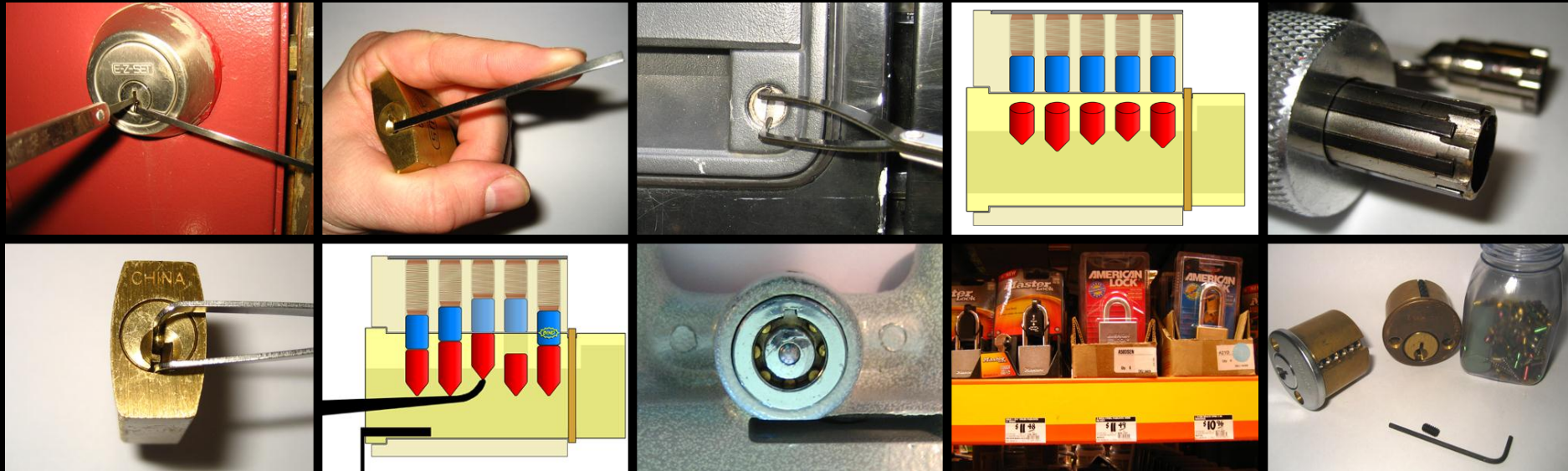


New

Ten Things You Should Know About Lockpicking

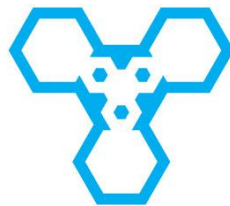


by Deviant Ollam and Babak Javadi
CONFidence 2011 - Krakow
2011-05-24

Who are we ?



Who are we ?



**THE
CORE
GROUP**

auditing
assessments
research
trainings

Who am i ?



**THE
CORE
GROUP**

auditing
assessments
research
trainings



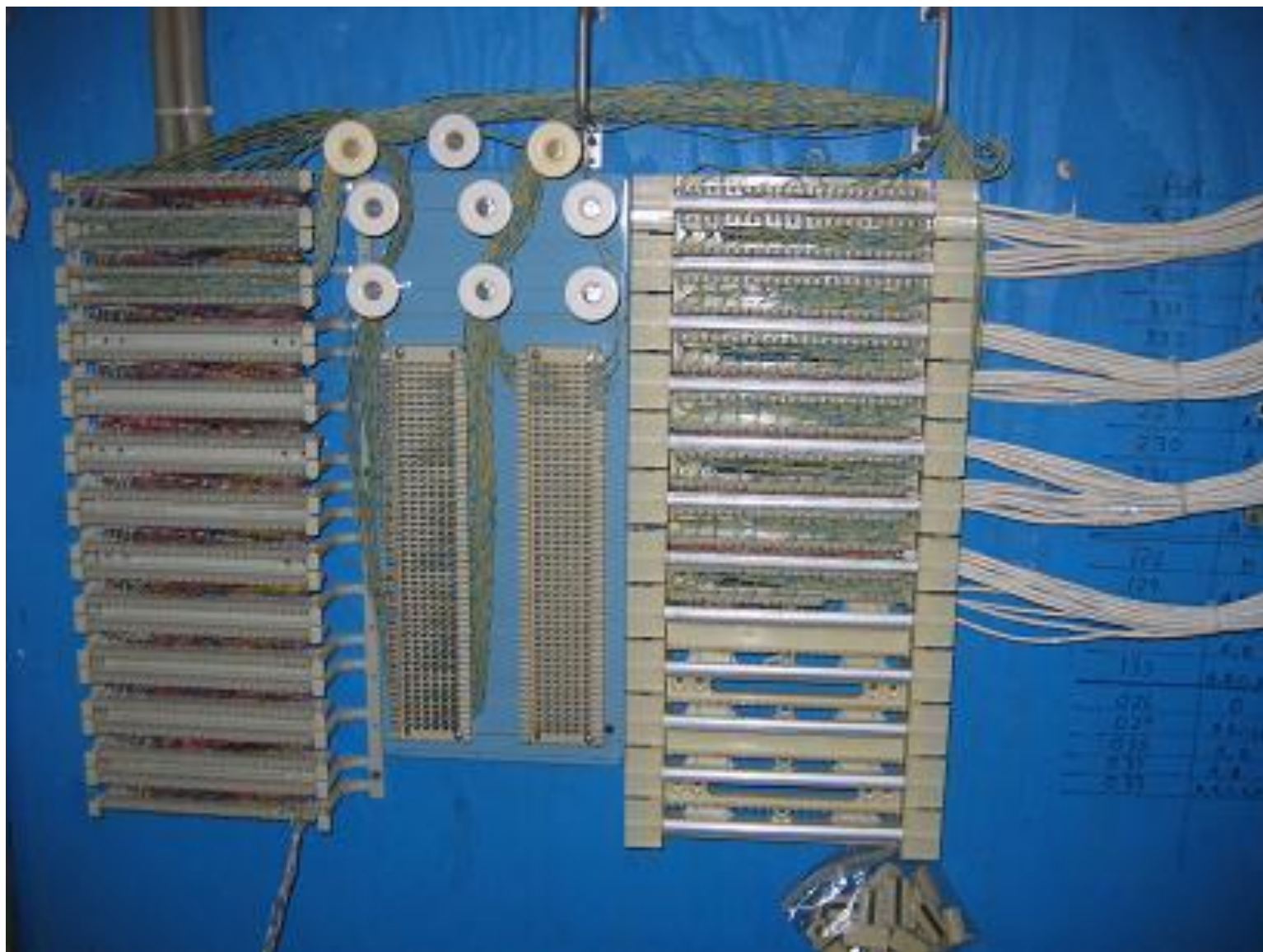
workshops
public lectures
lockpick village
contests & games

Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals









All your hard work here...



All your hard work here... gets undermined here



Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
- 2. Pin tumblers are universal**

