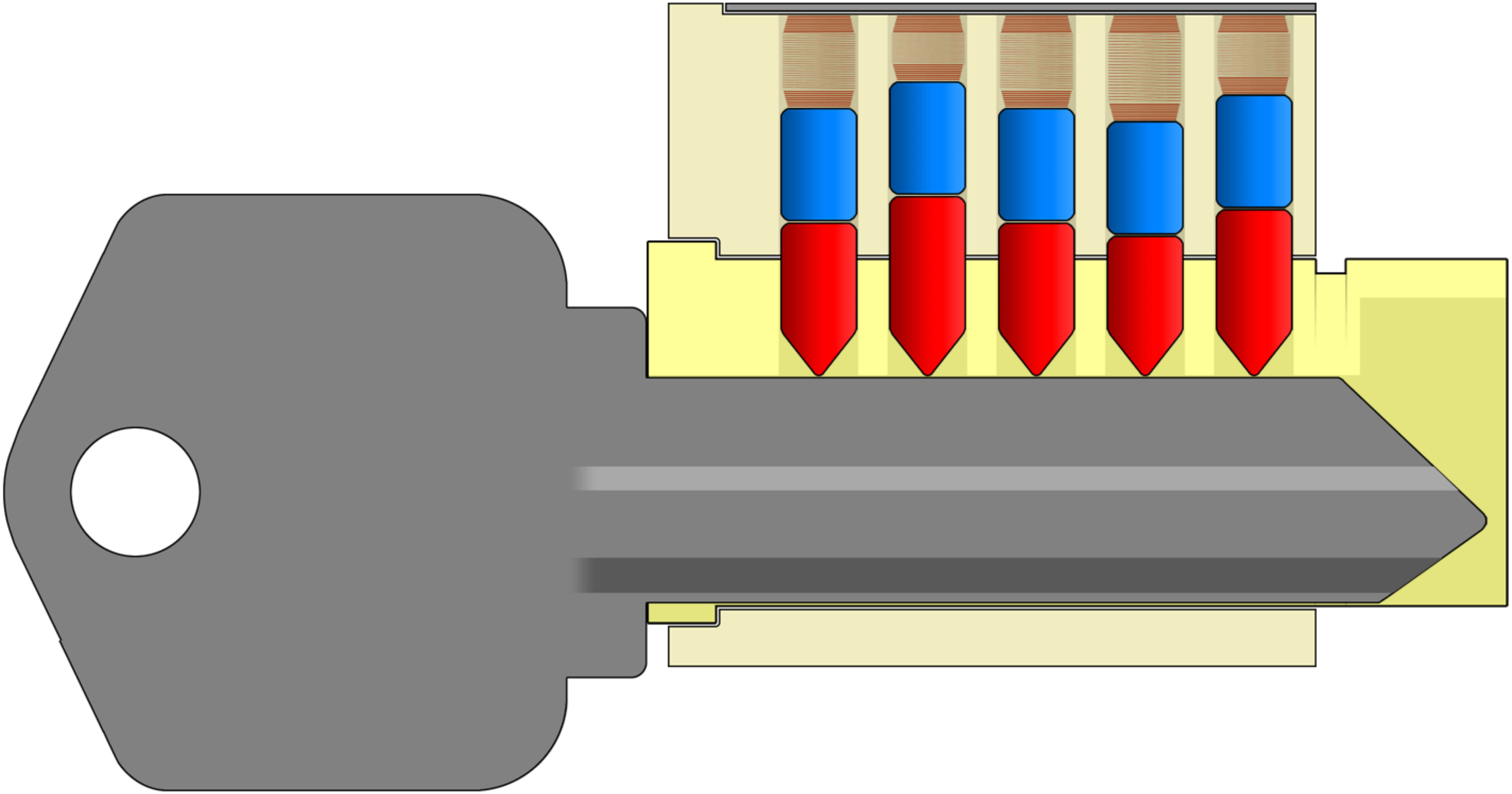
Impressioning – Blank Key to Raise all Stacks



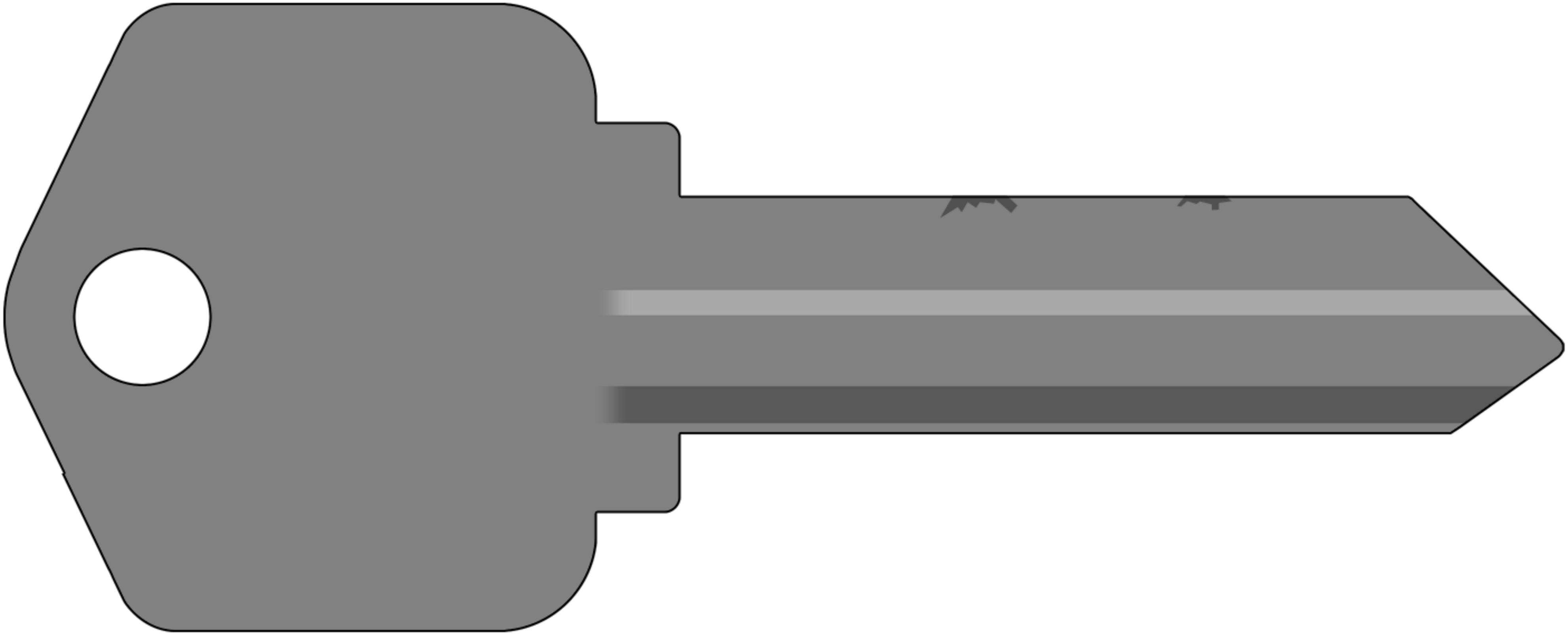
Impressioning – Turn Hard to Bind a Key Pin



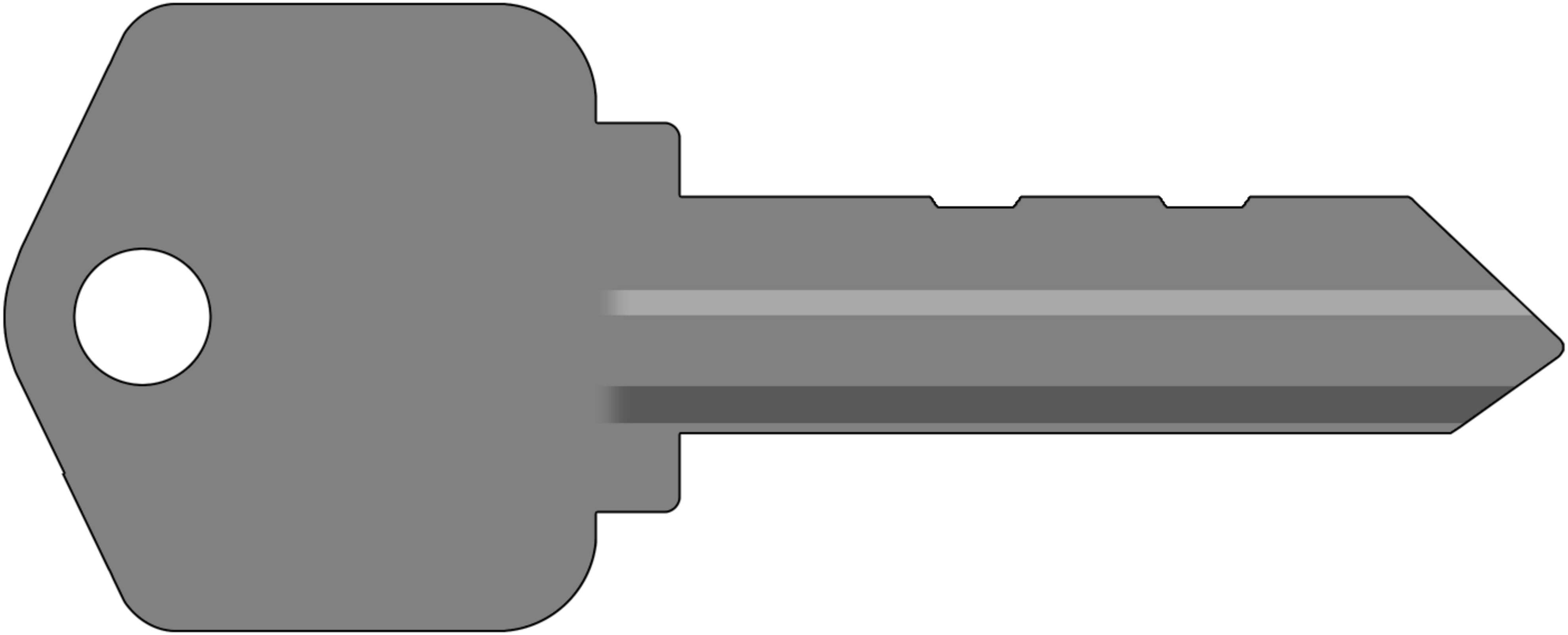
Impressioning – Binding and Wiggling Causes Rubbing