Pin Tumbler Locks



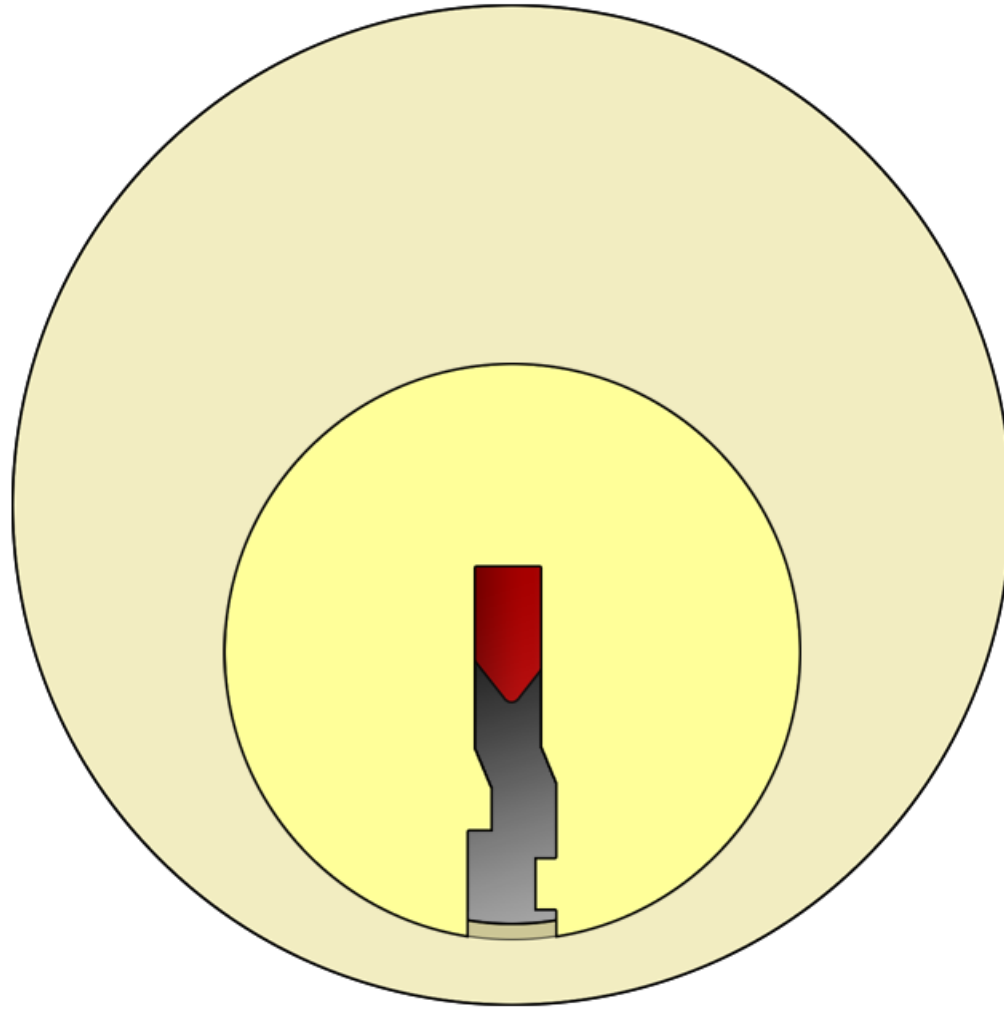
Pin Tumbler Locks



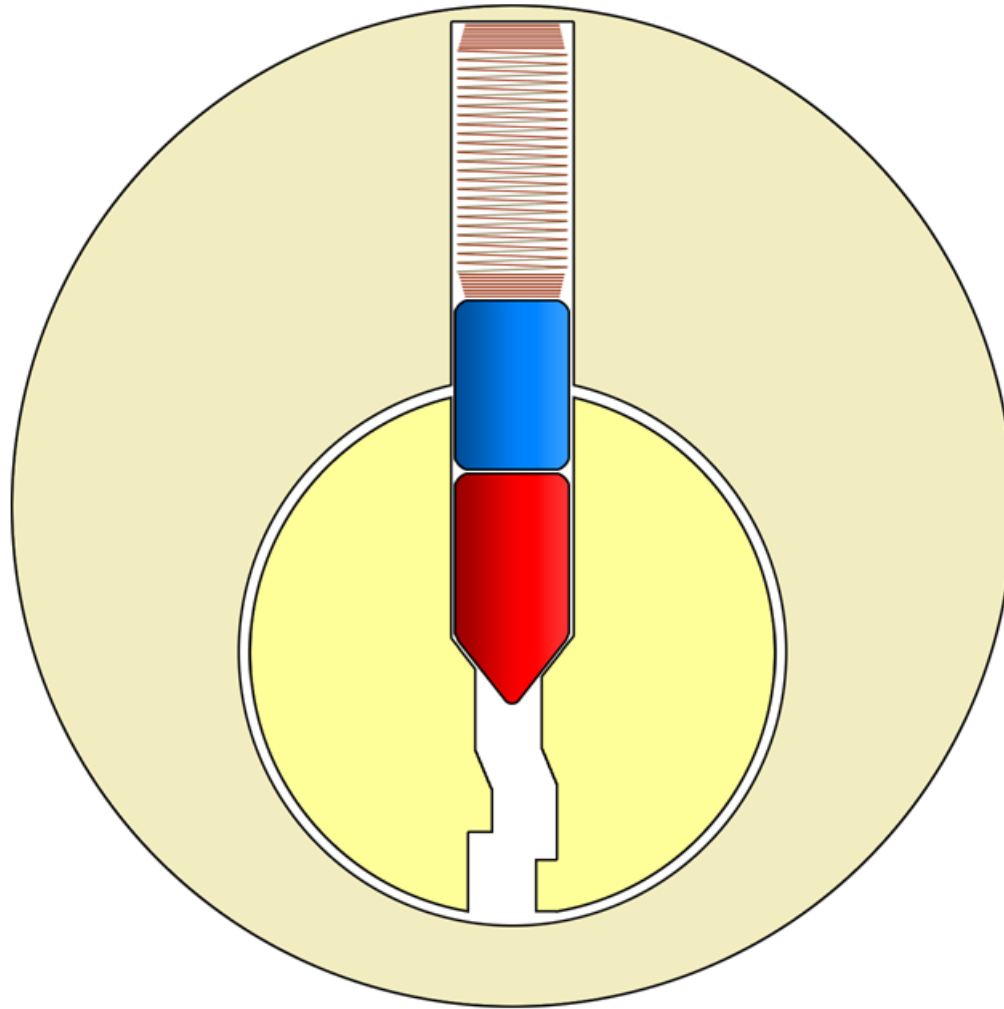
Pin Tumbler Locks



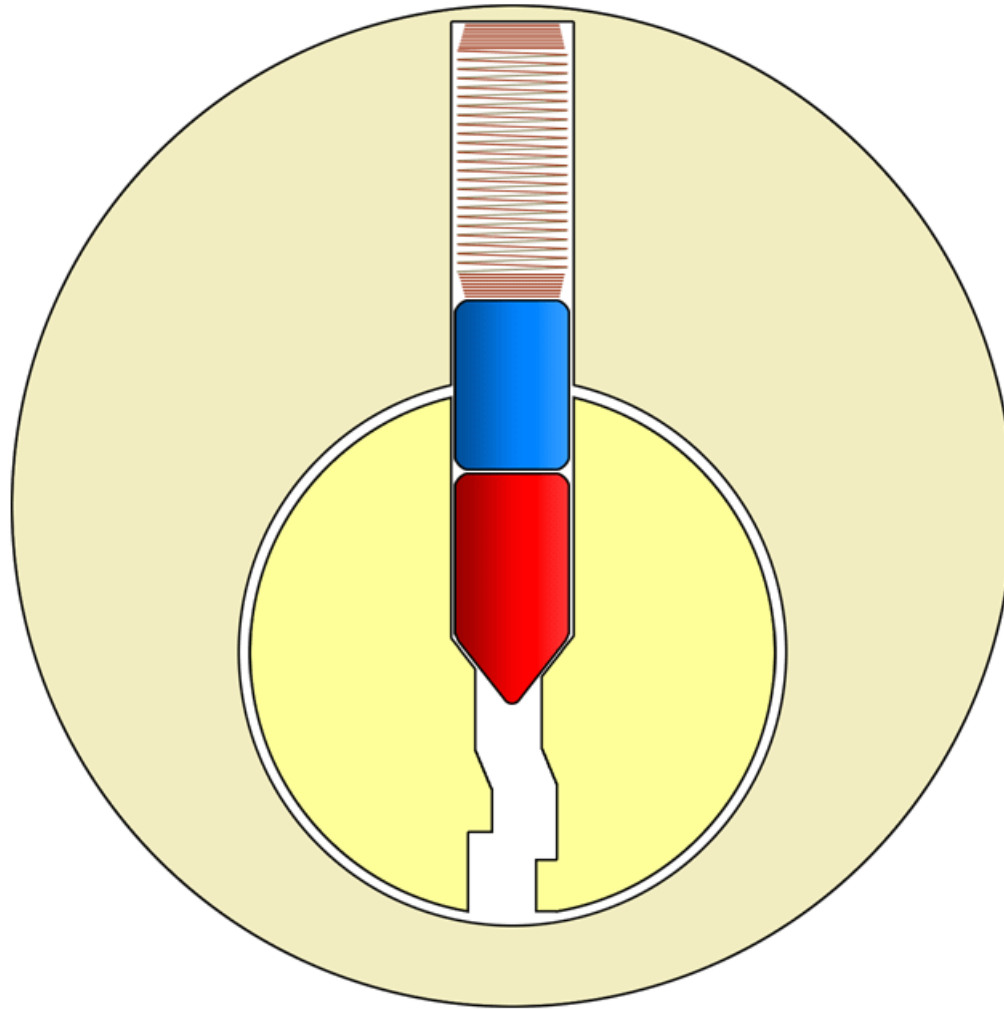
The View From Outside



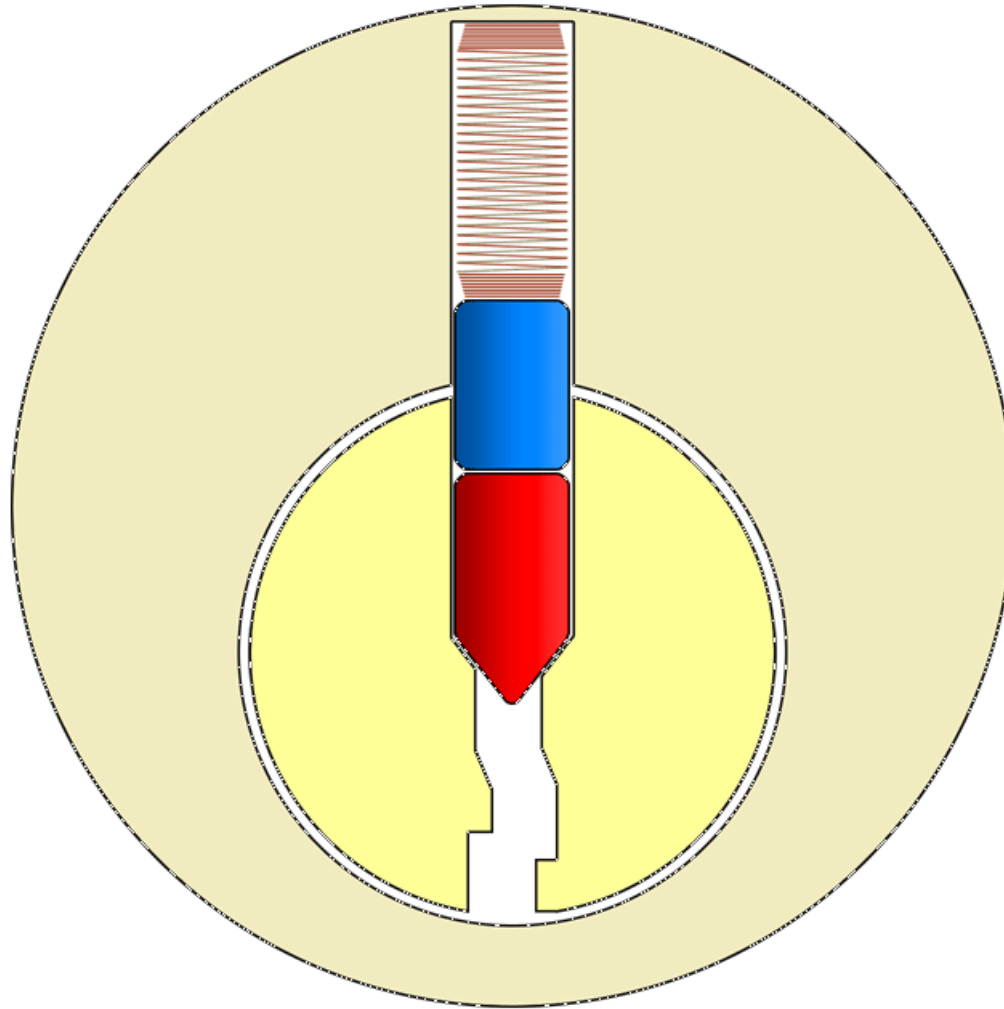
What's On The Inside



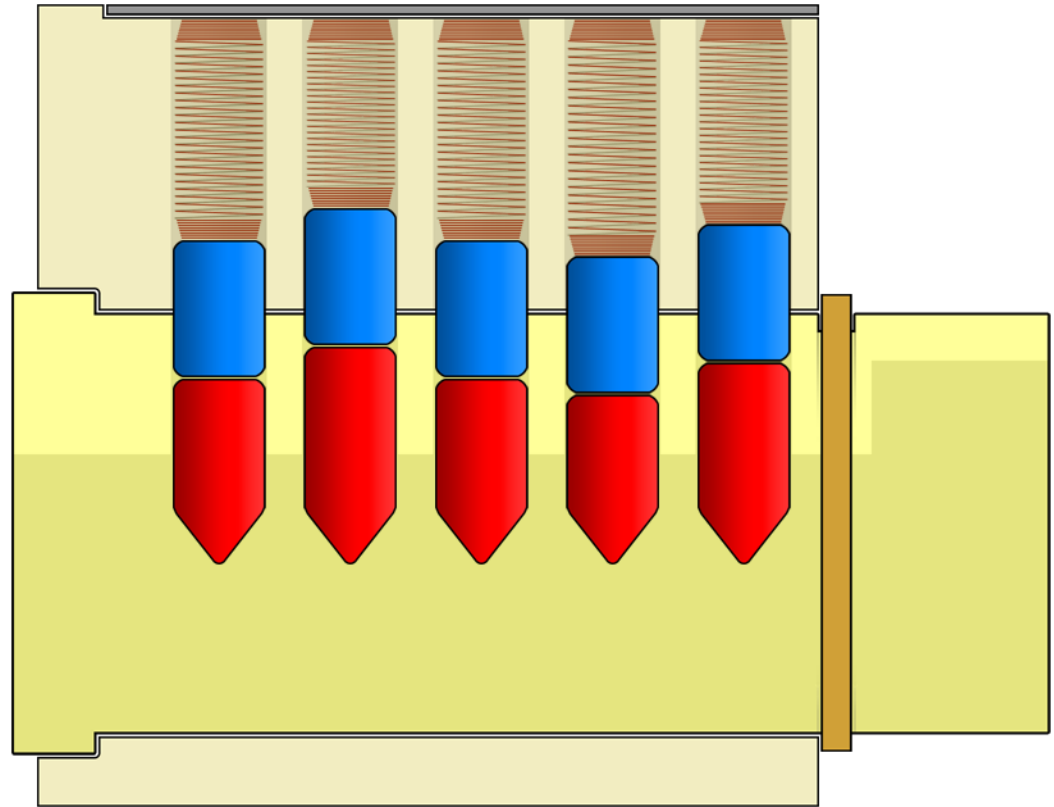
What's On The Inside



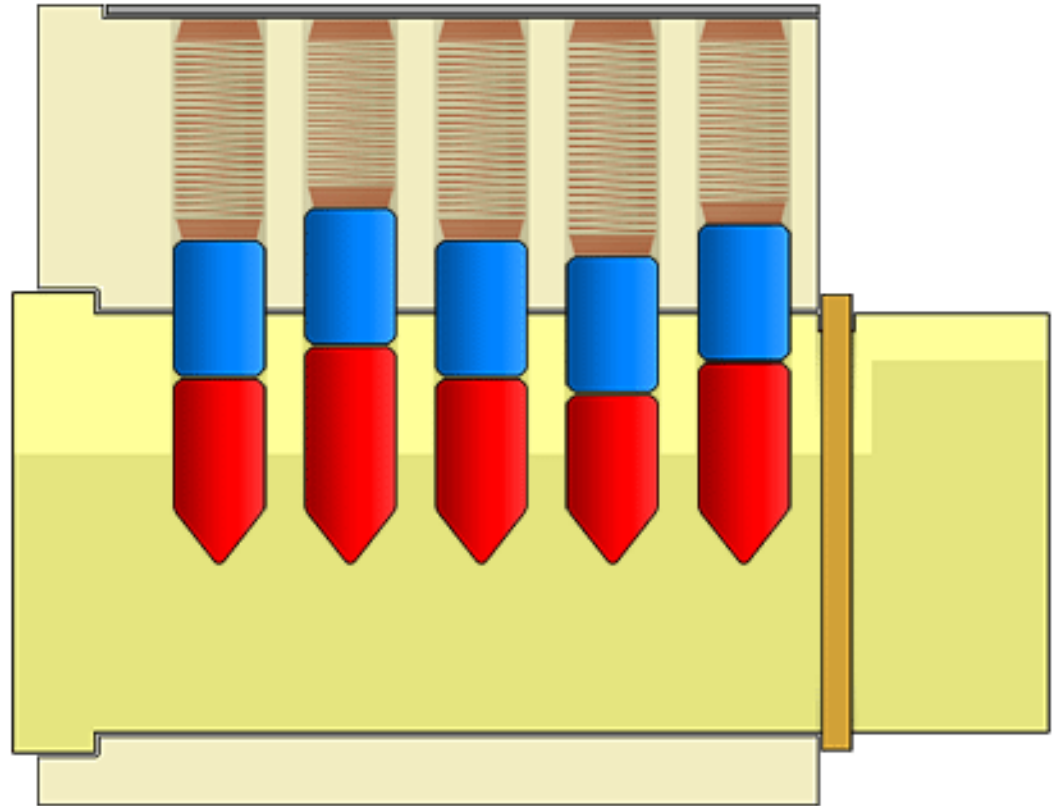
What's On The Inside



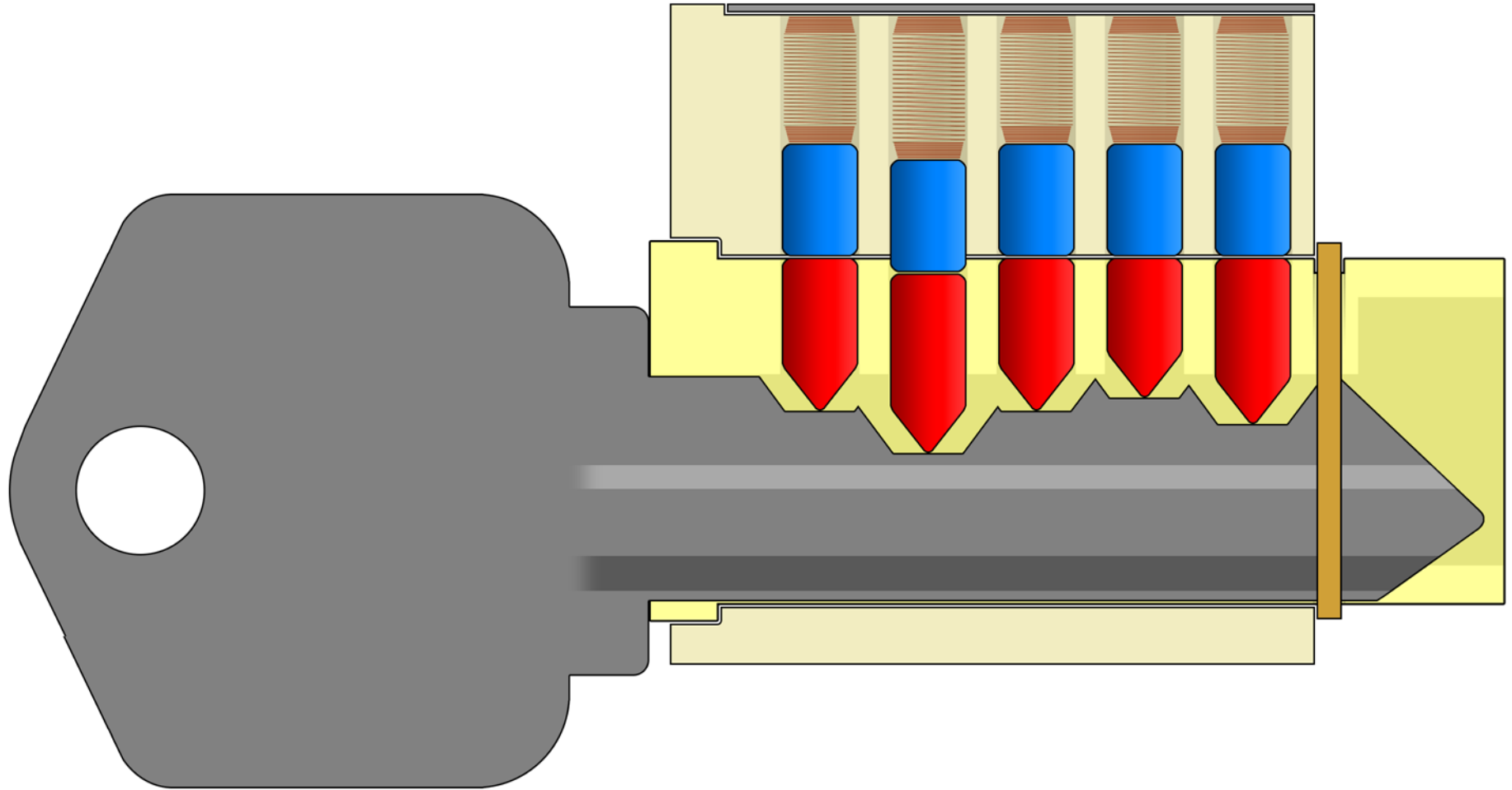
It's Not Just a Single Pin Stack



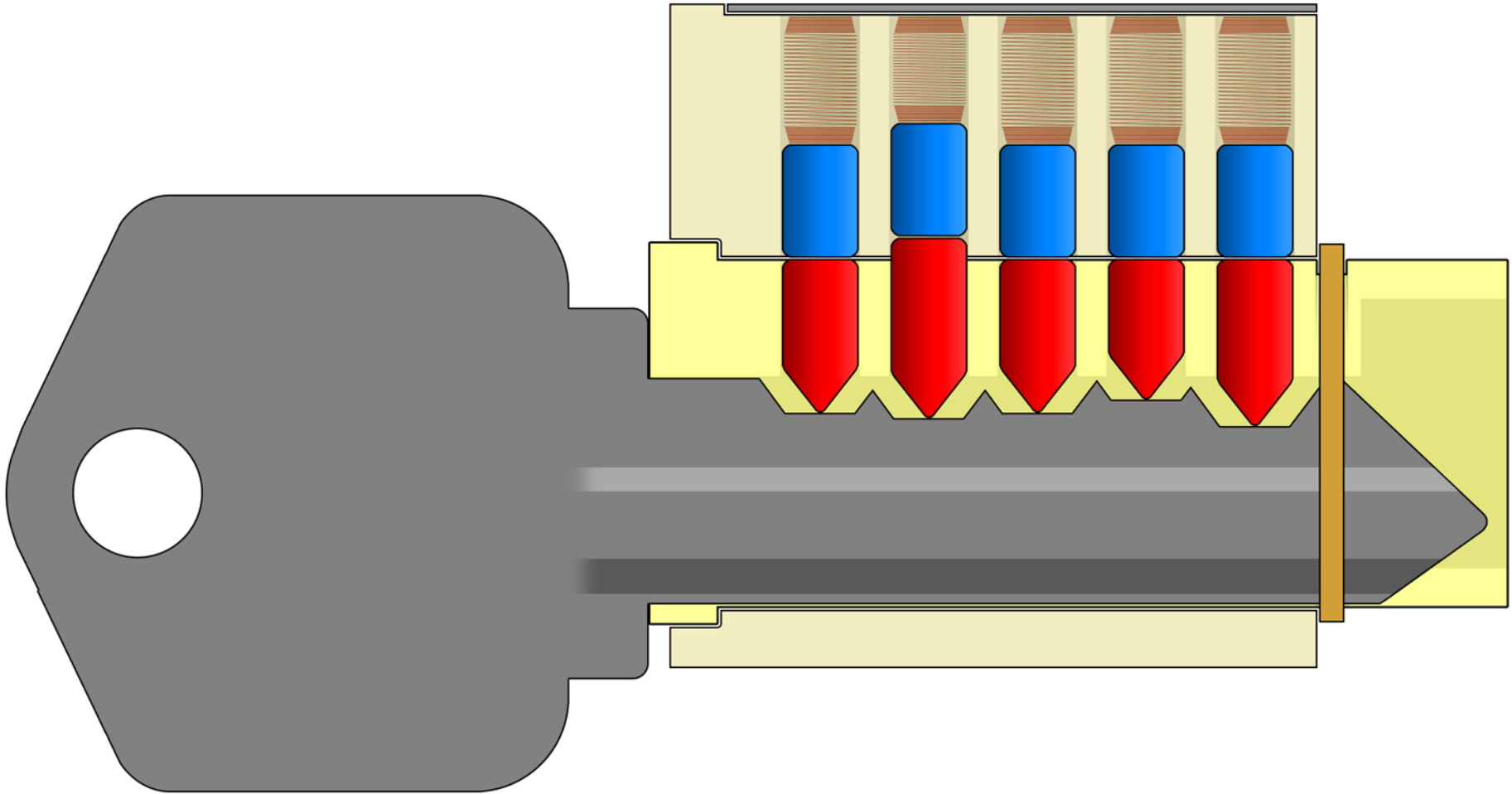
It's Not Just a Single Pin Stack



The Key Has To Be Just Right



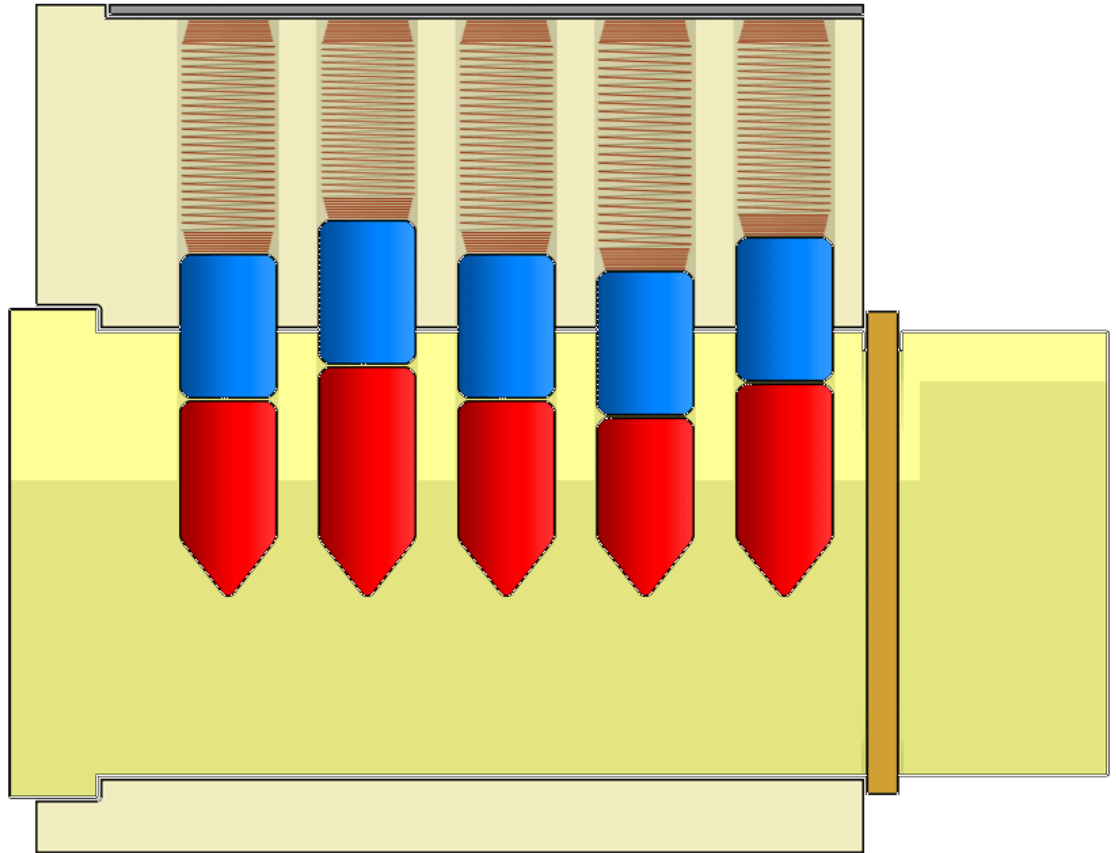
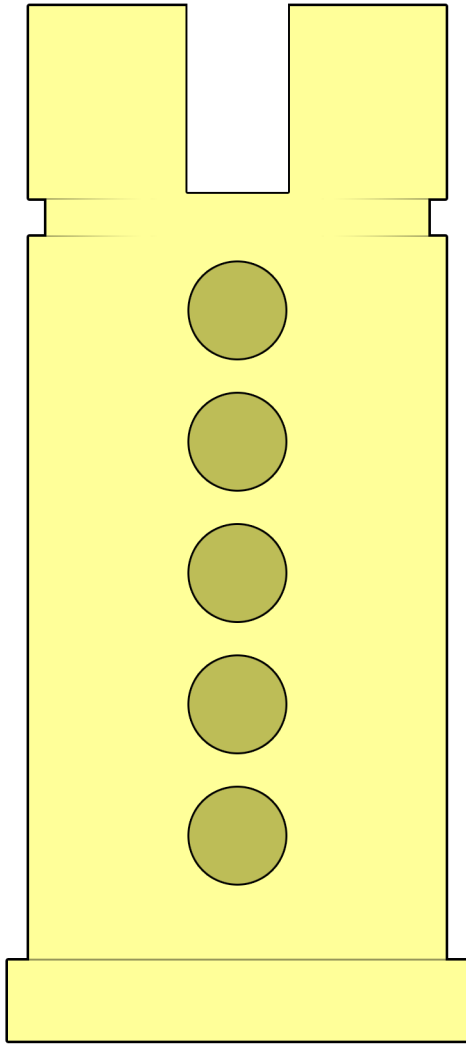
The Key Has To Be Just Right