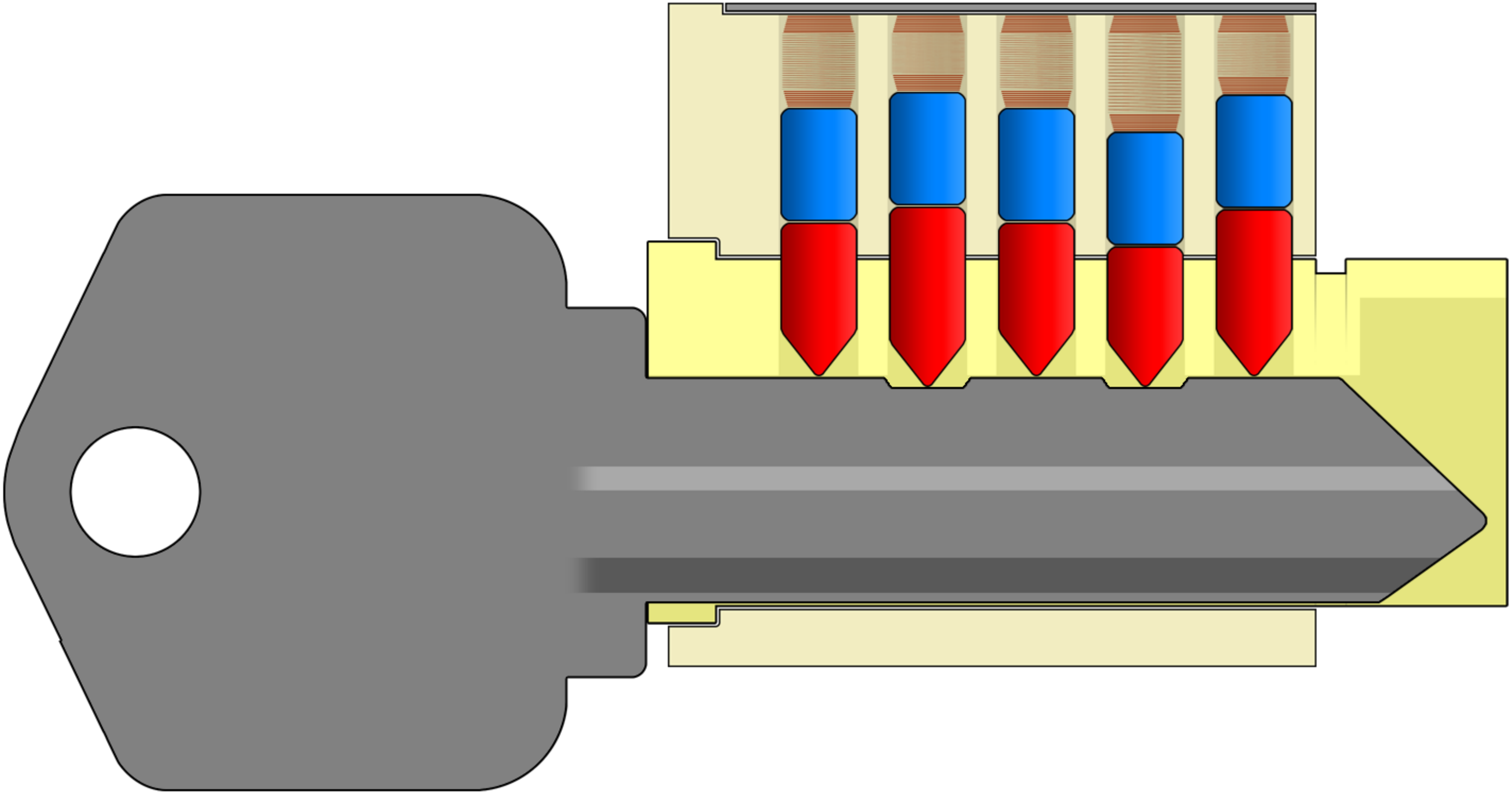
Impressioning – Observe the Rub Marks



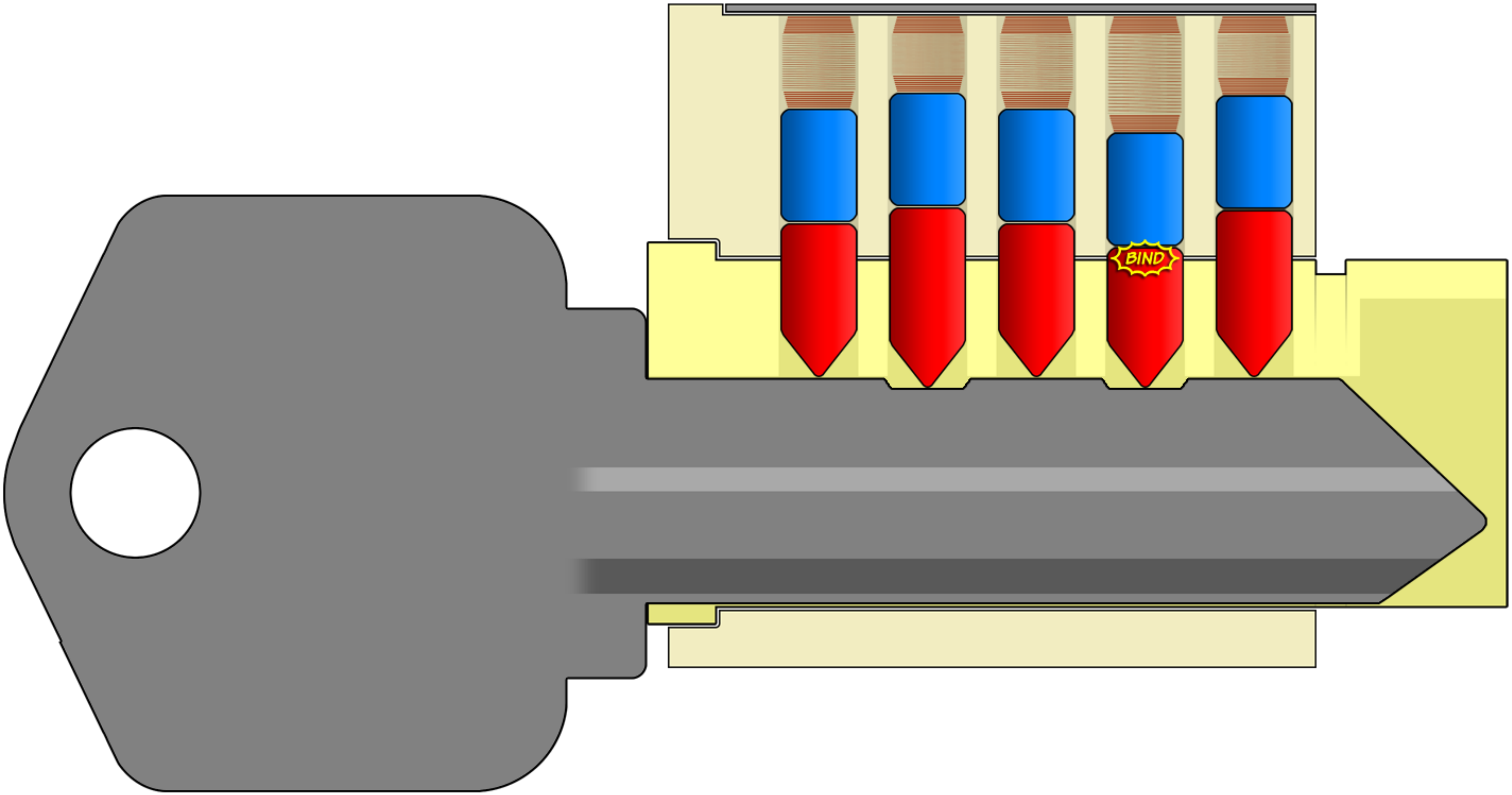
Impressioning – File Down at the Rub Marks