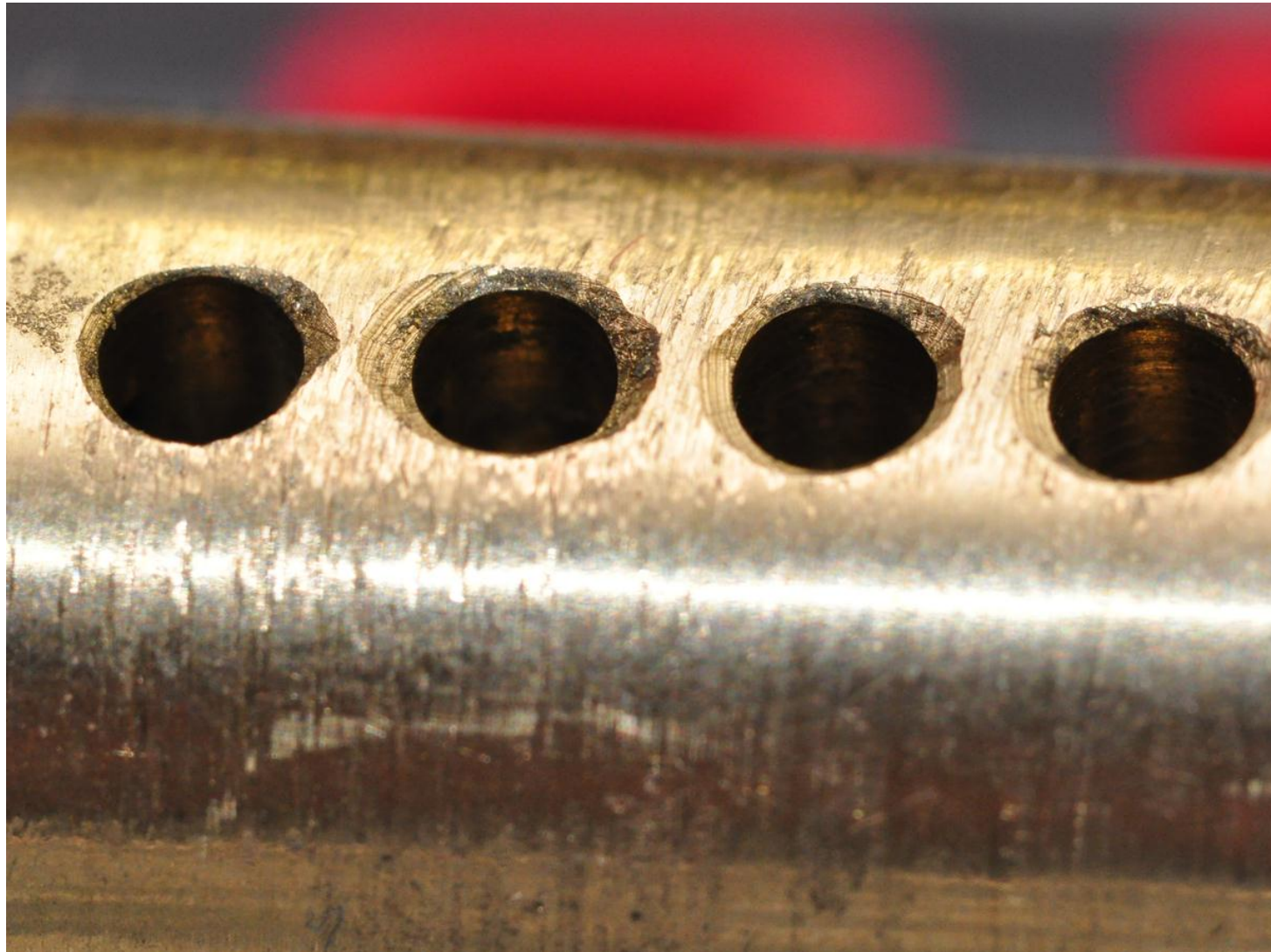
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
- 3. Picking is simple and fun**

In An Ideal World ...



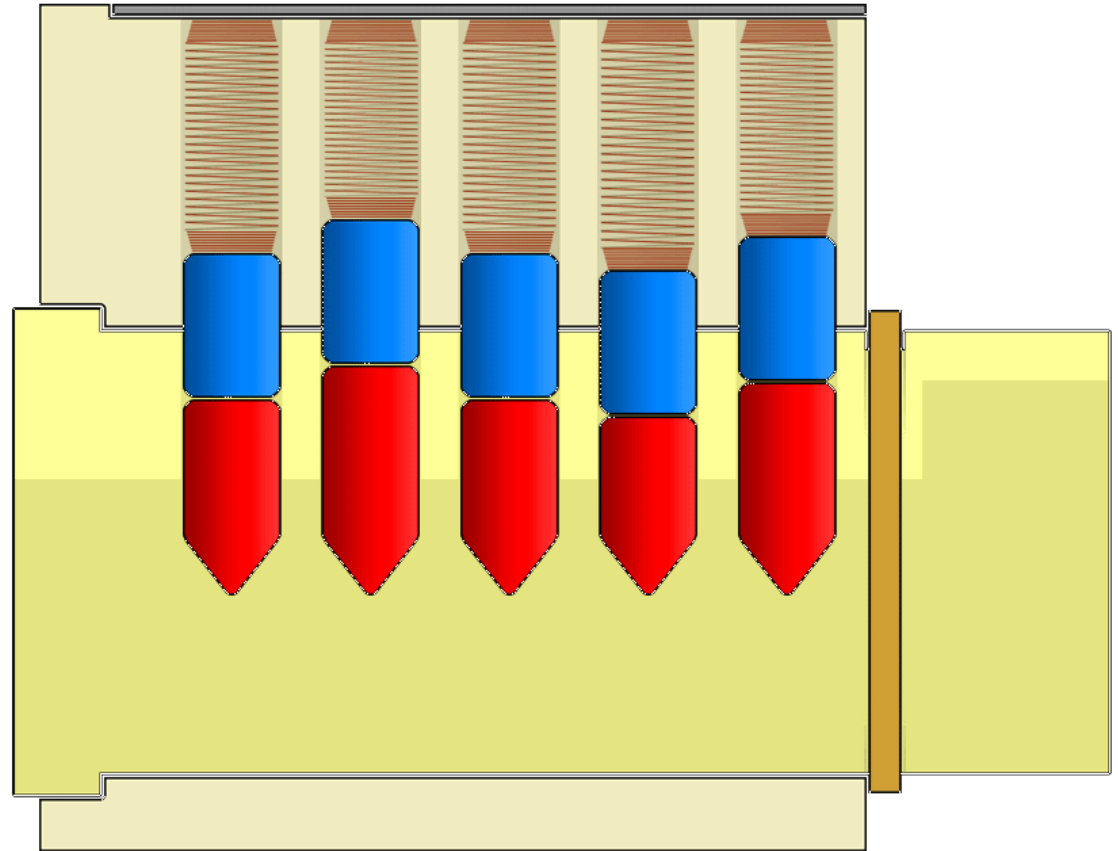
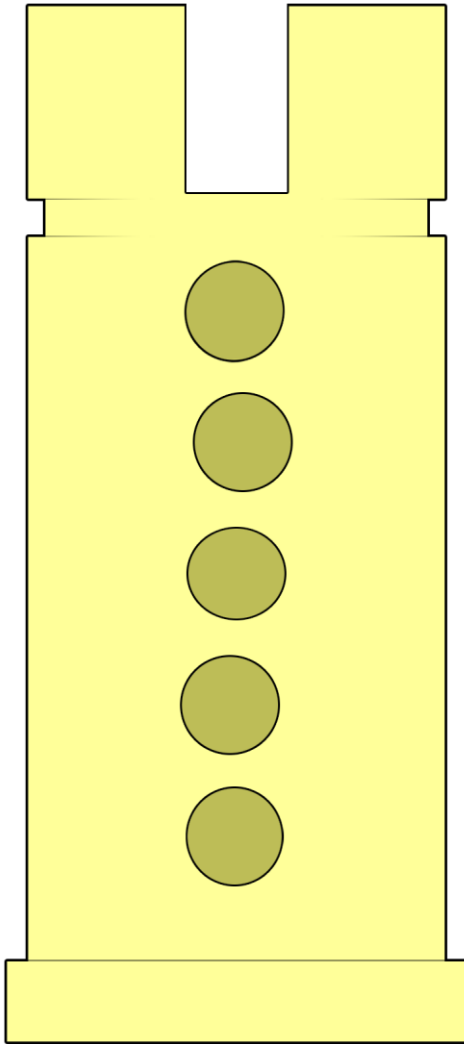
In The Real World...



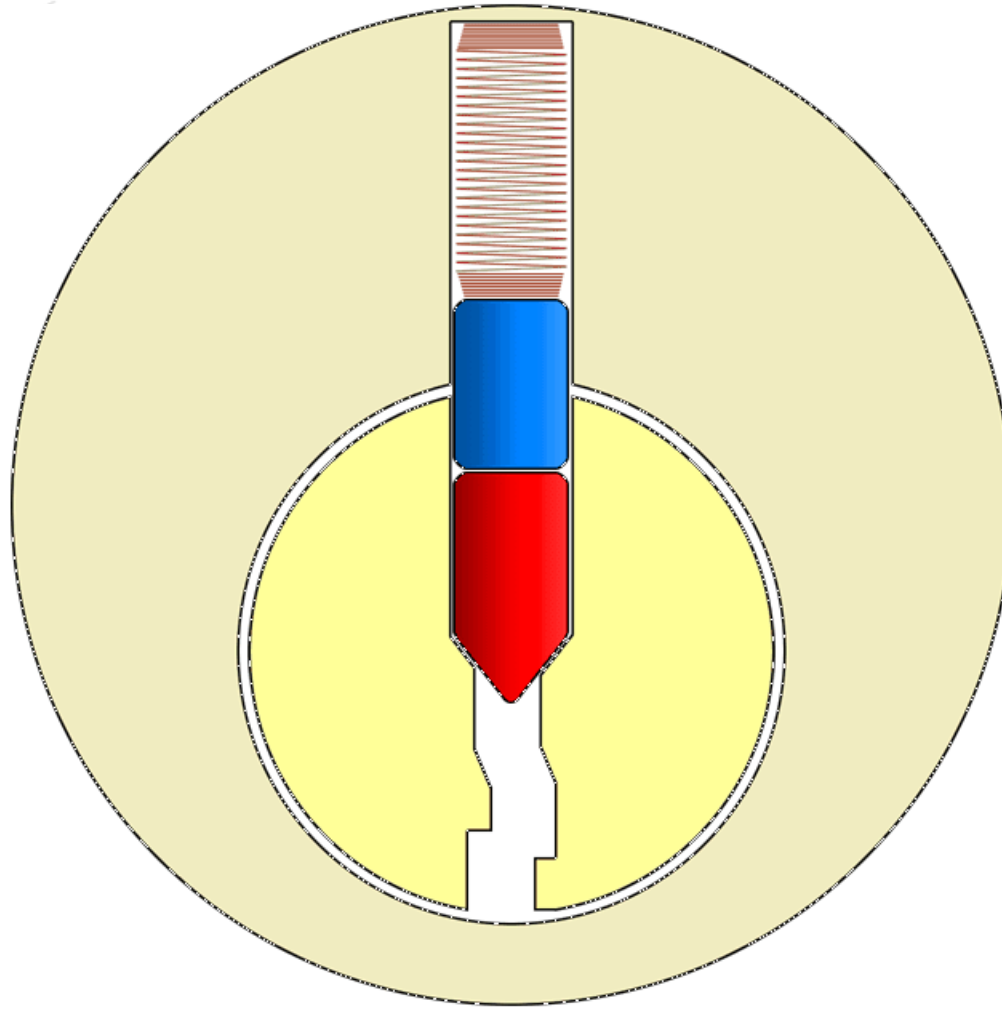
In The Real World...



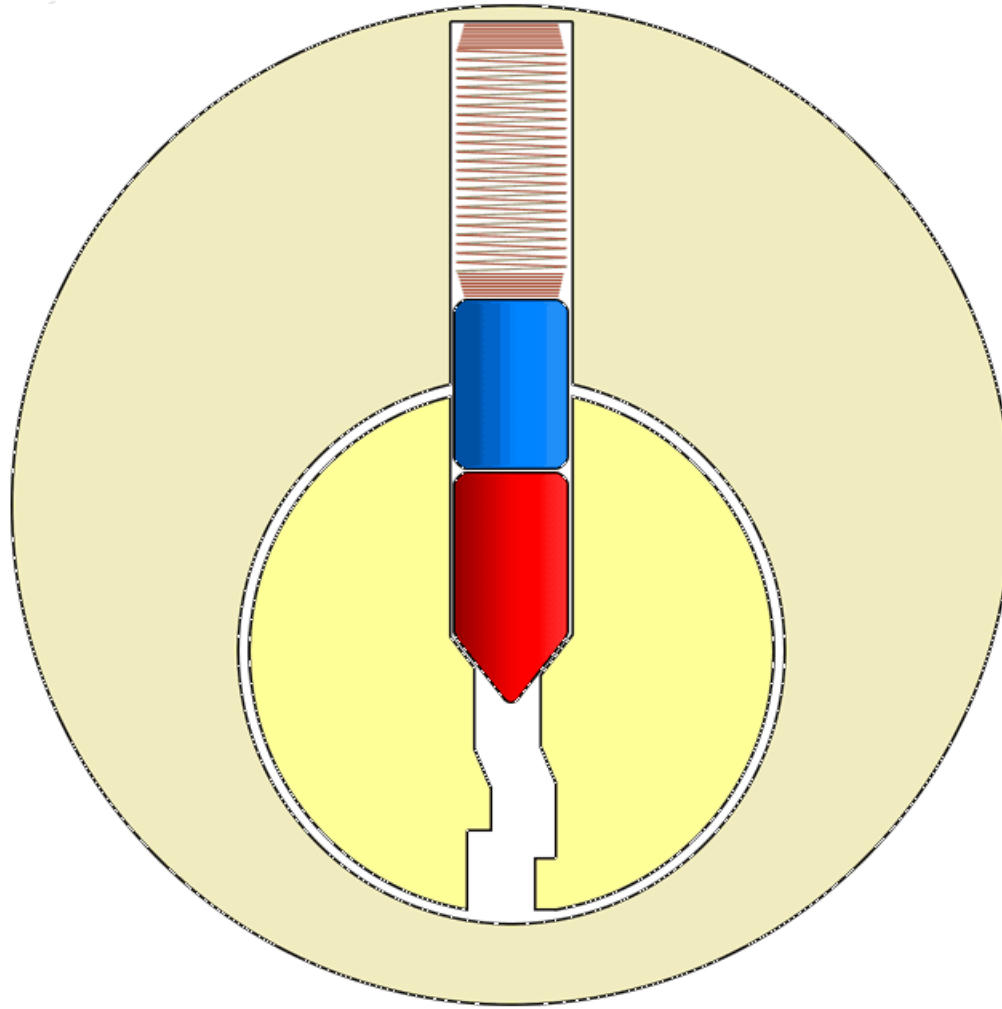
In The Real World ...



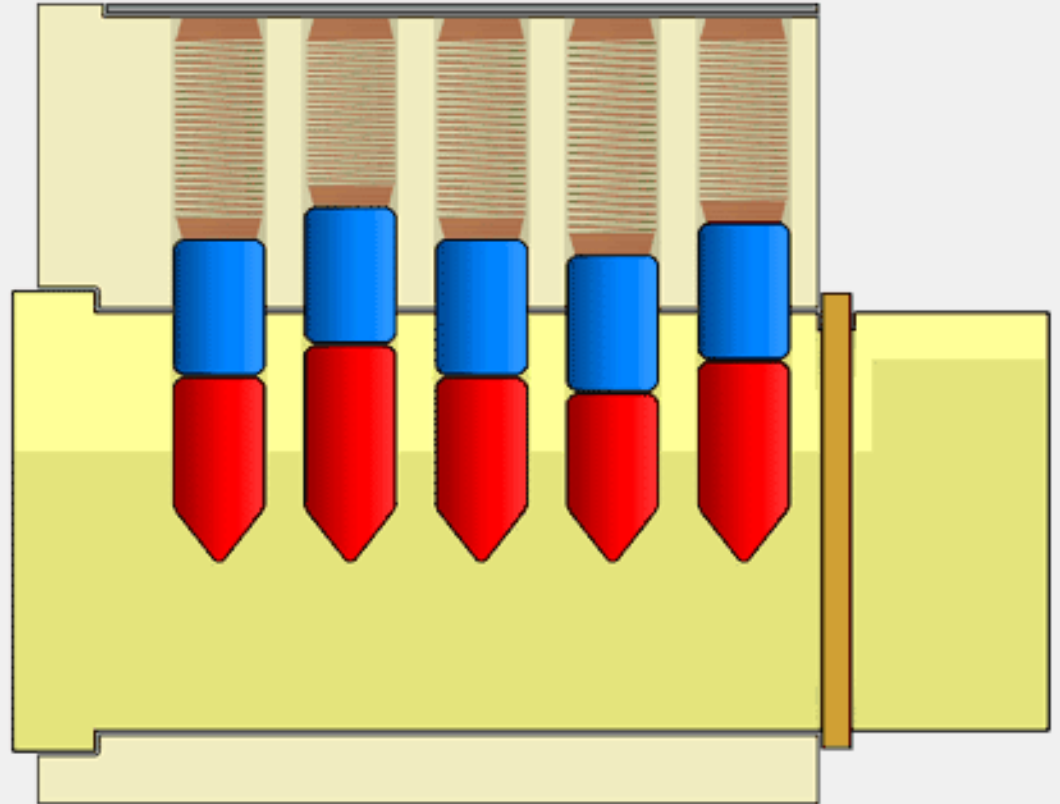
Setting a Pin



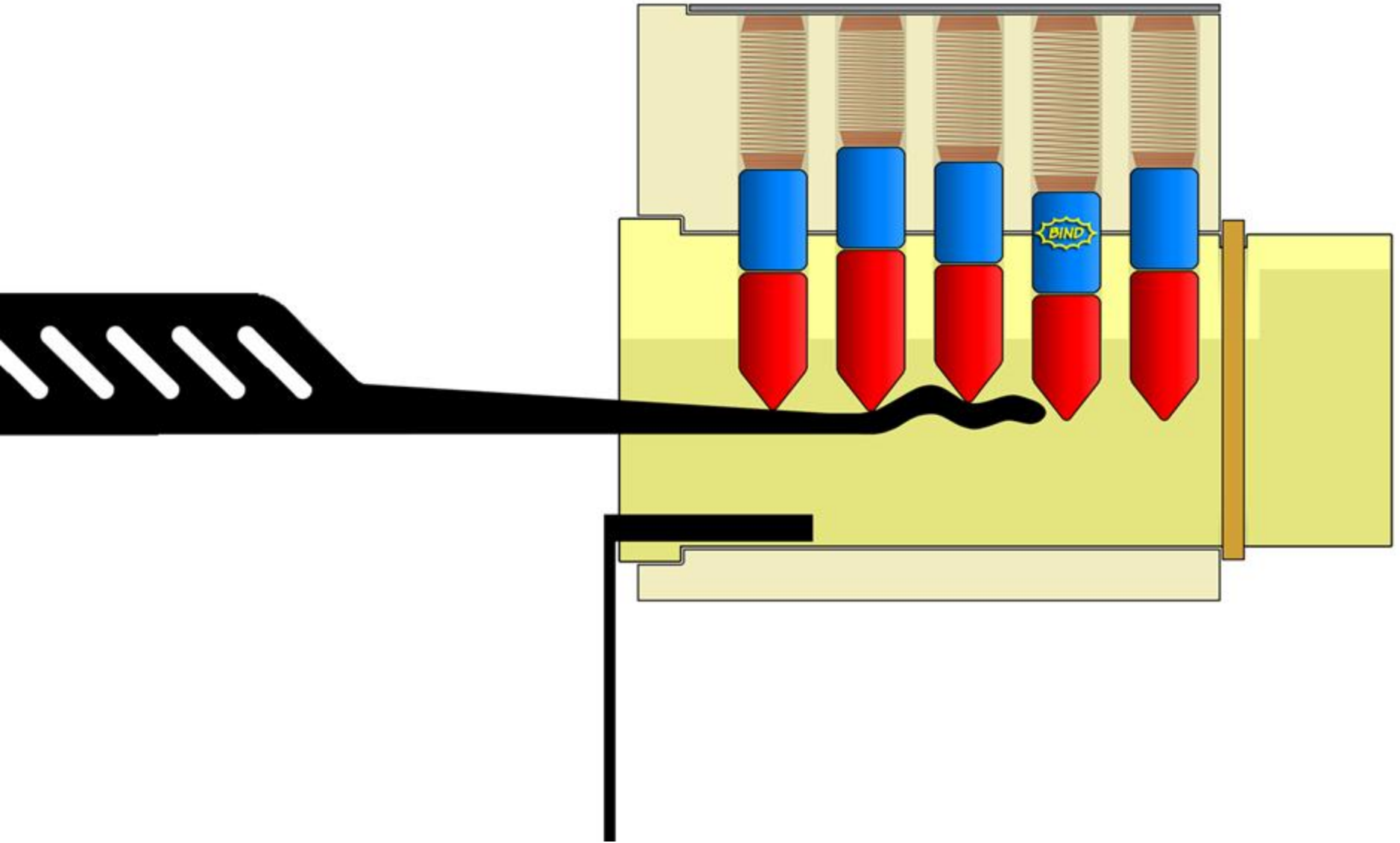
Setting a Pin



Setting the Pins



Setting the Pins



And You Can All Do This!



Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
- 4. Pins are pins, in any arrangement**

Other Ways of Arranging the Pins



Other Ways of Attacking the Pins



Other Ways of Attacking the Pins

But what about...



?

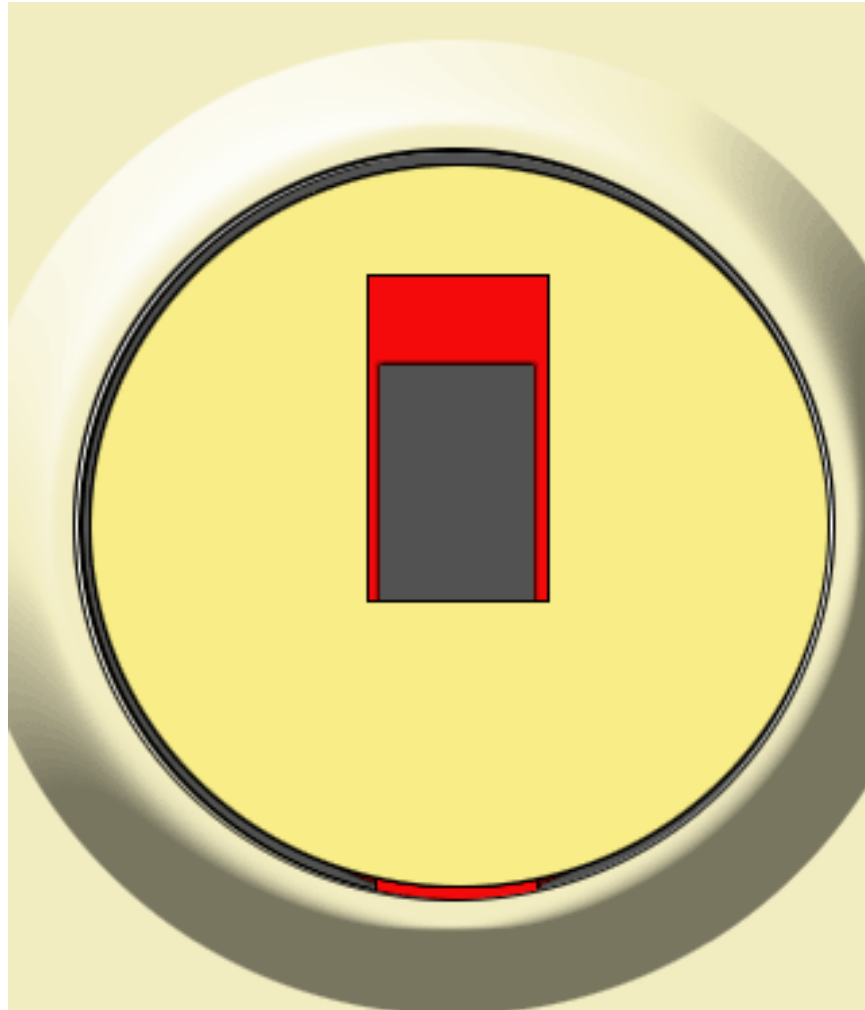
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. **Other everyday designs are often weak, too**

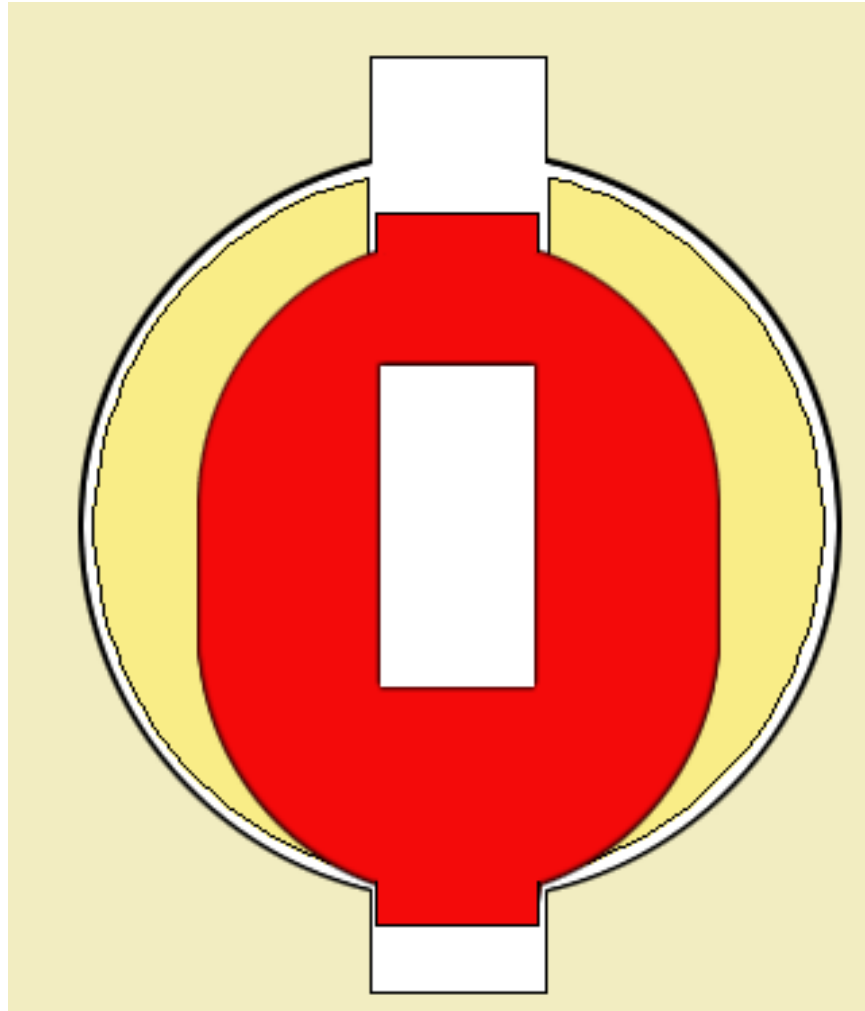
Wafer Locks



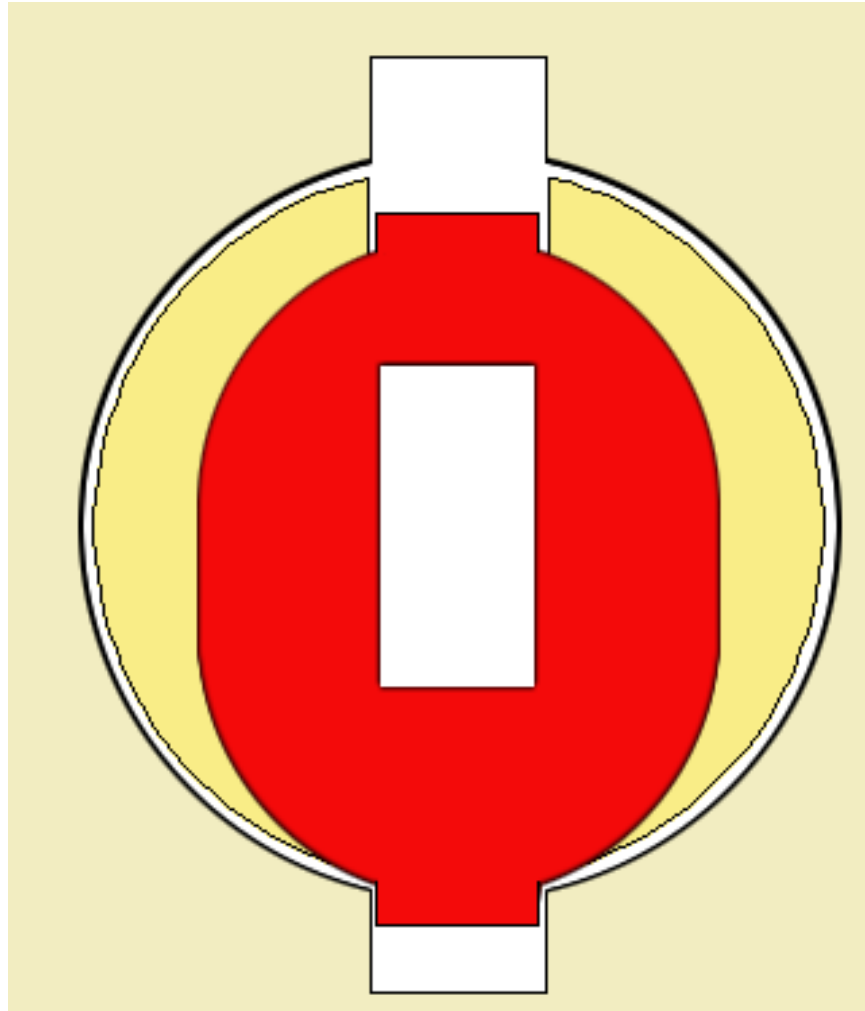
Wafer Locks



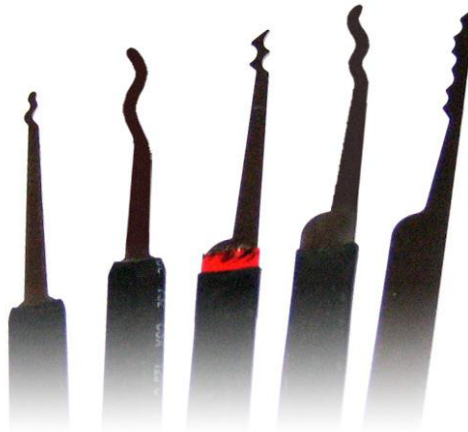
Wafer Locks



Wafer Locks



Raking & Jiggling



Raking & Jiggling



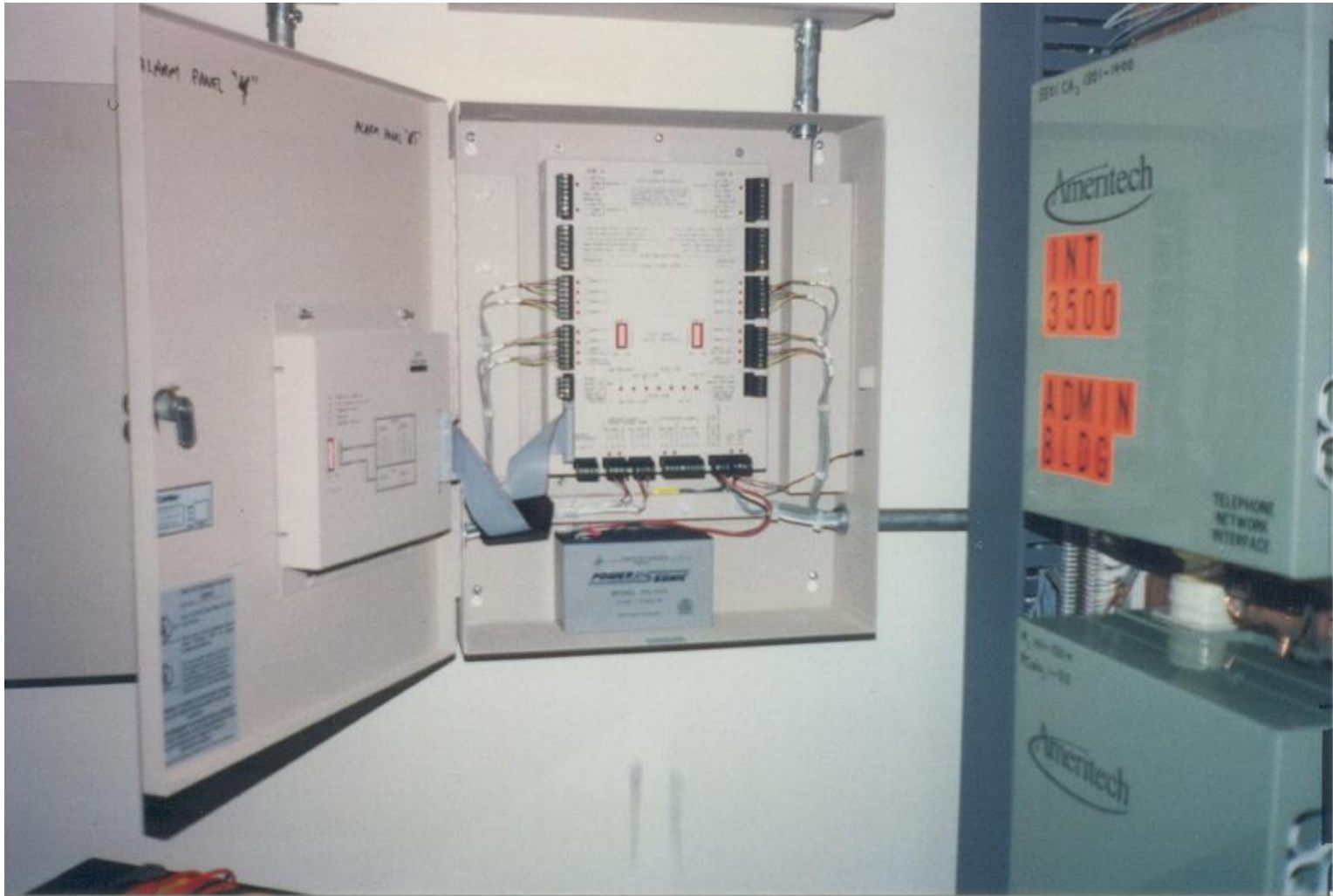
Wafer Lock Usage



Wafer Lock Usage



Wafer Lock Usage



Wafer Lock Usage



Wafer Lock Usage



Wafer Lock Usage



Wafer Lock Usage



Wafer Lock Usage



Wafer Lock Usage



Wafer Lock Usage



Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings

Popular Padlocks



Terrible Padlocks



Padlock Shims



Padlock Shims... From a Catalog



Padlock Shims... From a Beer Can



Padlock Shims



Padlock Shim Prevention

Double Ball Mechanism



Padlock Shim Prevention

Which Padlocks are Protected?