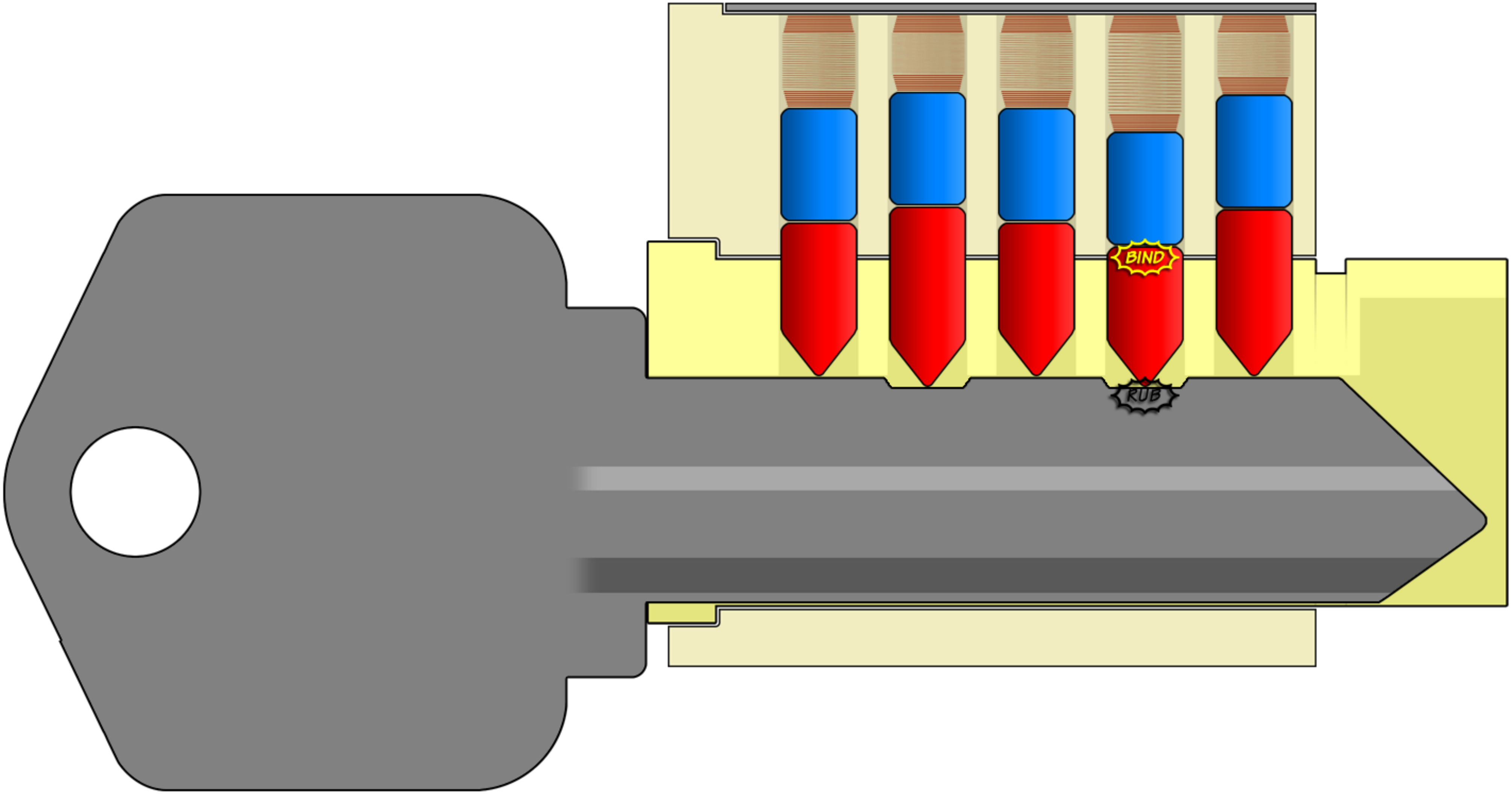
Impressioning – Repeat the Process



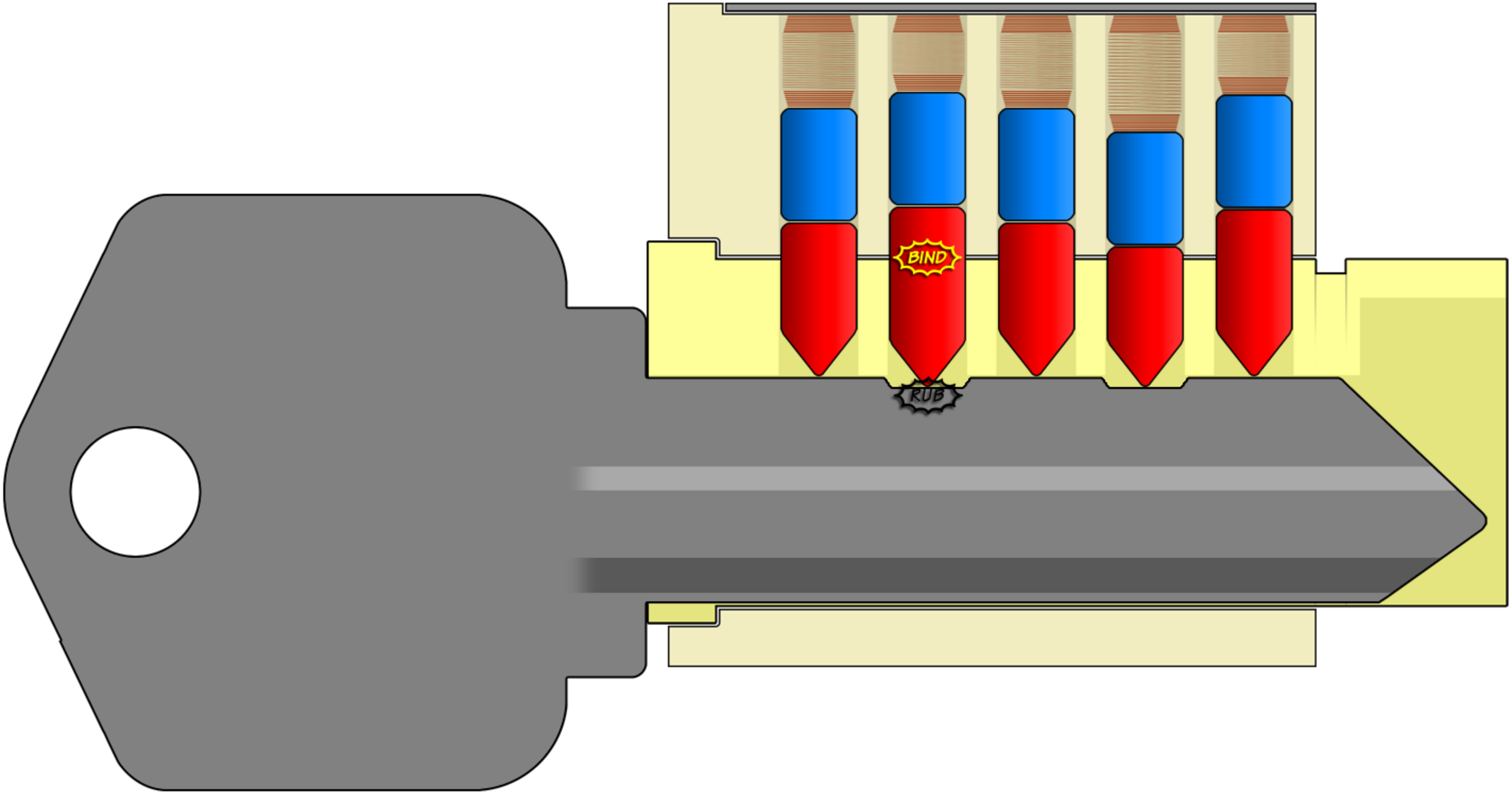
Impressioning – Stack 4 is still Binding



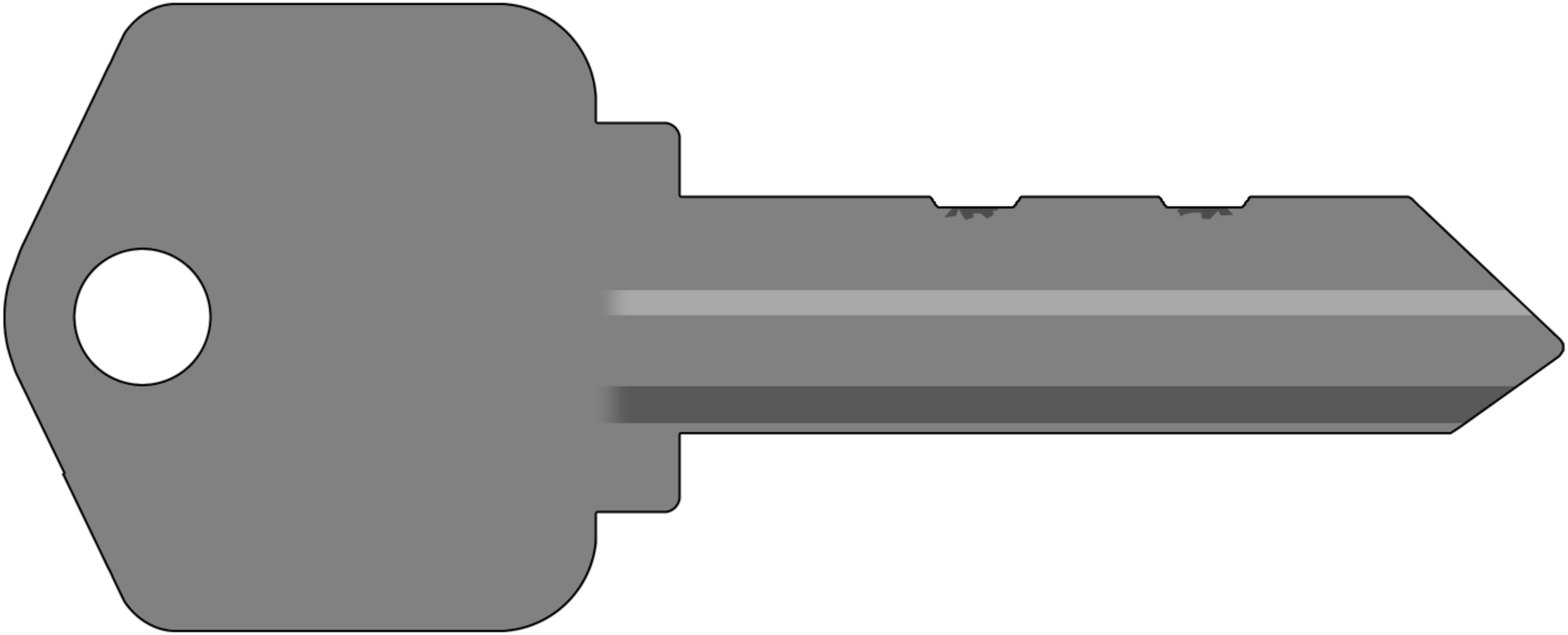
Impressioning – Stack 4 is still Rubbing



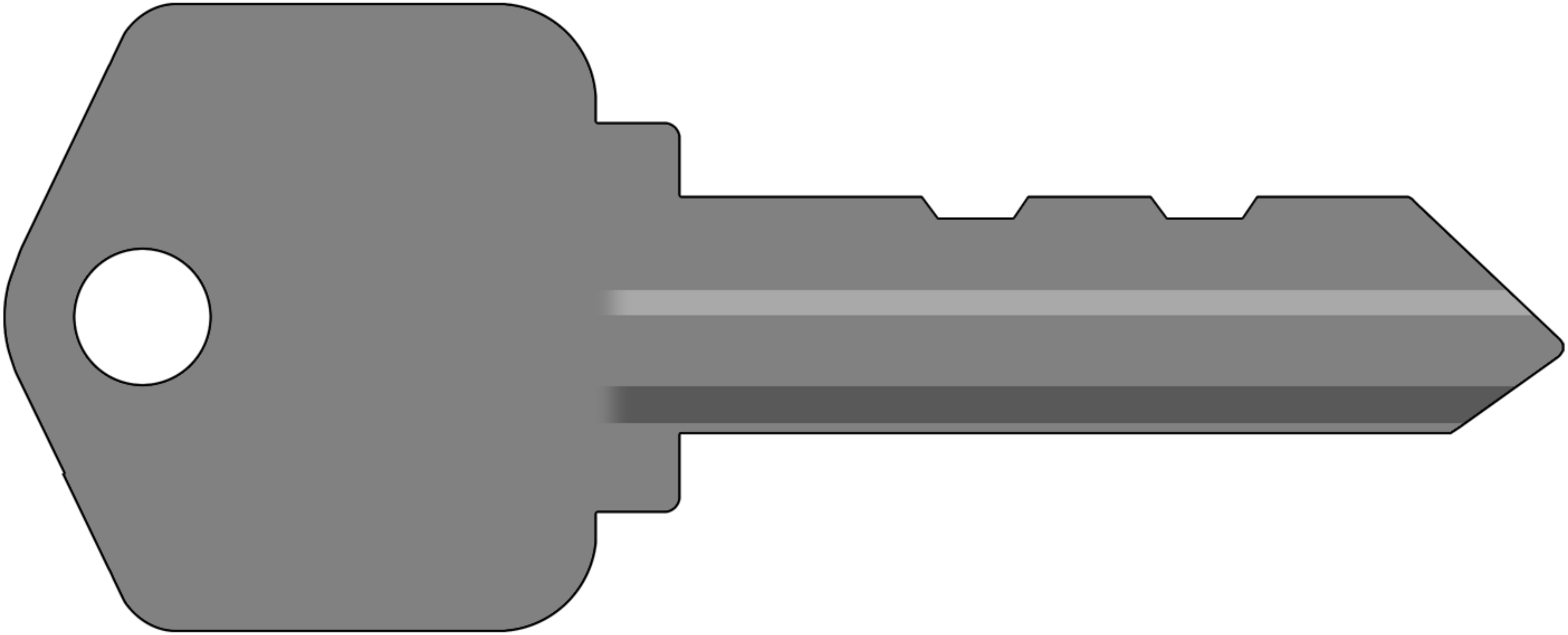
Impressioning – Stack 2 is still Rubbing and Binding



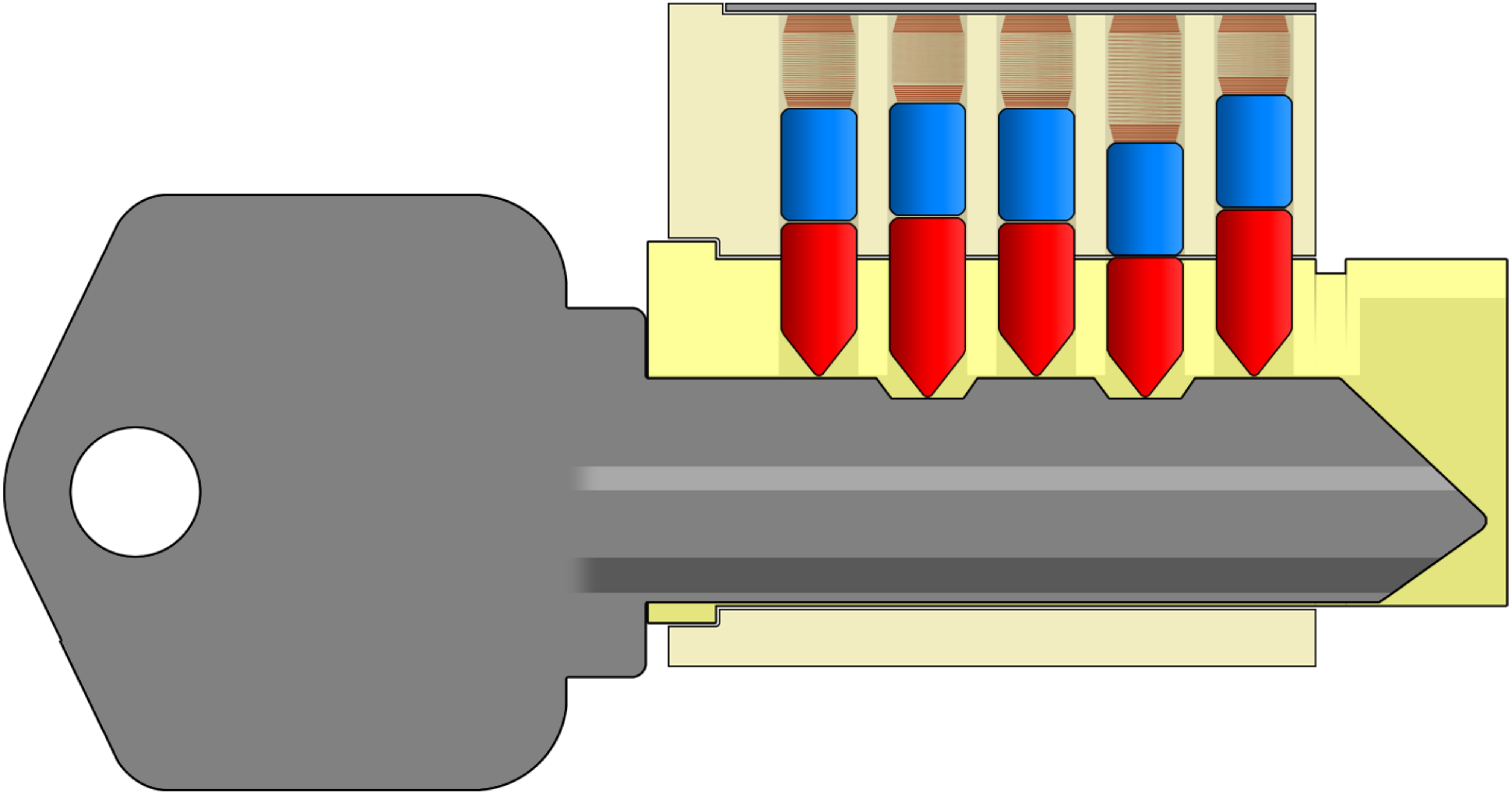
Impressioning – Continued Rub Marks



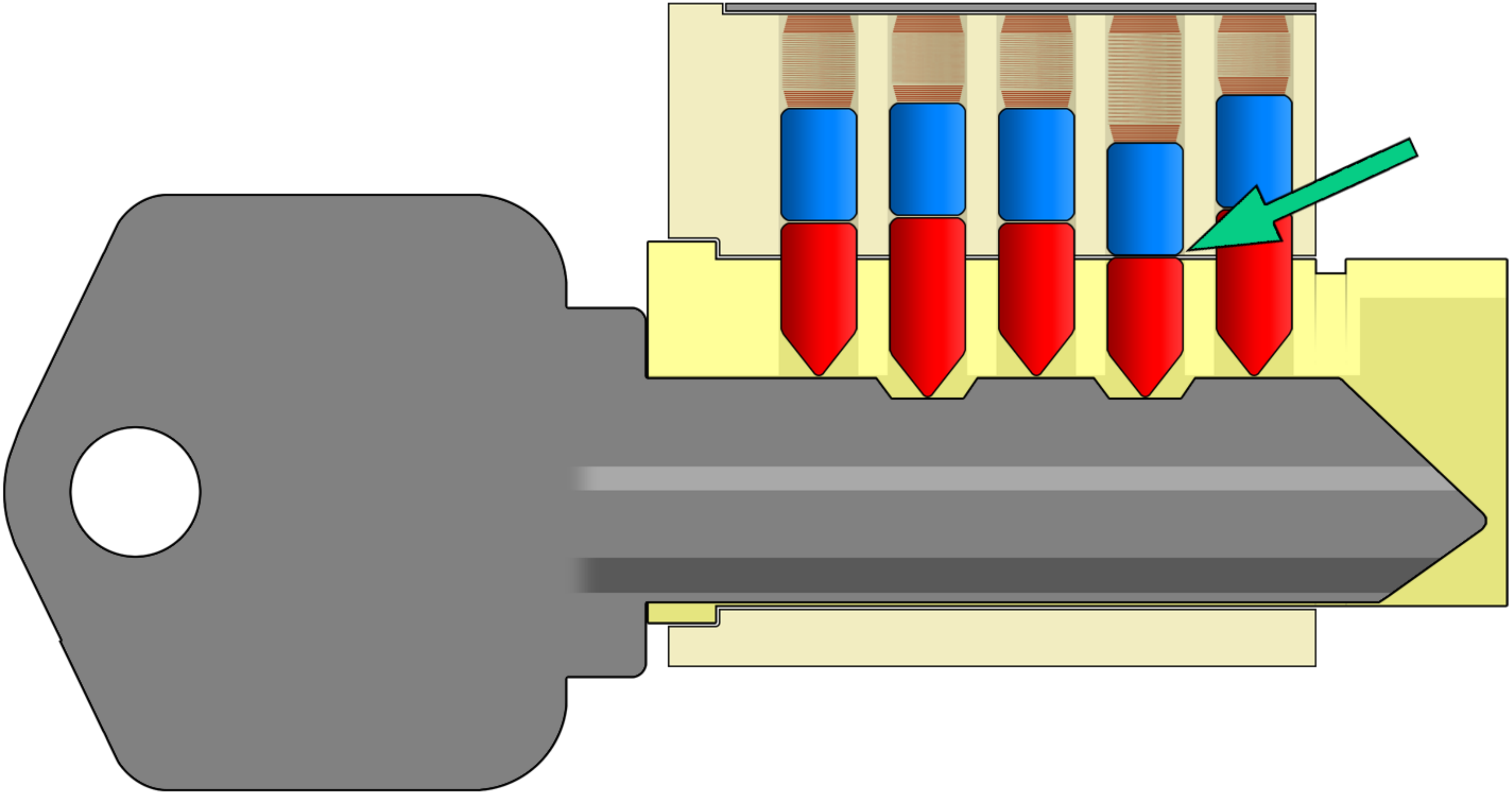
Impressioning – Continued Filing



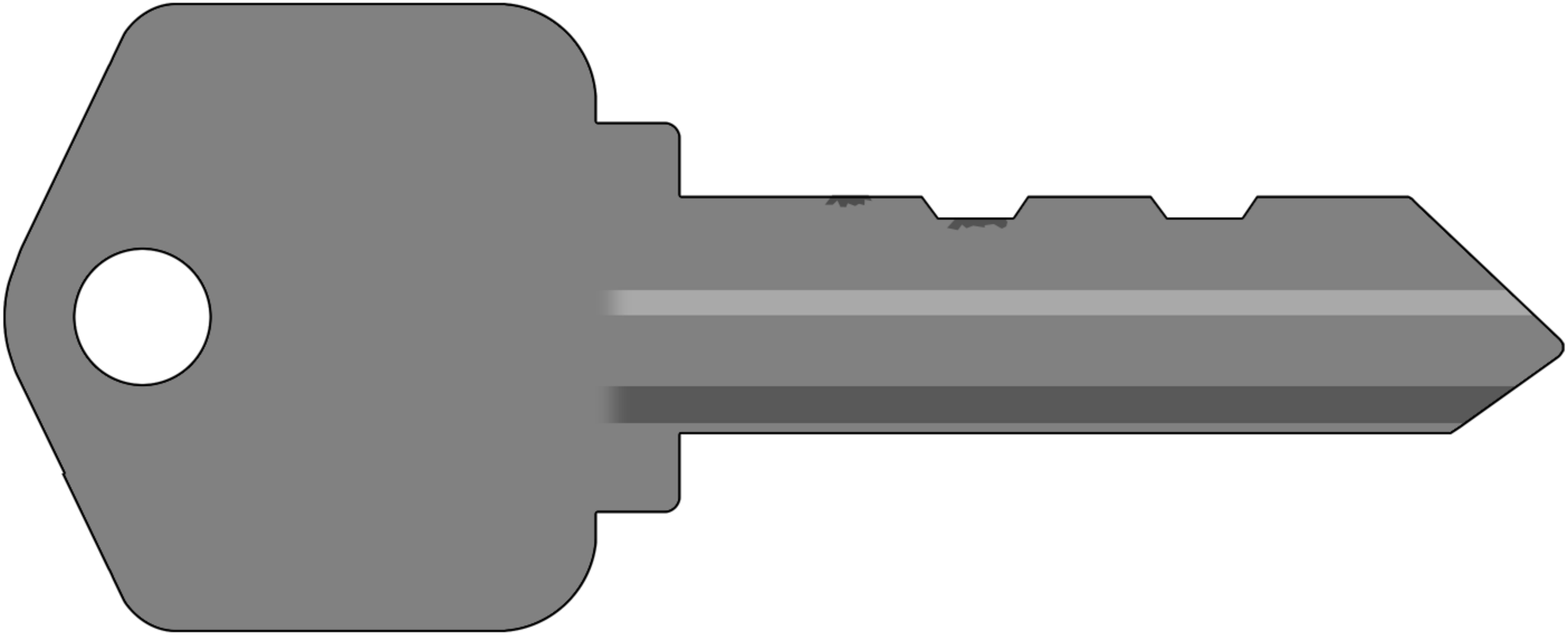
When the Key is Inserted Now...