Padlock Shim Prevention

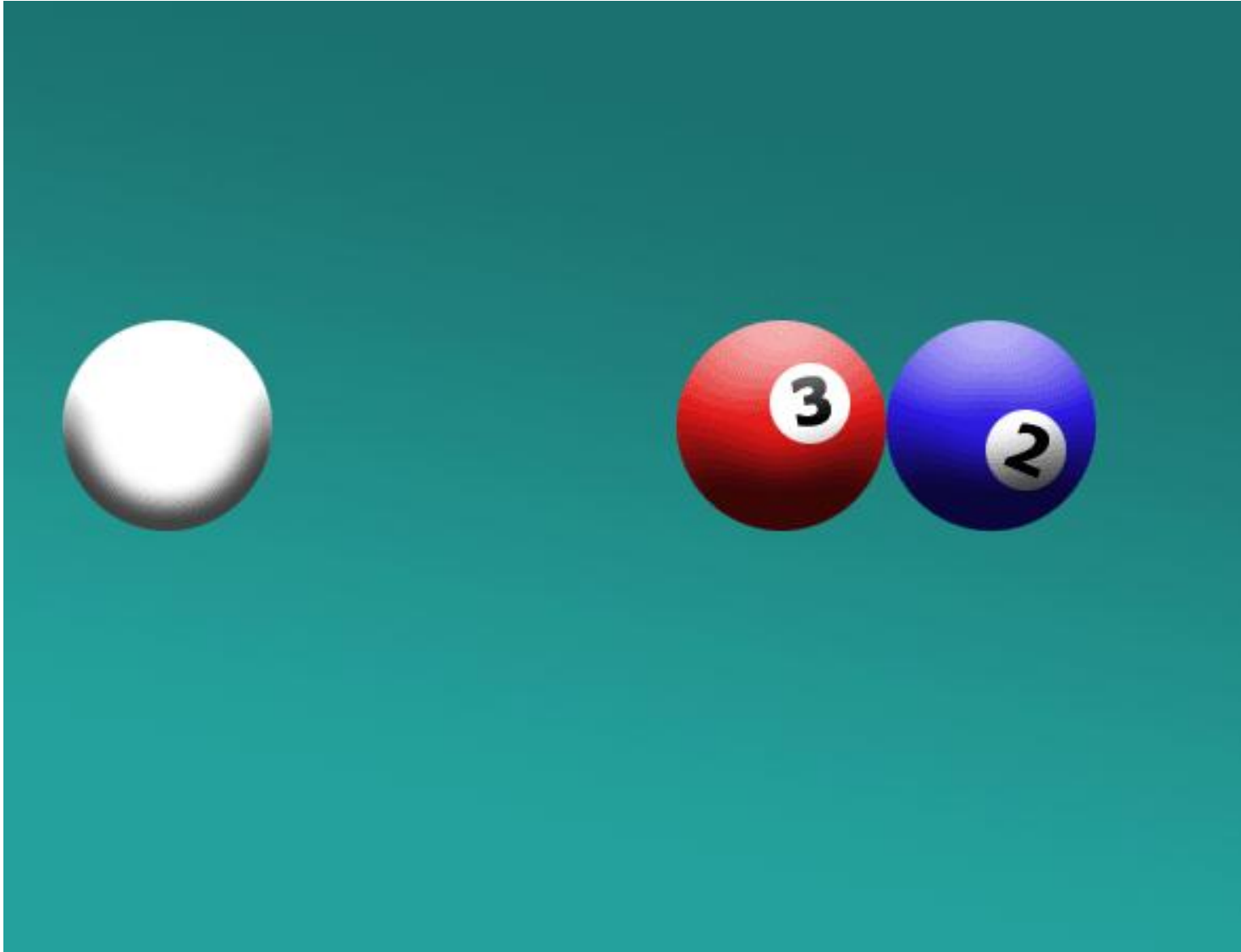


Padlock Shim Prevention

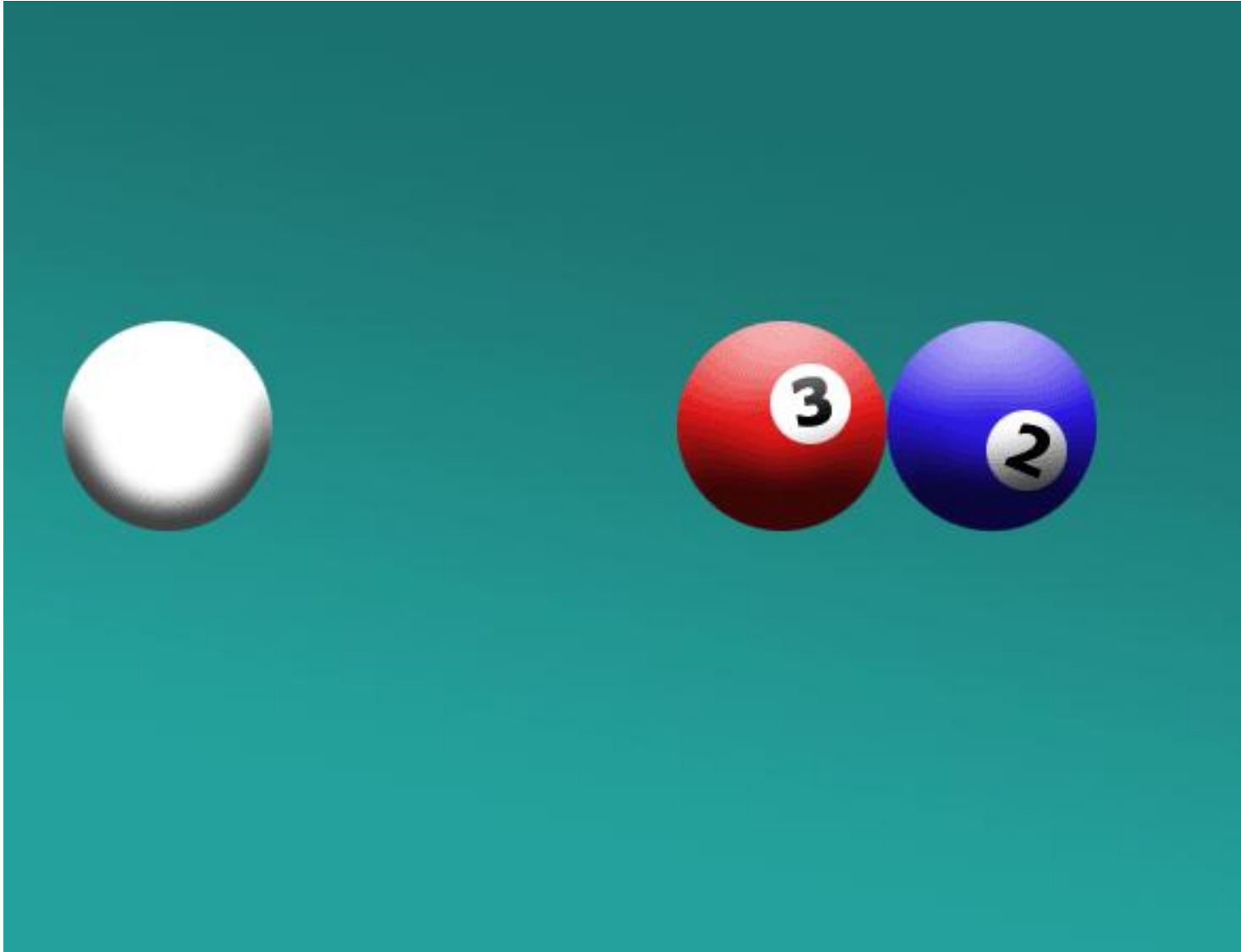


Candado doble traba a bolilla
acero inoxidable

Bumping



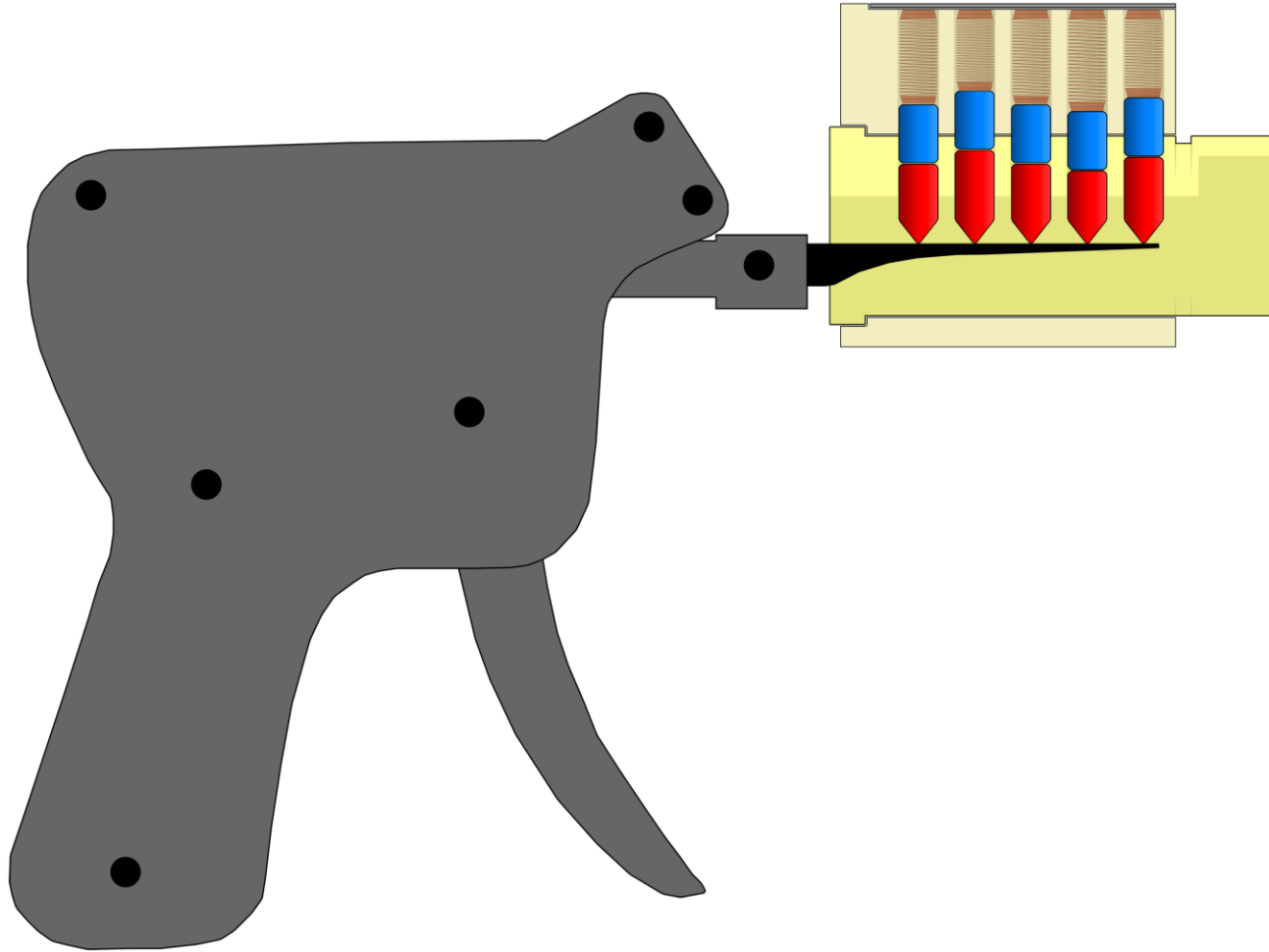
Bumping



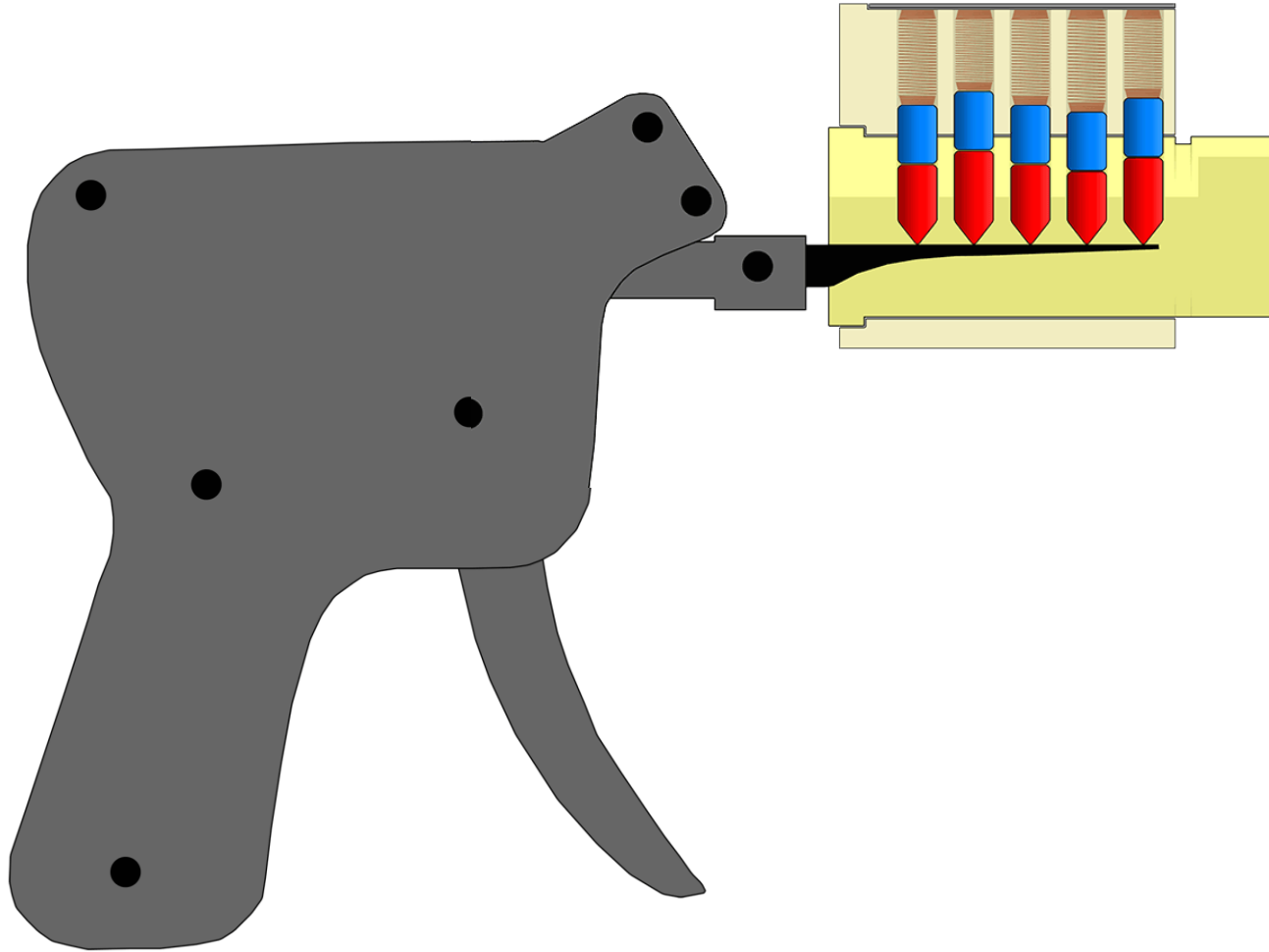
Bumping



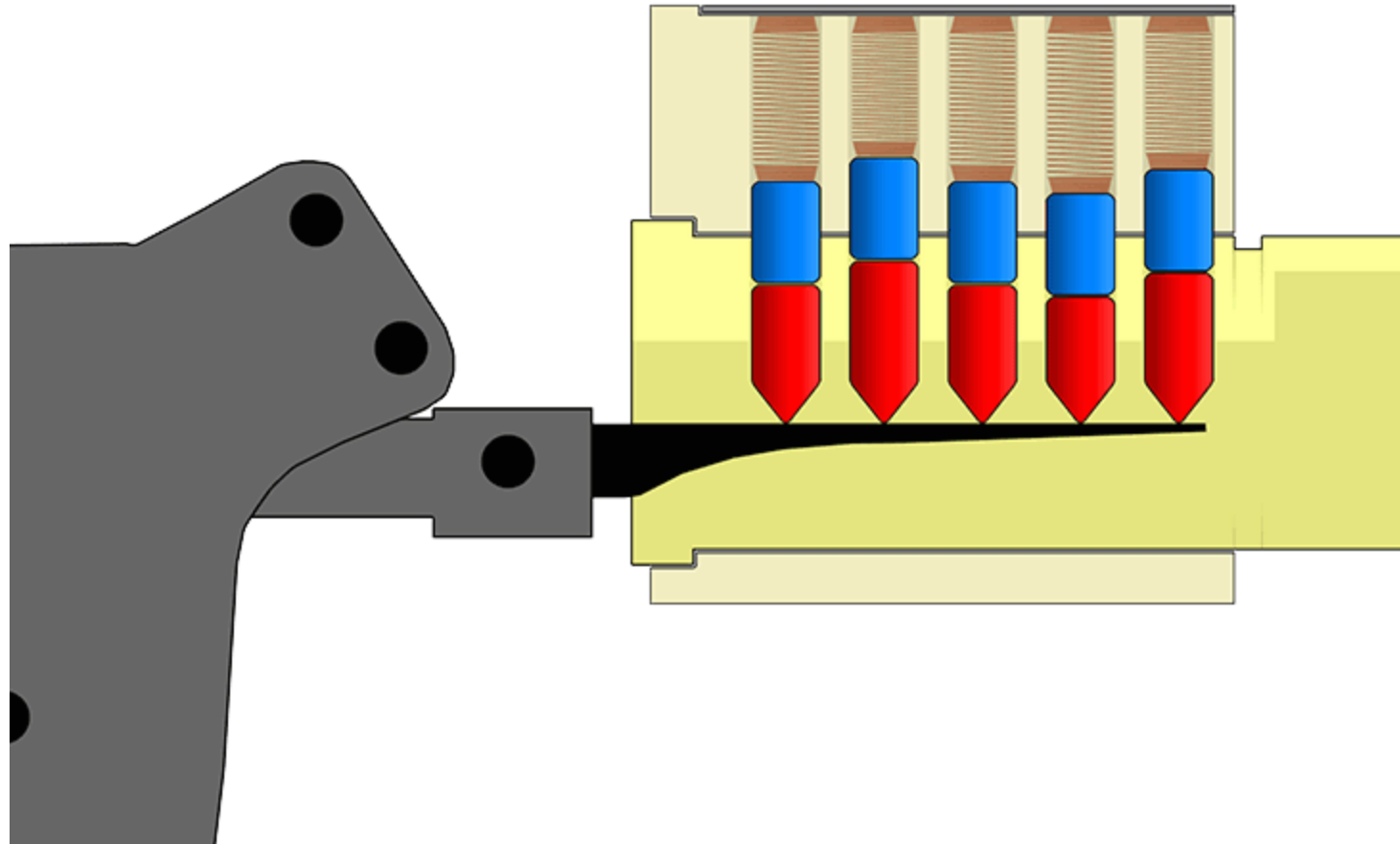
Bumping



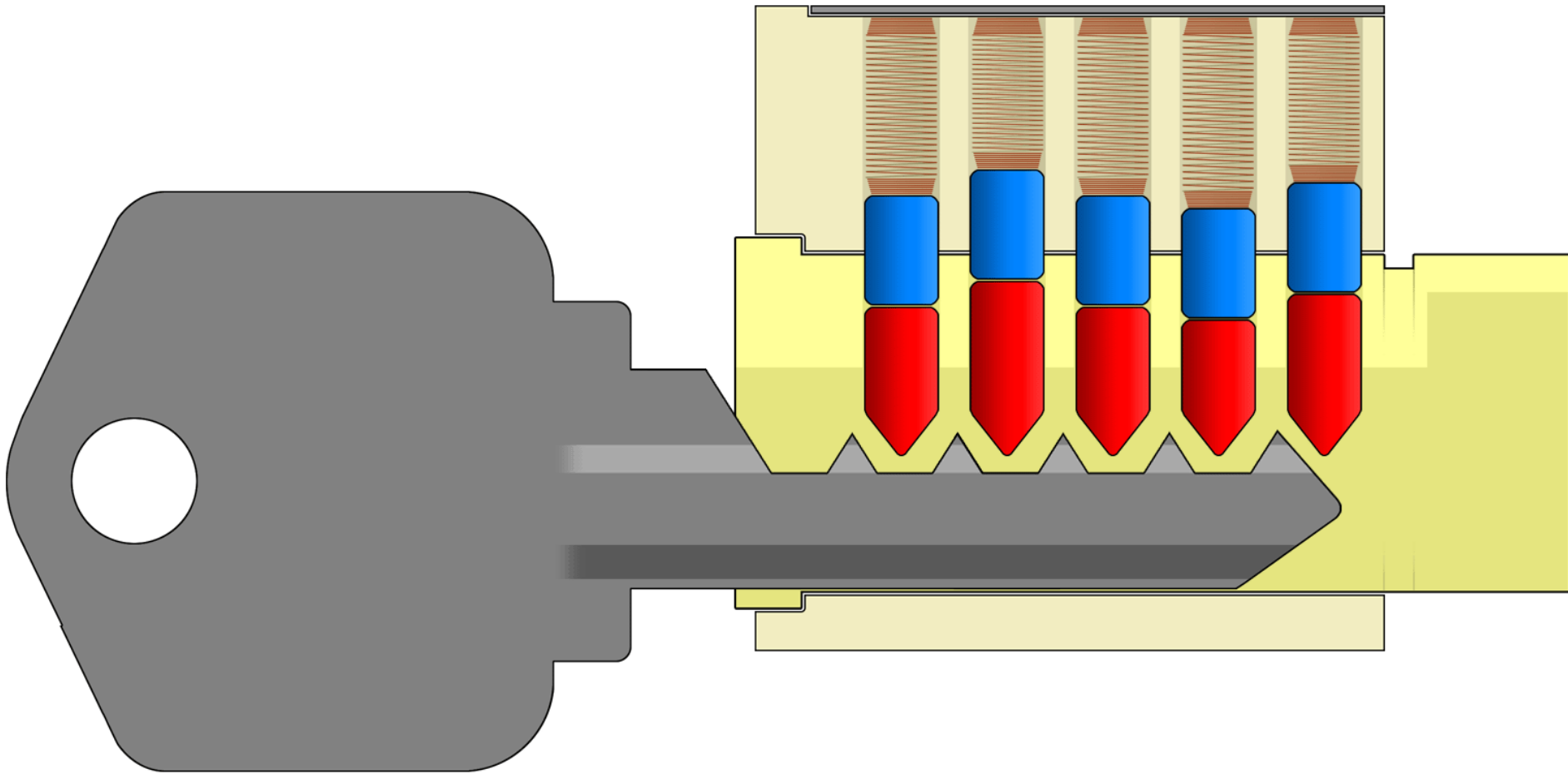
Bumping



Bumping



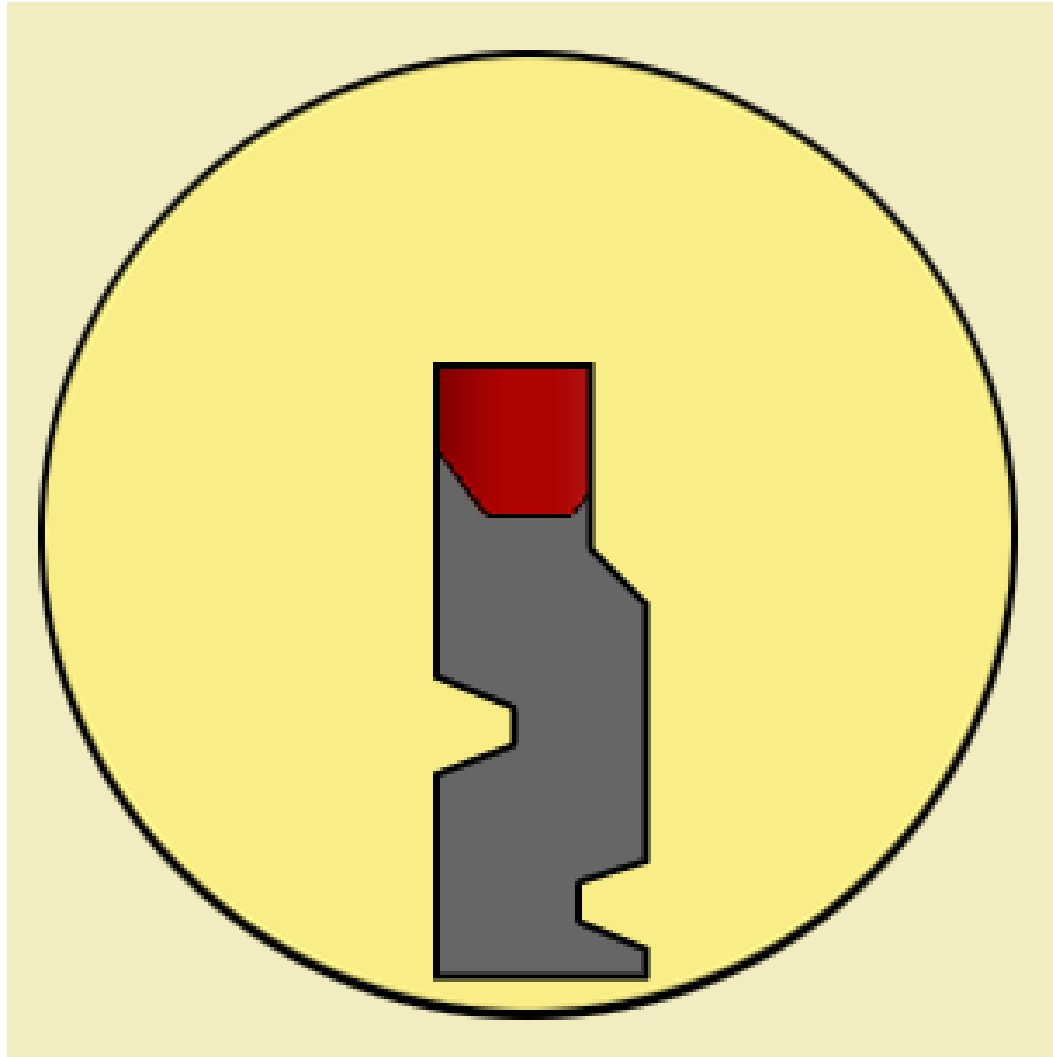
Bumping



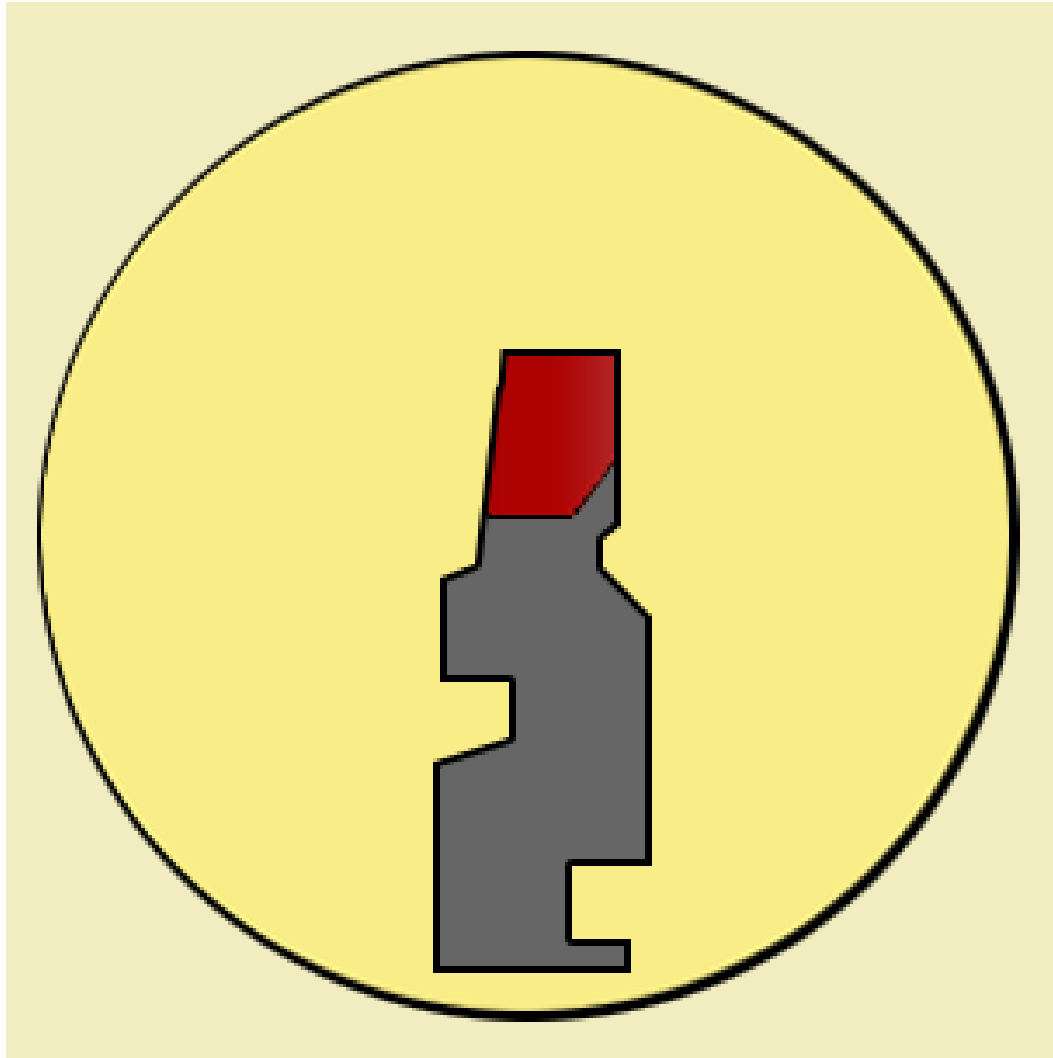
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings
- 7. Many locks are pick resistant**