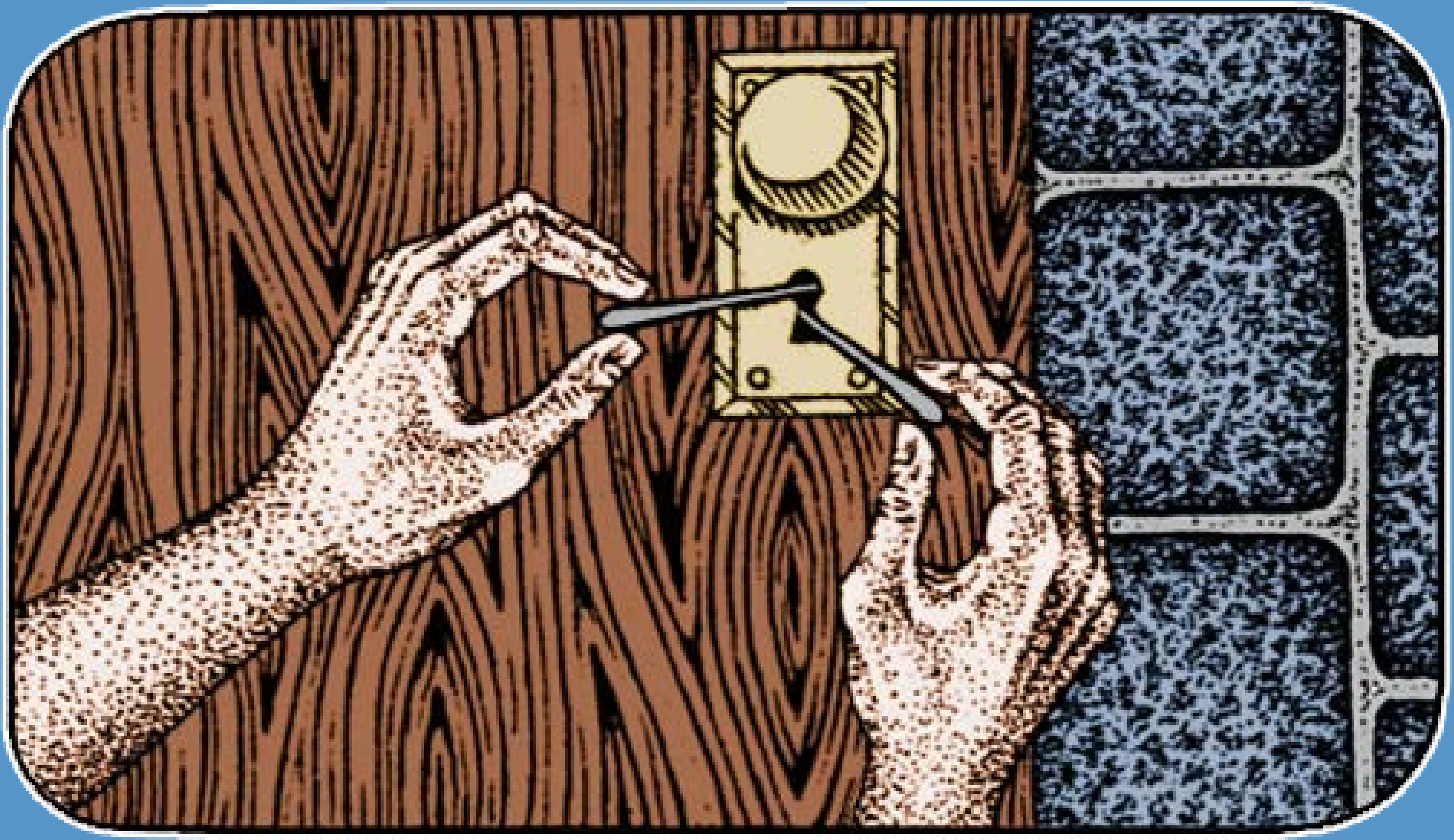
Pin Stack Number 4 is No Longer Binding



You'll Know This Has Happened When *New* Marks Appear



Bypass

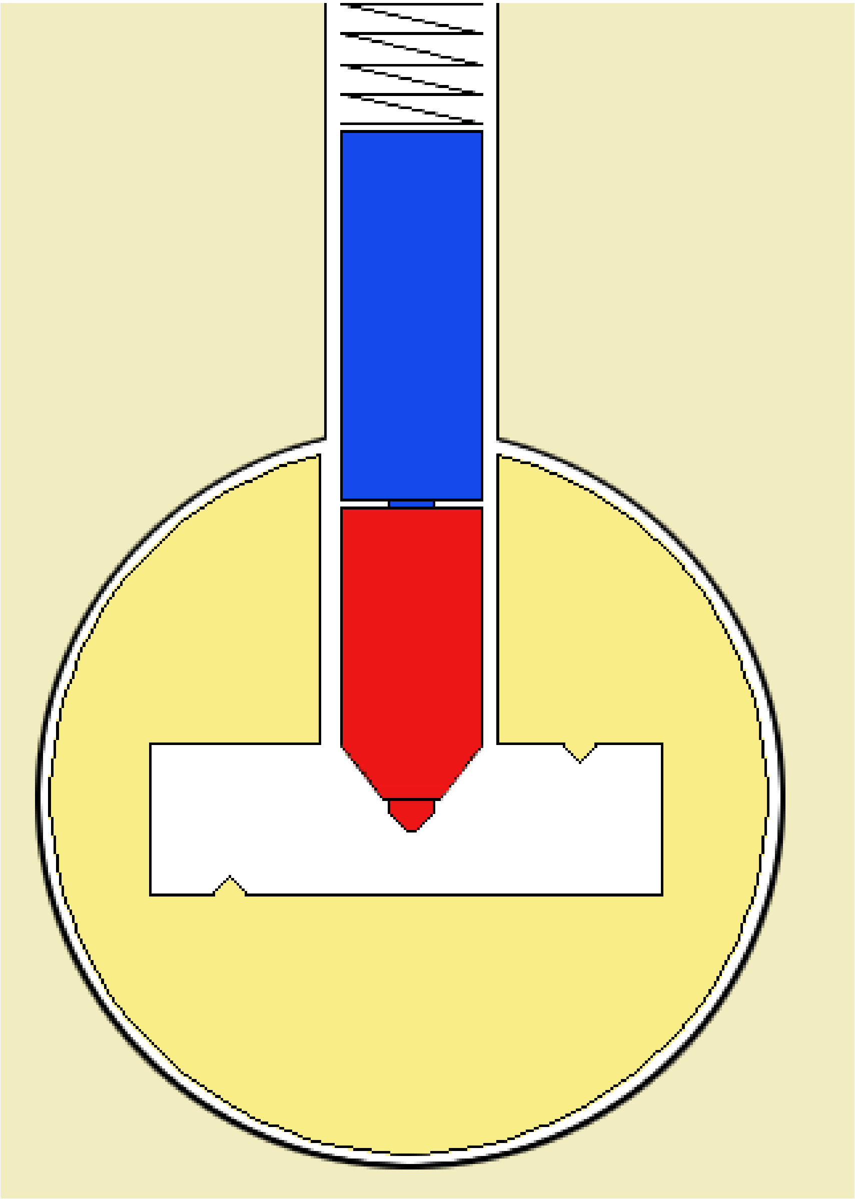


Bypass

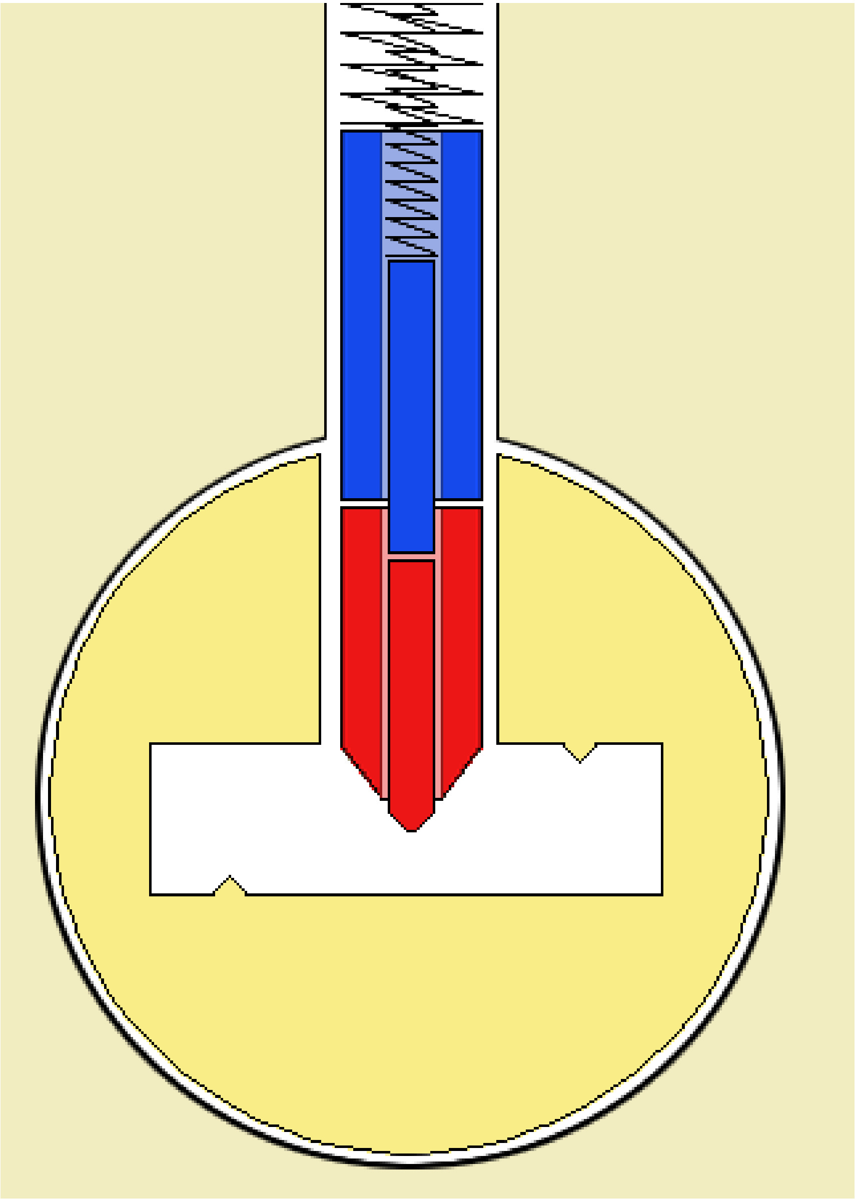
- Locked Door vs. Open Window
- Partial Security Mechanism Bypass
- Improper Installations
- ADA Compliance Woes

Mul-T-Lock Michaud Bypass

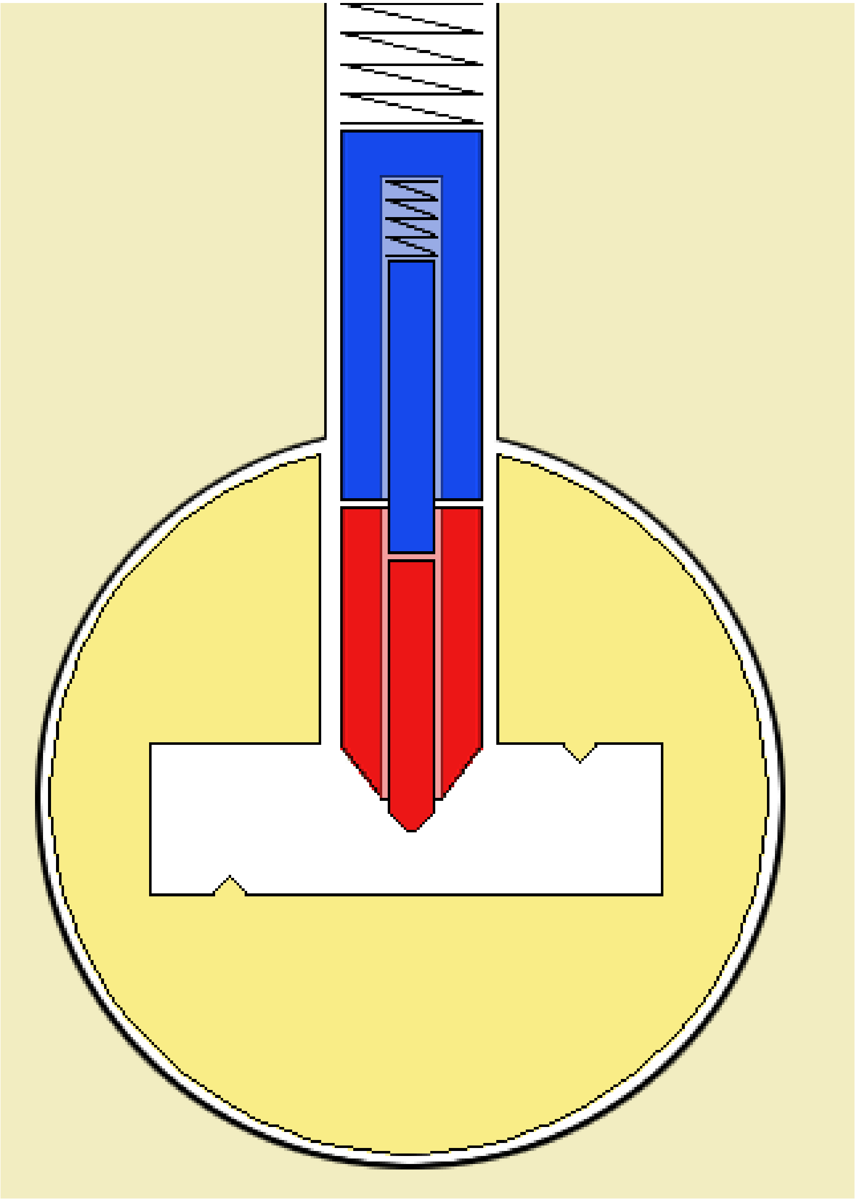
Mul-T-Lock Michaud Bypass



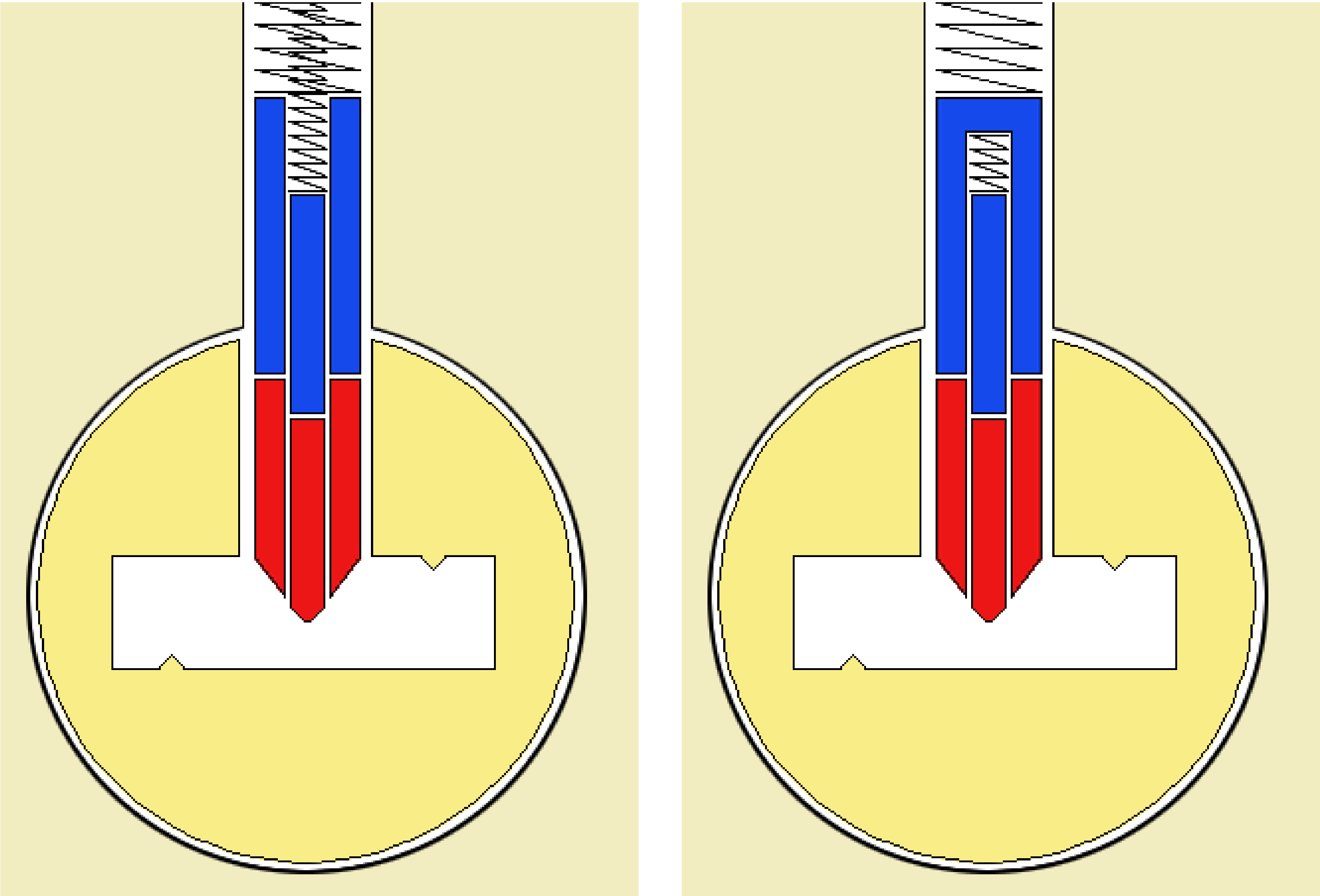
Mul-T-Lock Michaud Bypass



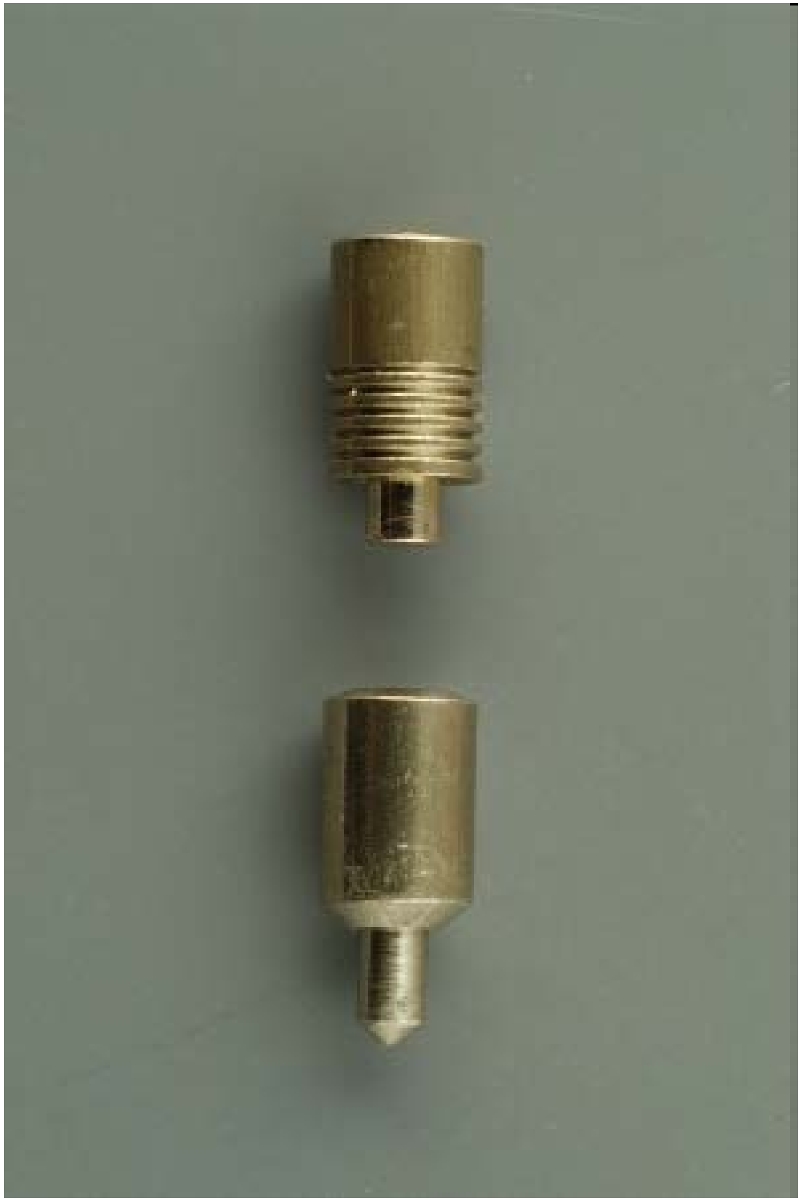
Mul-T-Lock Michaud Bypass

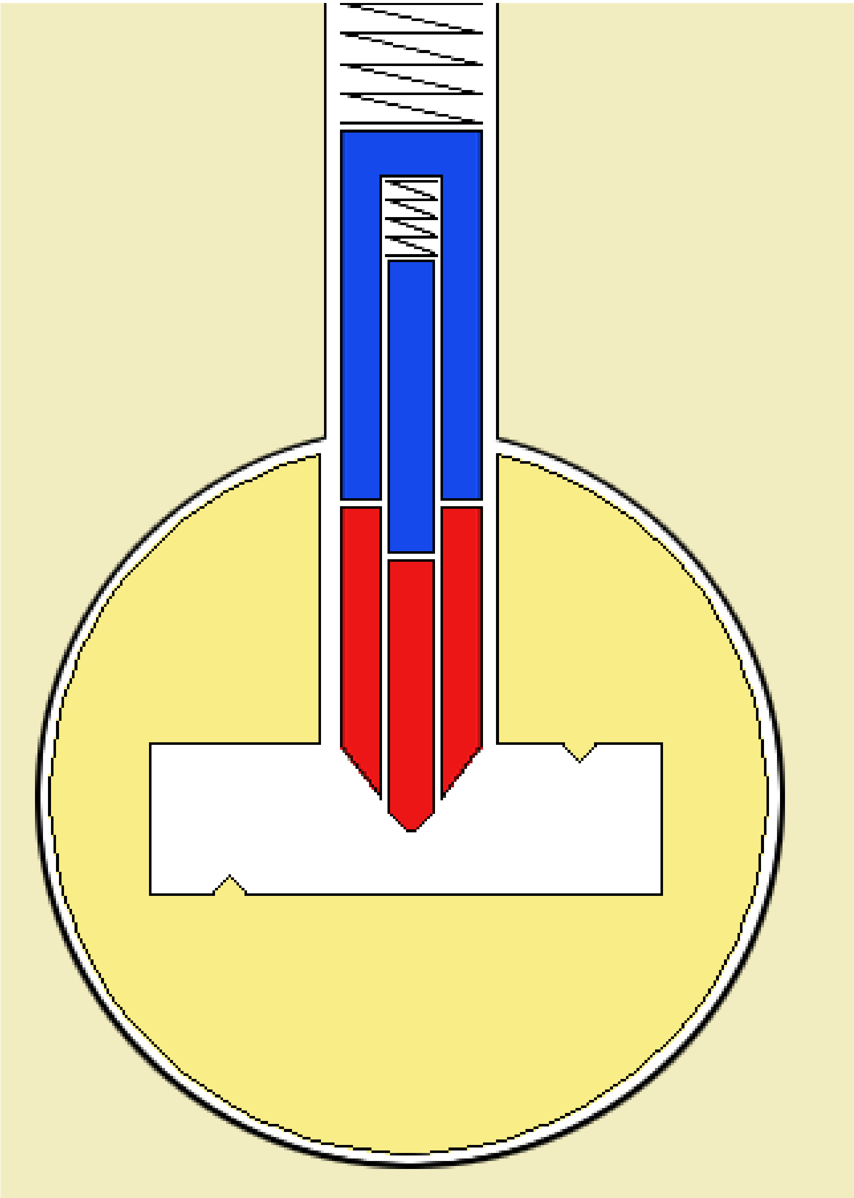


Mul-T-Lock Michaud Bypass

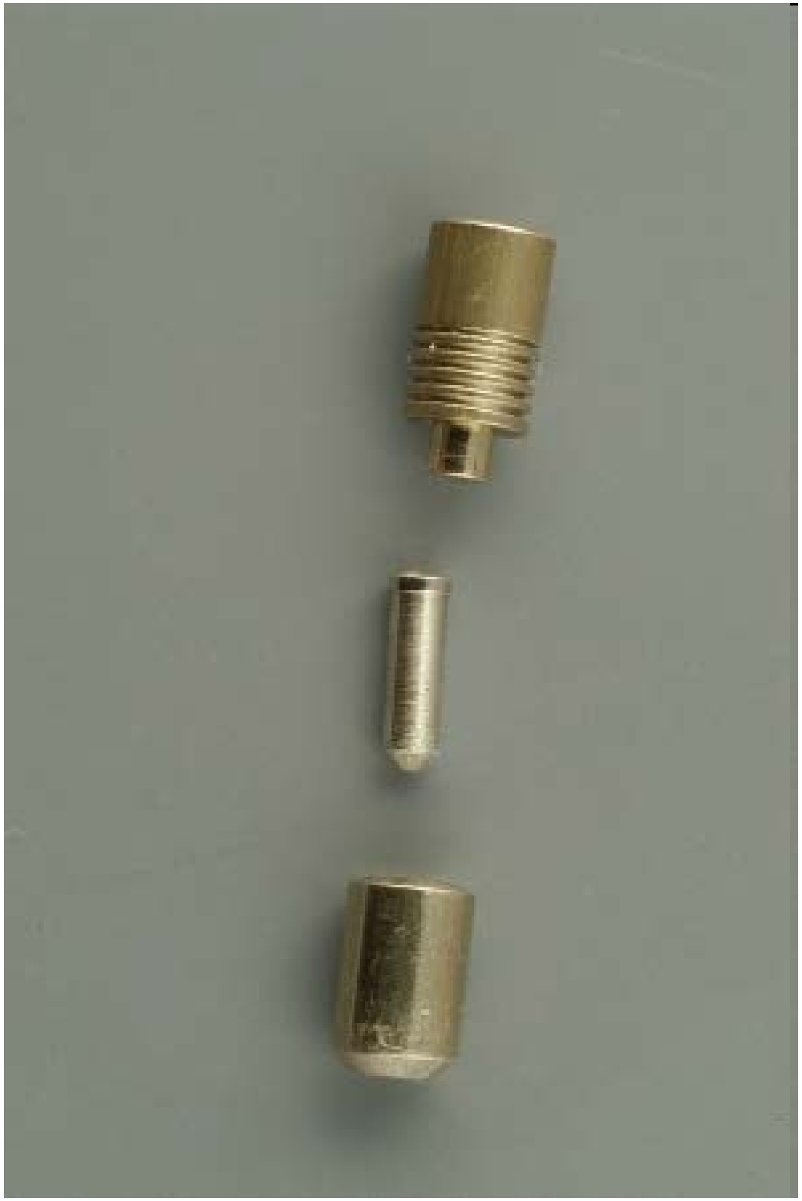


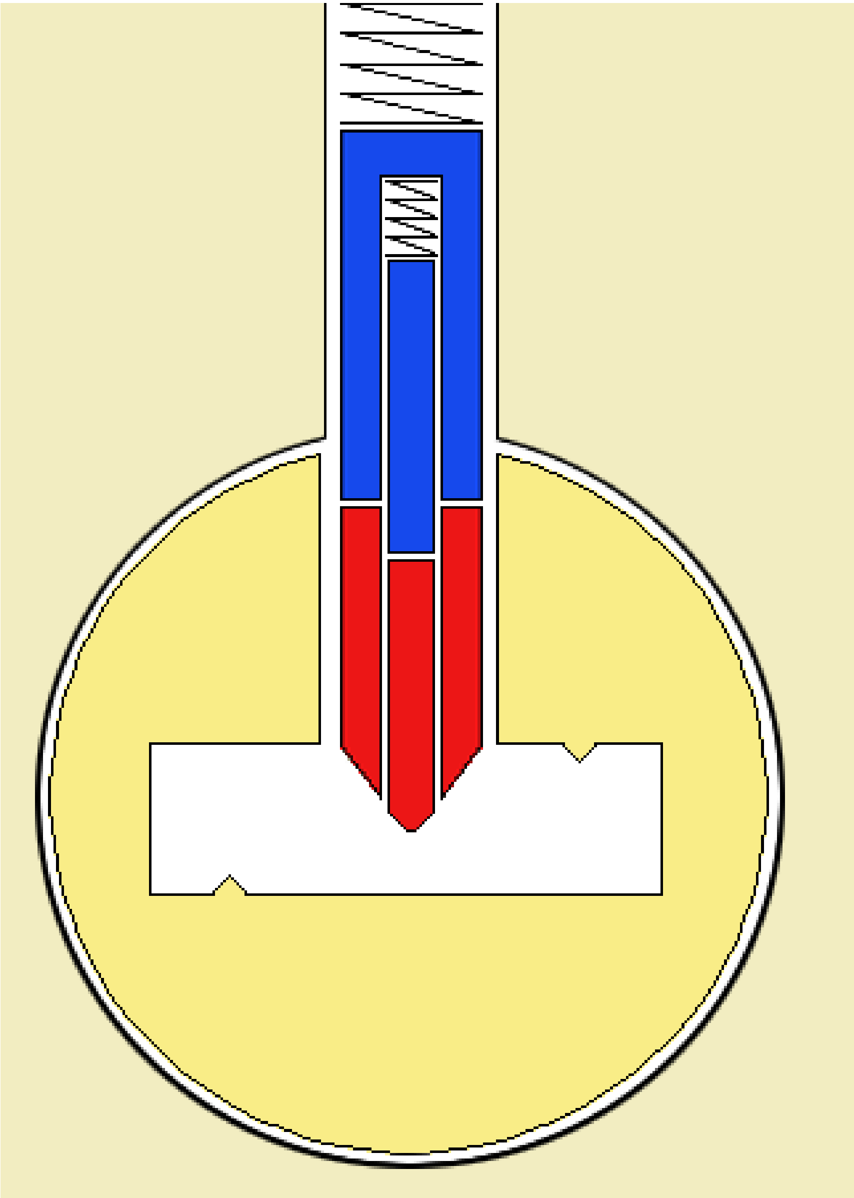
Mul-T-Lock Michaud Bypass



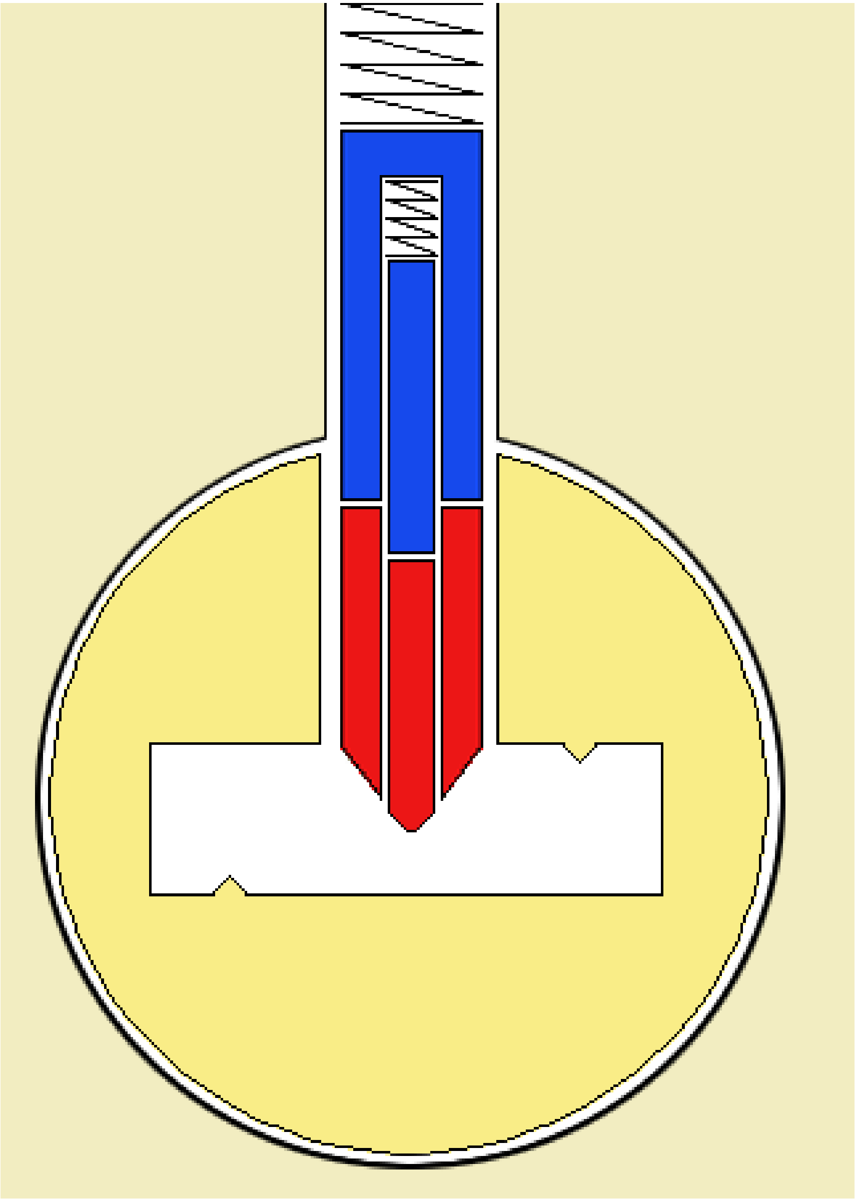


Mul-T-Lock Michaud Bypass

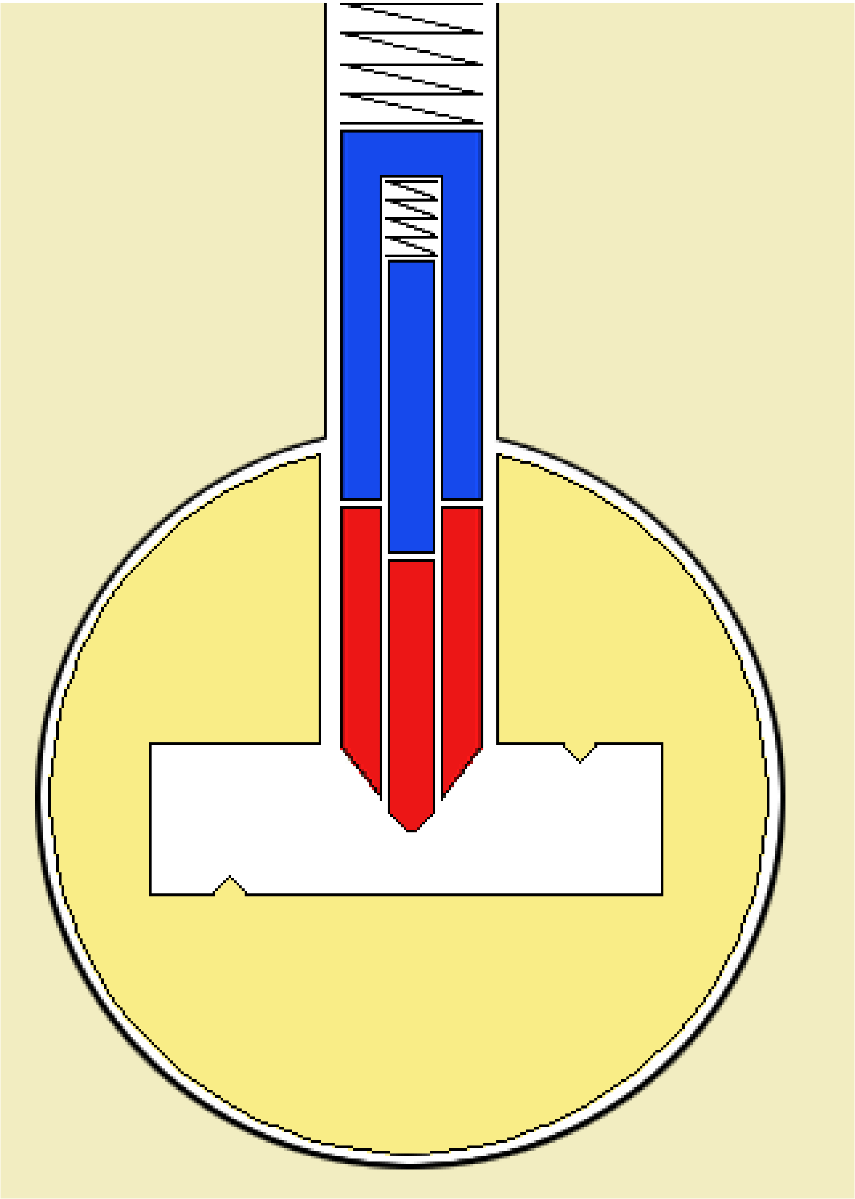




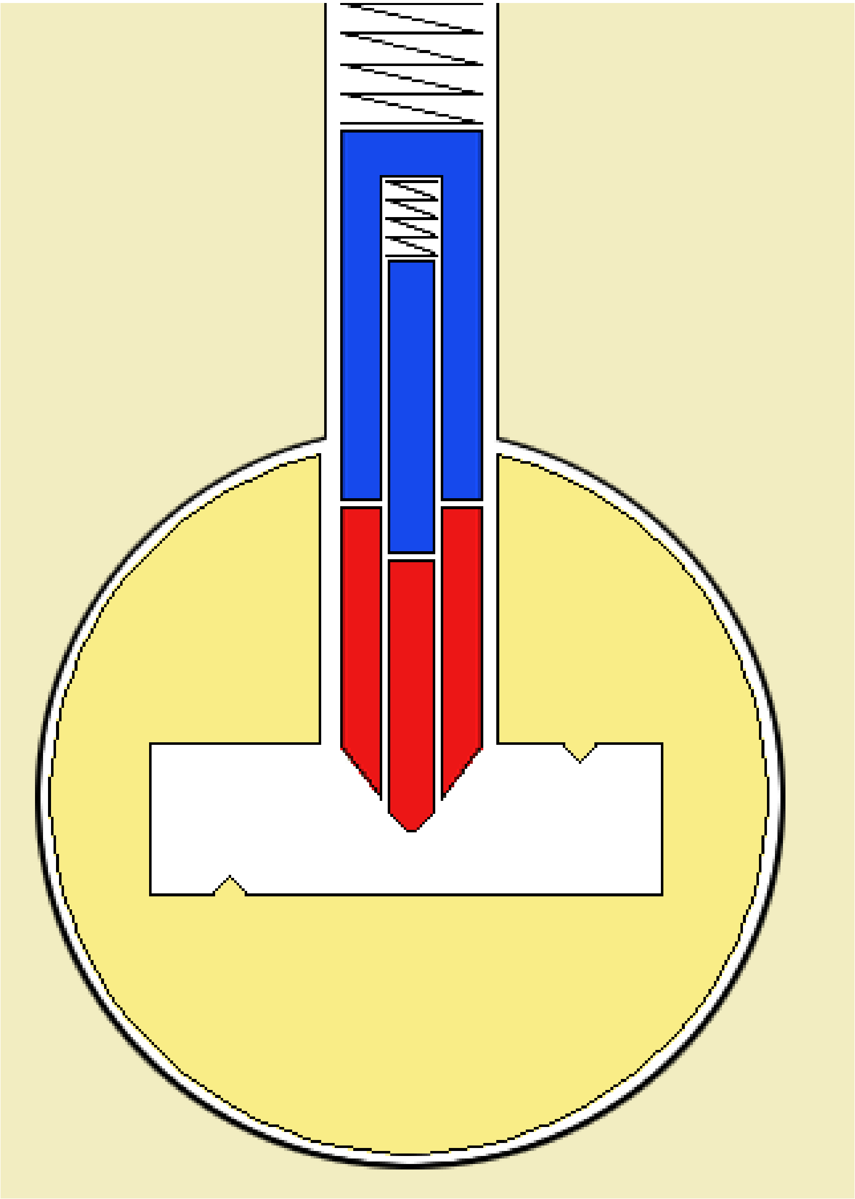
Mul-T-Lock Michaud Bypass



Mul-T-Lock Michaud Bypass



Mul-T-Lock Michaud Bypass



CodeLocks CL5000 Design Flaw

Codelocks

Weaponizing an exploit

- What do you do when a flaw is found?
- Establish Repeatability
- Make the Exploit Execution Efficient
- Potential to combine tools to decrease the toolkit footprint

Documentation and Reporting

- Why?
- Legitimacy
- Delivery to manufacturers
- Delivery to clients
- Information reuse in other projects
- Publishing any research

Review/Questions

Babak Javadi
alpha@enterthecore.net

Shane Lawson
slawson@tenacitysolutions.net

Thanks To:

Deviant Ollam, Datagram, Eric Michaud, Marc Tobias, TOOOL, FOOLS, and anyone we forgot to mention!