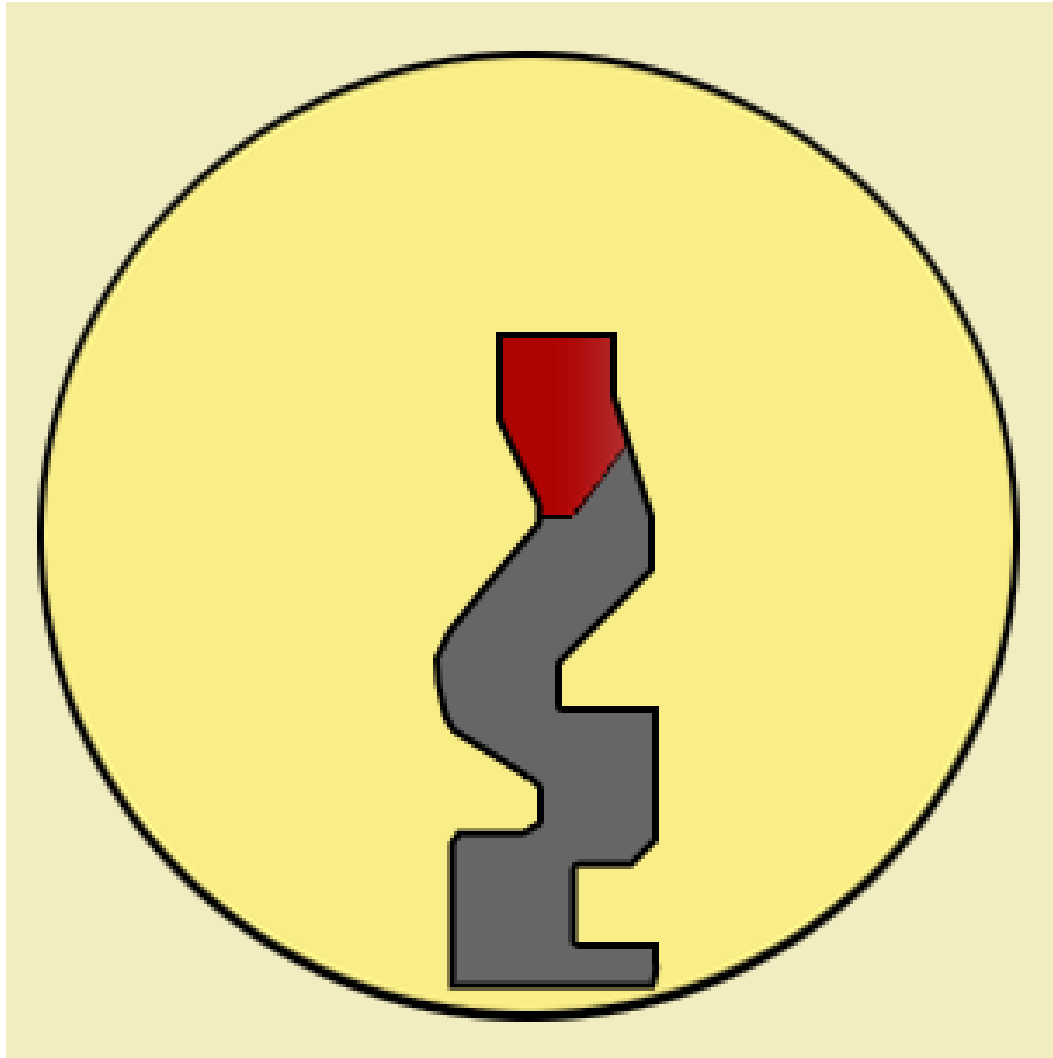
Pick-Resistant Keyways



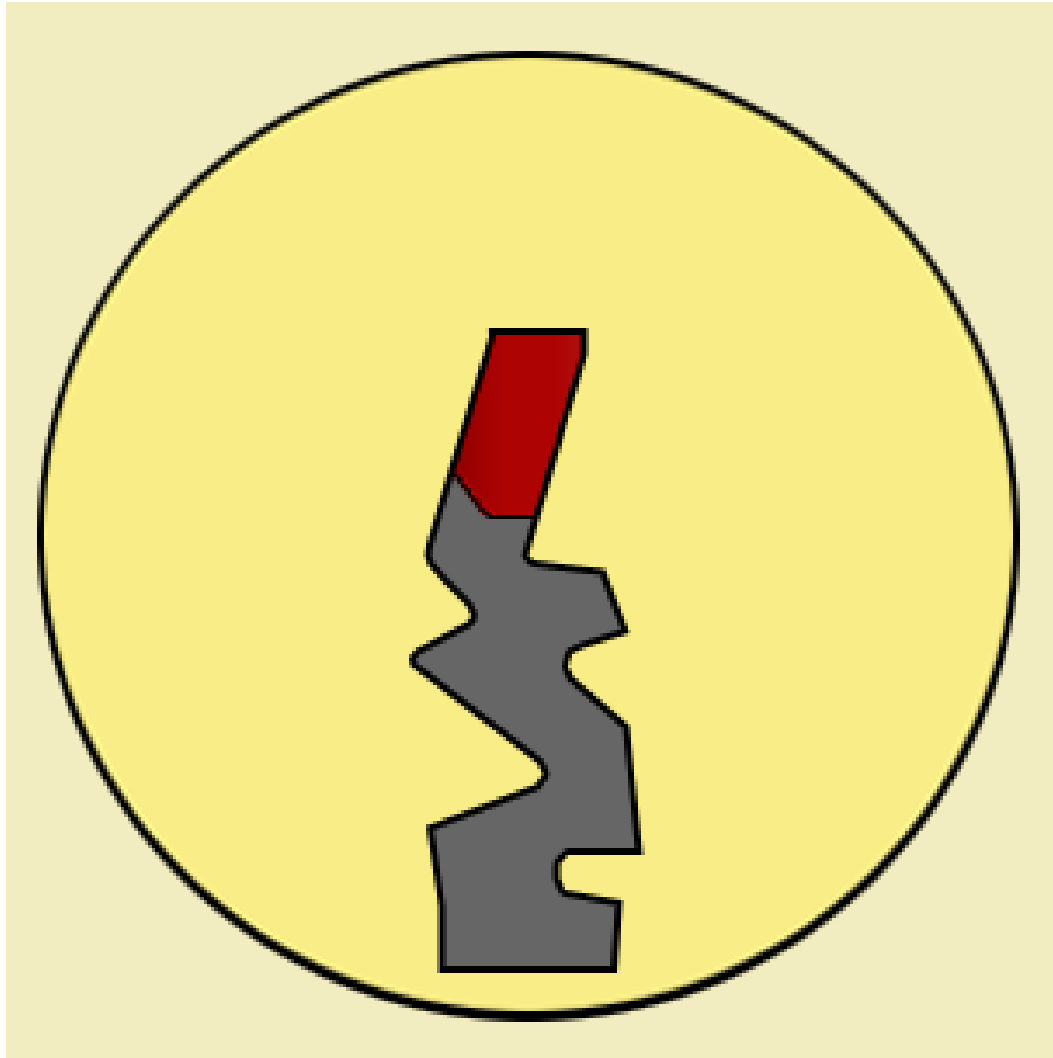
Pick-Resistant Keyways



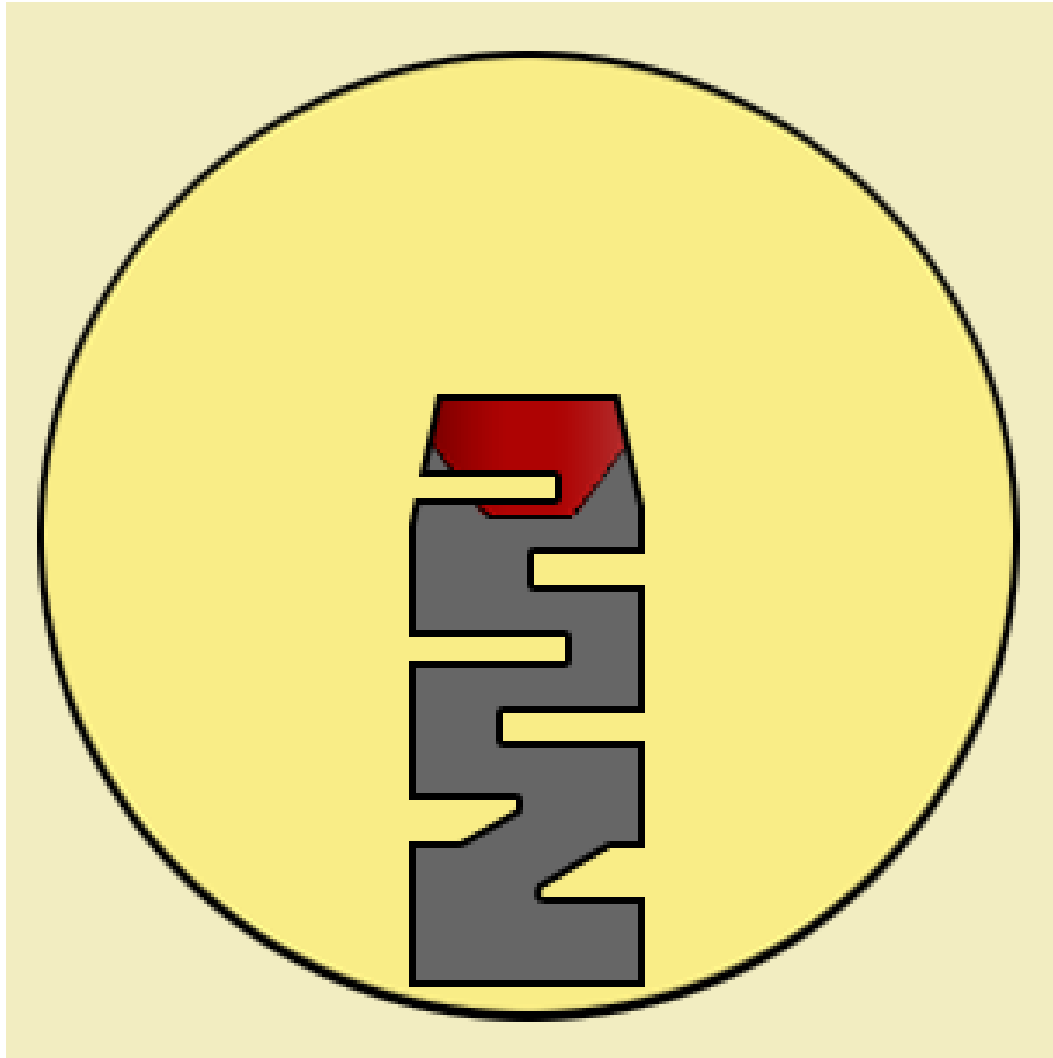
Pick-Resistant Keyways



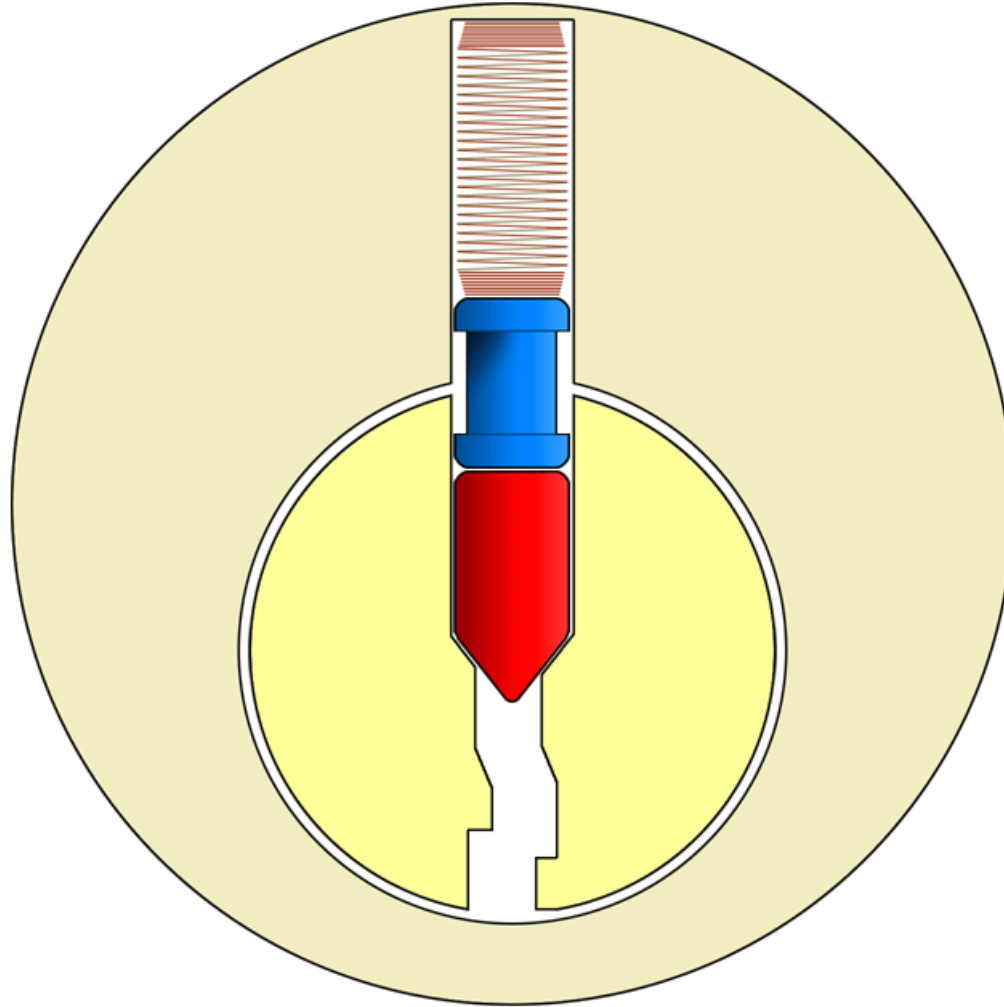
Pick-Resistant Keyways



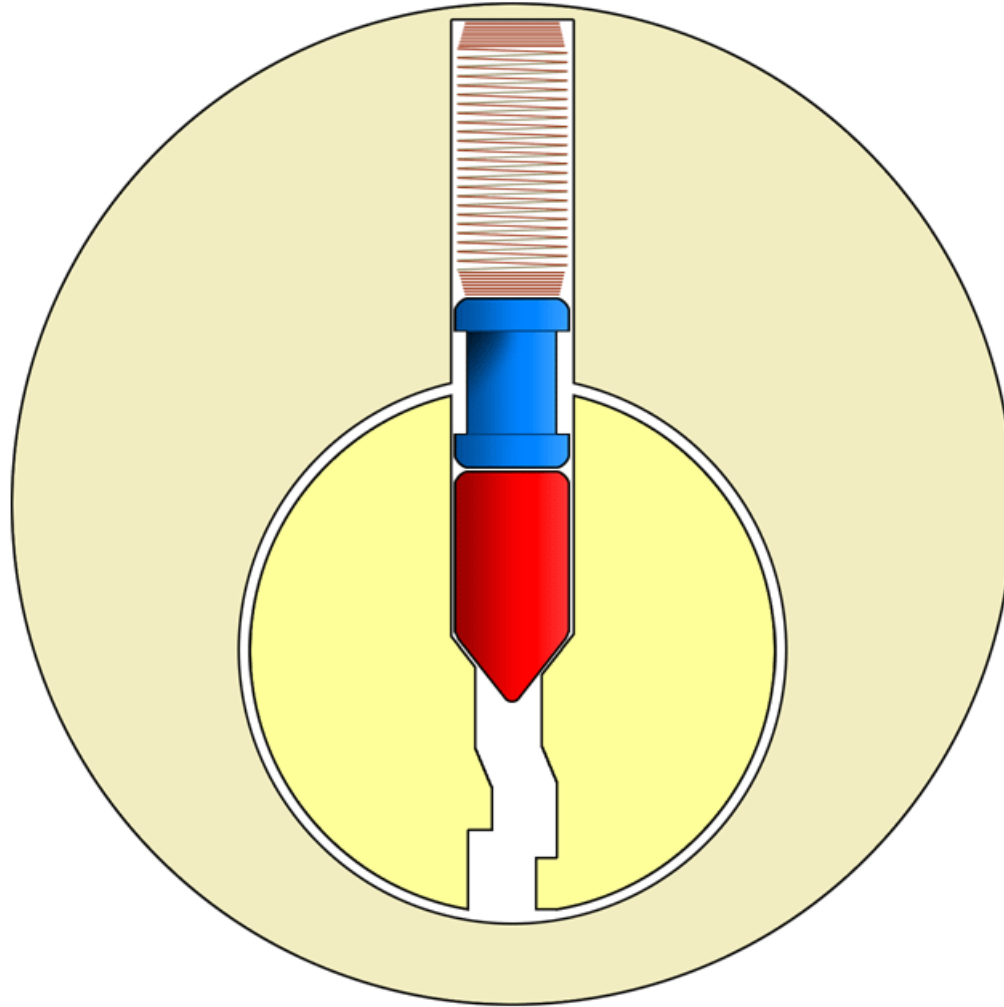
Pick-Resistant Keyways



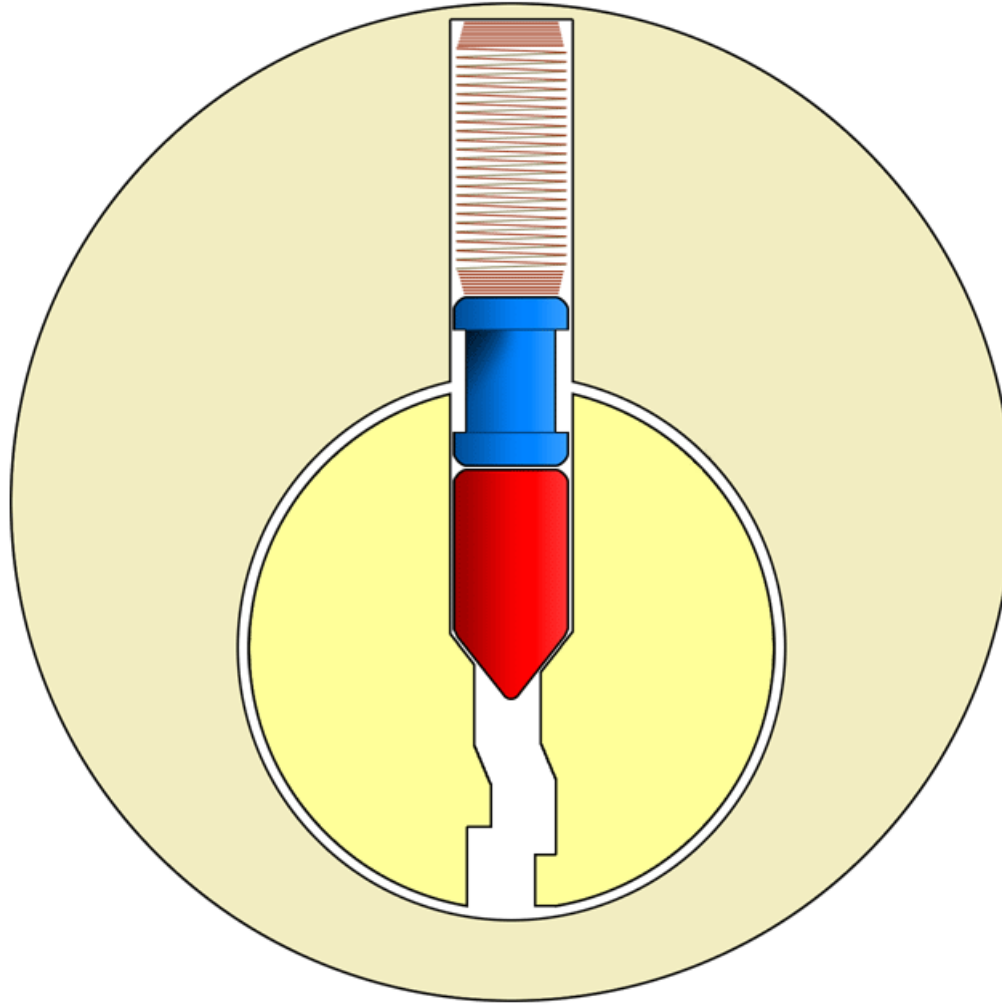
Pick-Resistant Pins



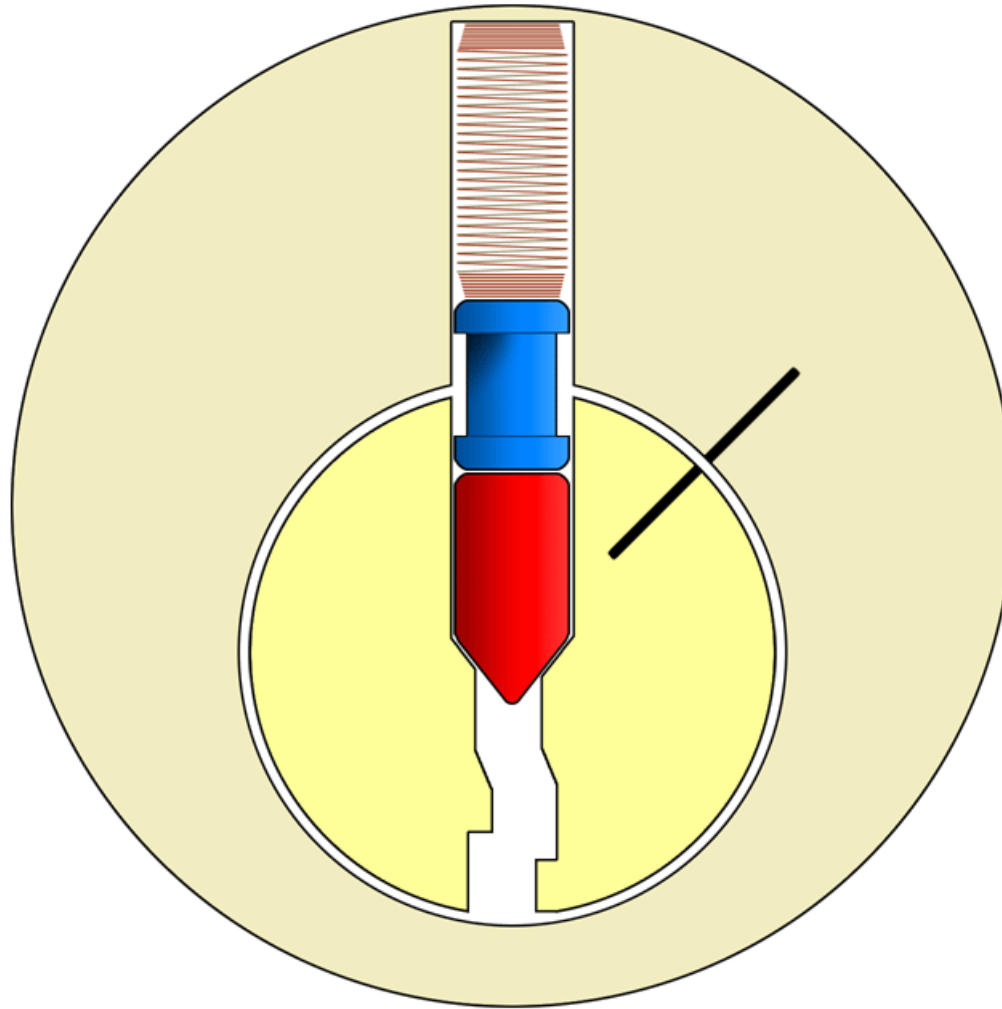
Pick-Resistant Pins



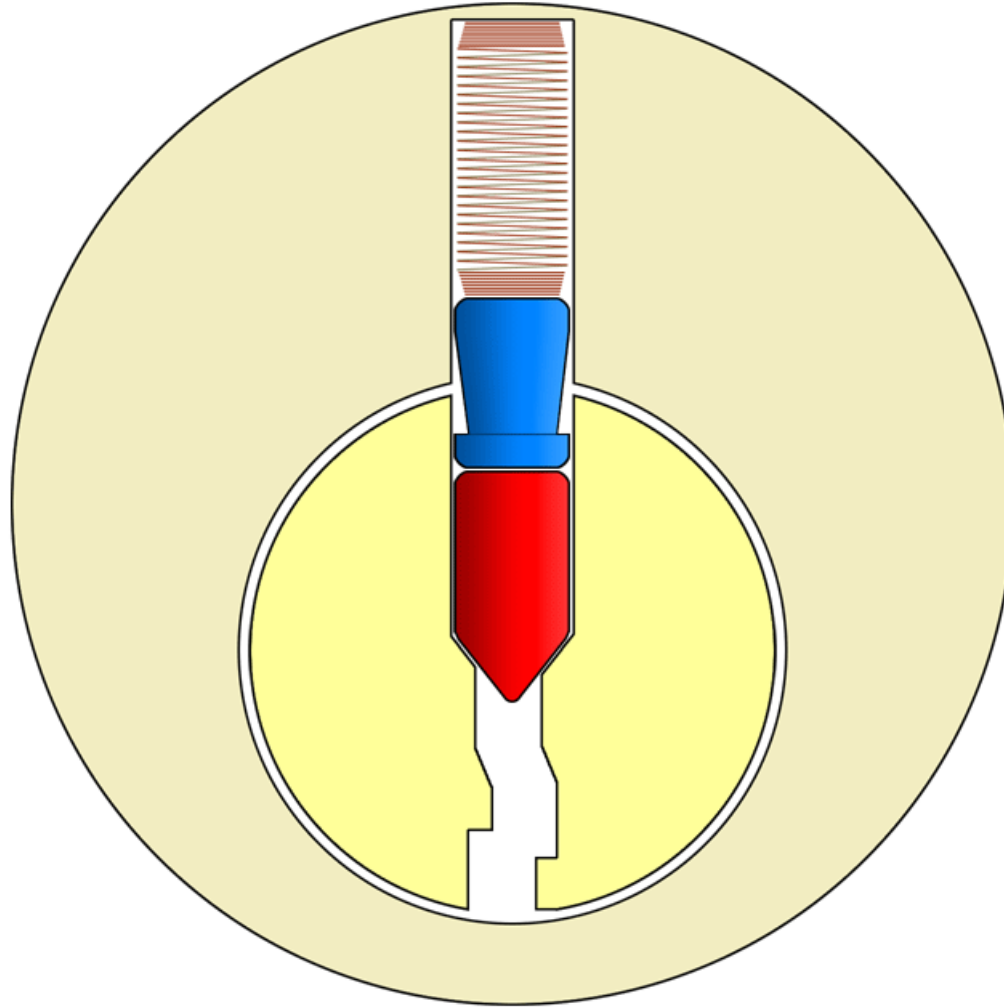
Pick-Resistant Pins



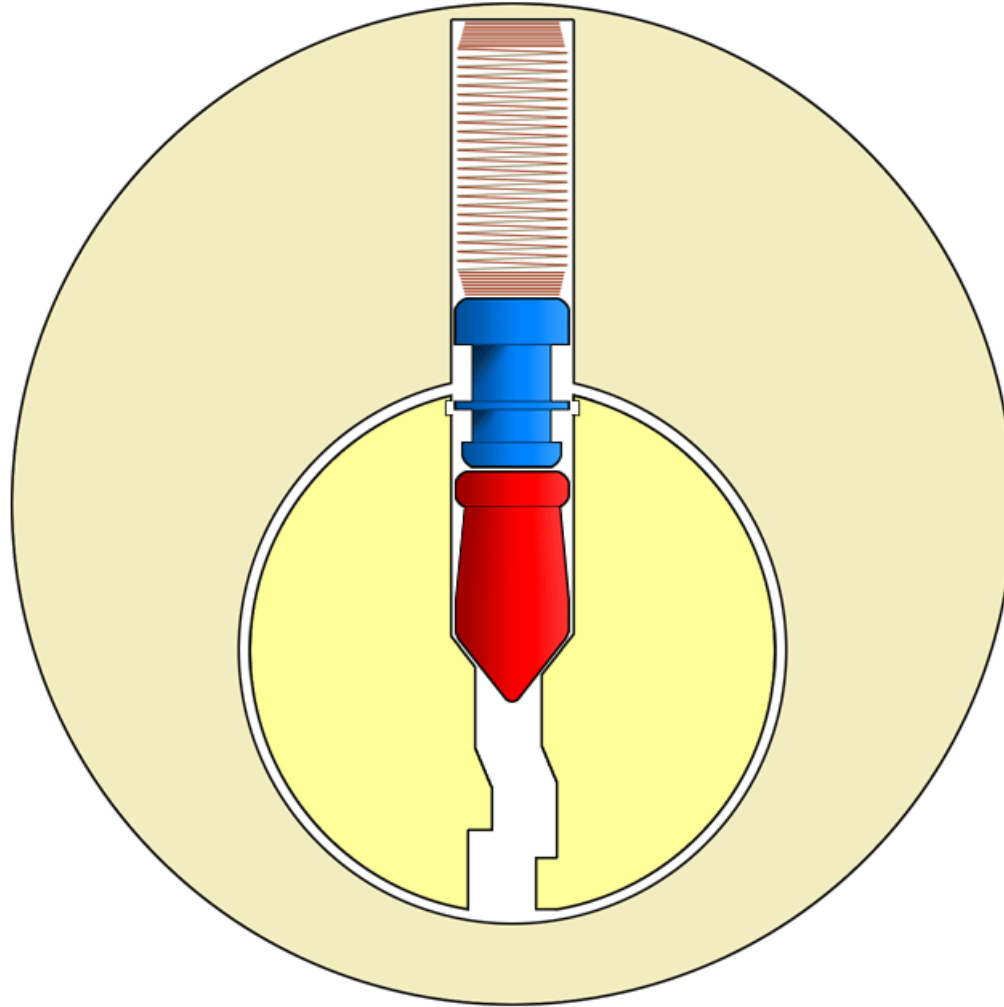
Pick-Resistant Pins



Pick-Resistant Pins



Pick-Resistant Pins



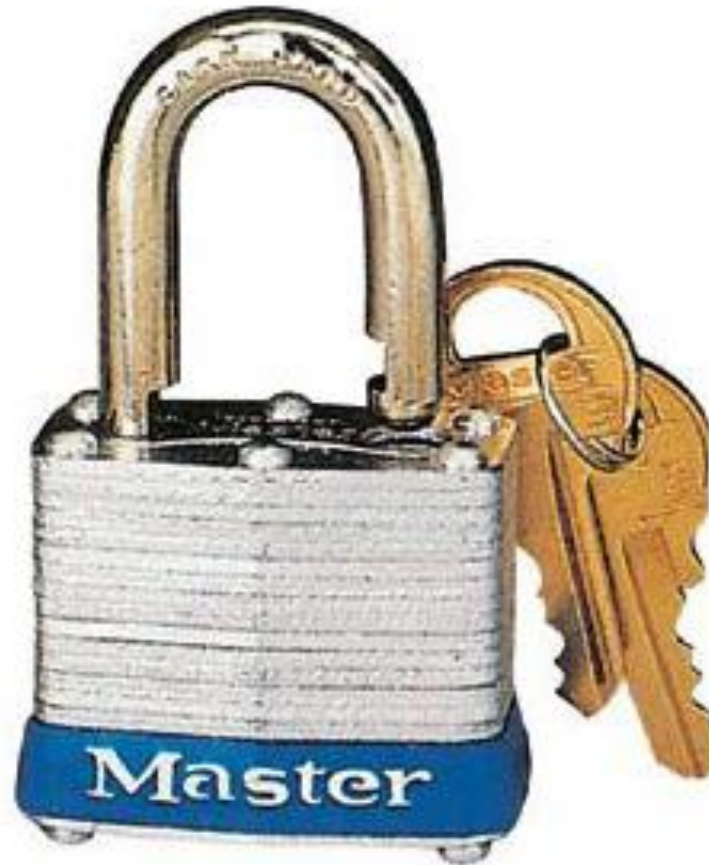
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings
7. Many locks are pick resistant
- 8. Poor locks spread like a contamination**

Contamination by Poor Locks



Contamination by Poor Locks



Contamination by Poor Locks



Contamination by Poor Locks



Contamination by Poor Locks



Contamination by Poor Locks



Contamination by Poor Locks



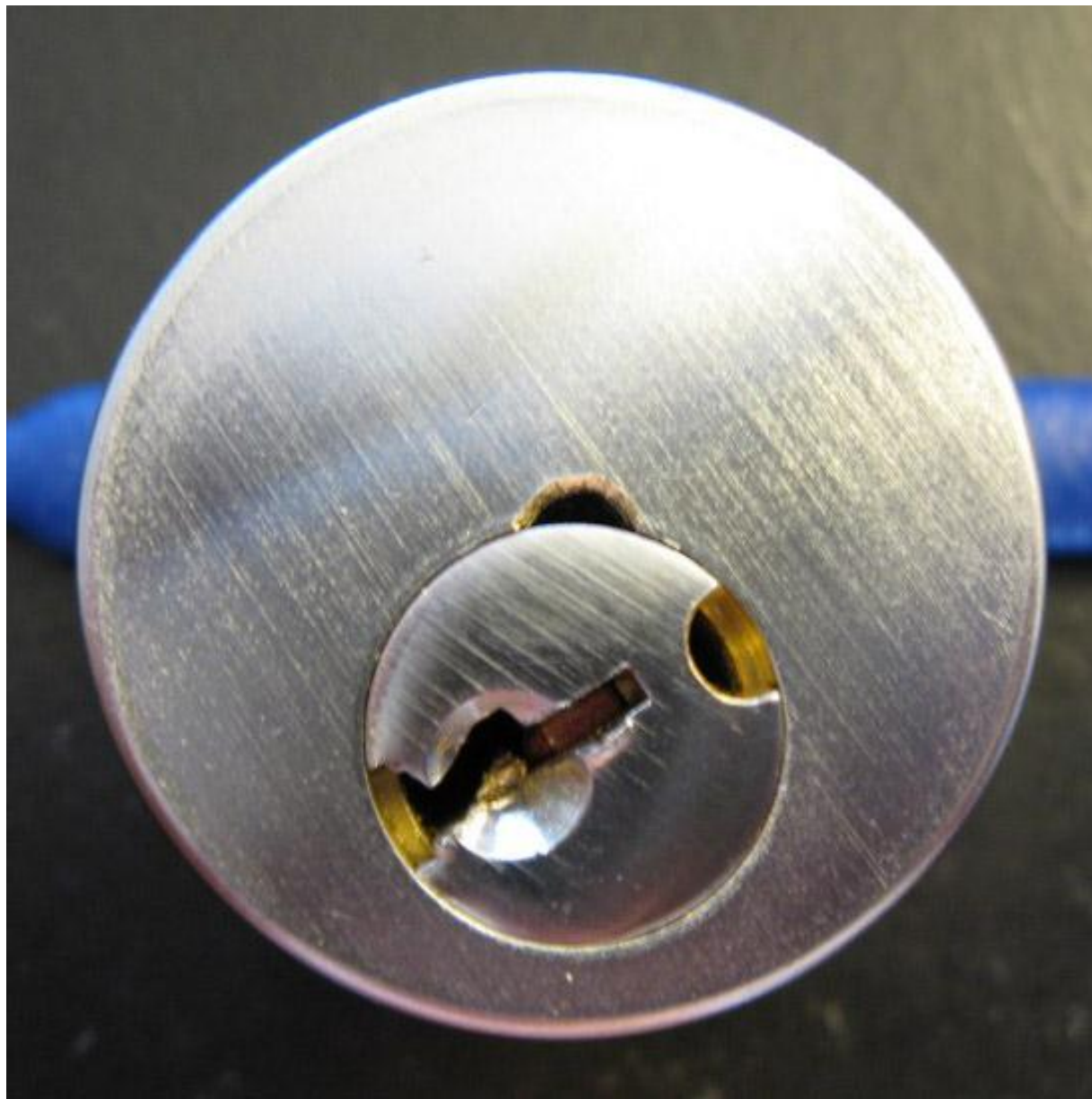
Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings
7. Many locks are pick resistant
8. Poor locks spread like a contamination
9. It comes down to your attackers and defenders













Most Attacks are Brute Force



But Covert Entry Is A Risk



This Lock Did Its Job (sort of)



High Security Locks as Seals



Things You Should Know about Lockpicking...

1. Why locks matter to IT professionals
2. Pin tumblers are universal
3. Picking is simple and fun
4. Pins are pins, in any arrangement
5. Other everyday designs are often weak, too
6. You can open locks with beer and beatings
7. Many locks are pick resistant
8. Poor locks spread like a contamination
9. It comes down to your attackers and defenders
10. Many times, the lock isn't what is attacked

Bypassing



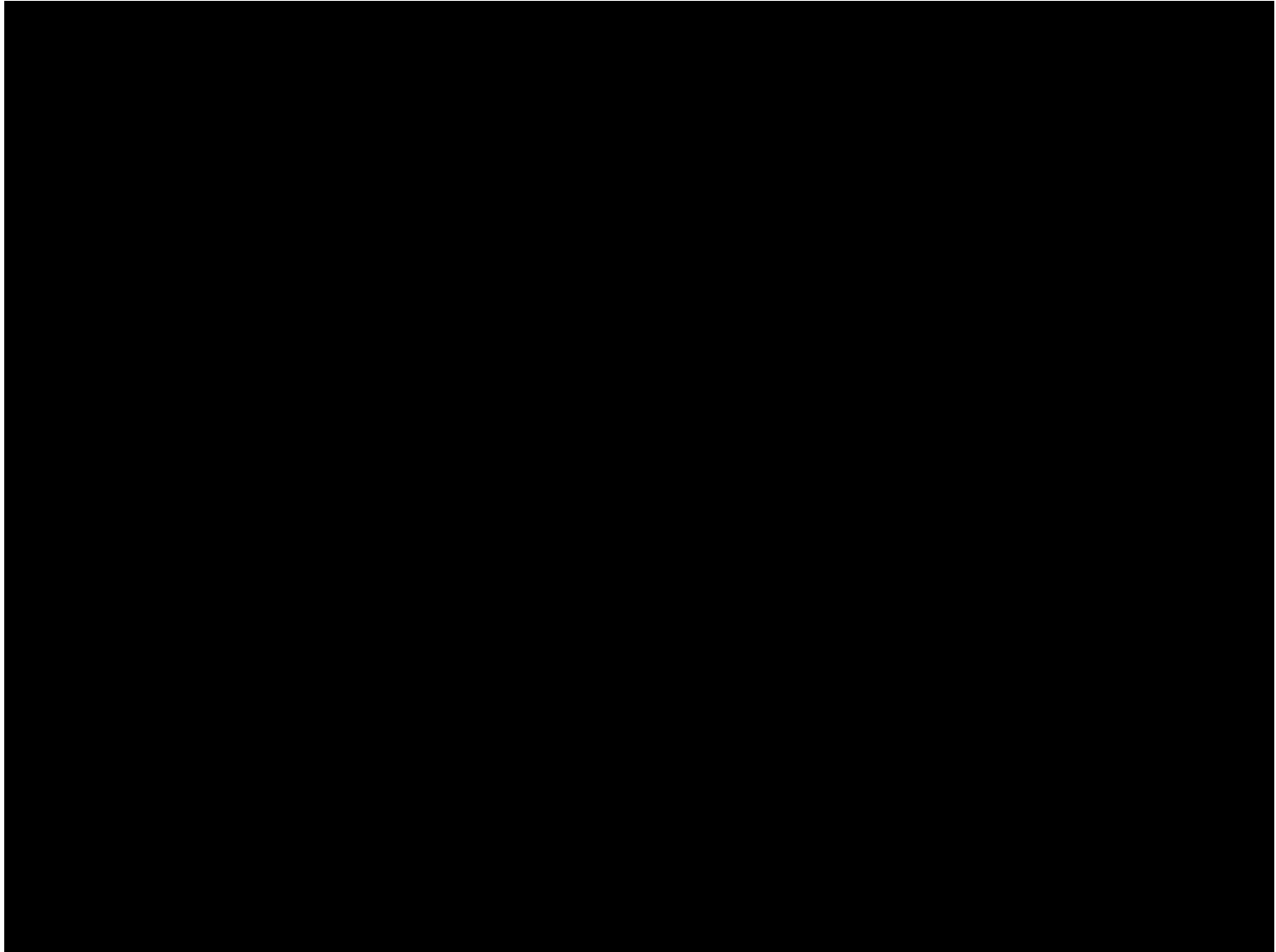
Bypassing



Bypassing



Bypassing



Bypassing



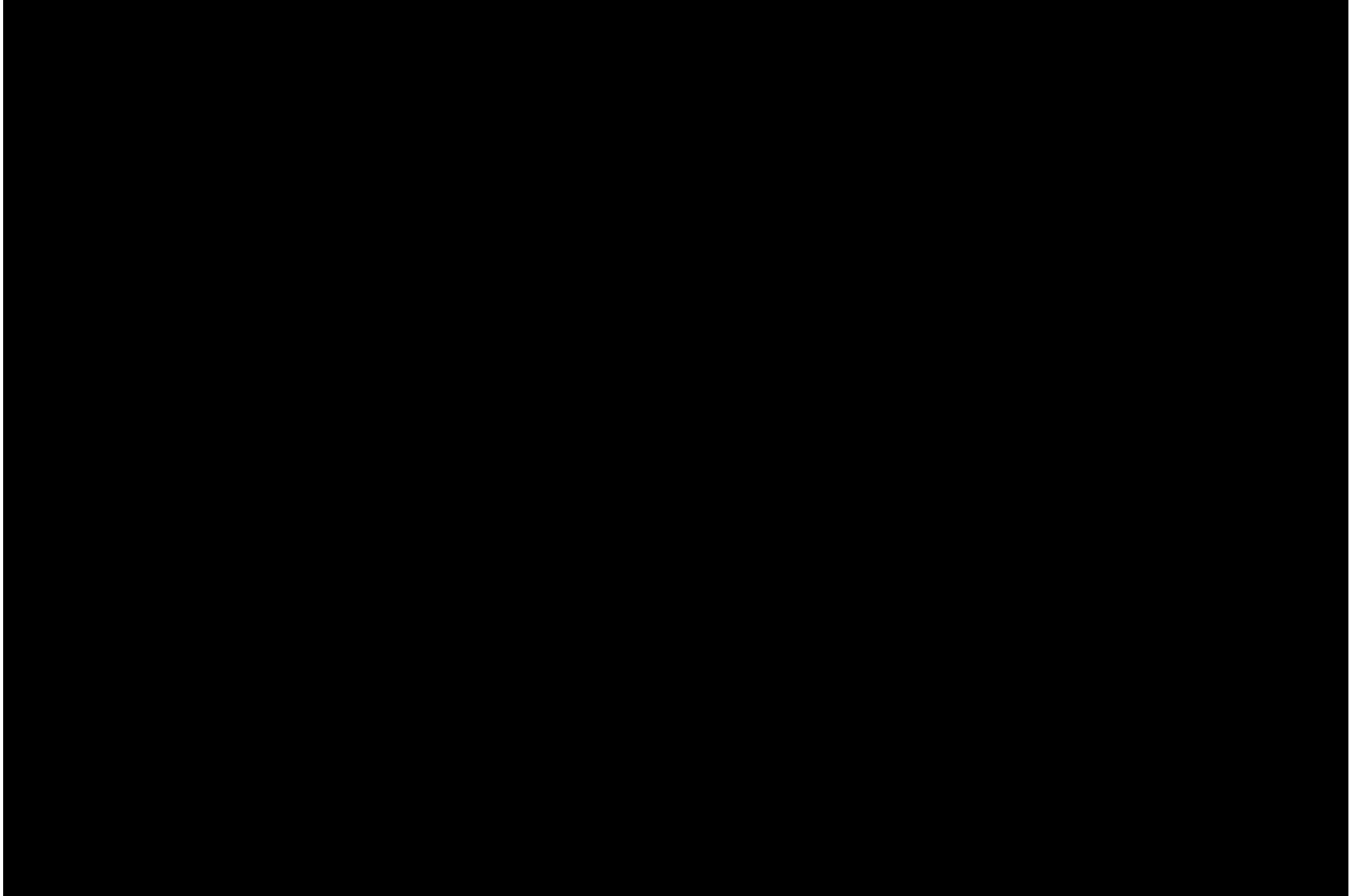
Bypassing



Bypassing



Bypassing



Bypassing



"How To Pwn and Protect Your Office Space" **by Dr. Tran** **Security B-Sides**

Bypassing



Bypassing



So, in conclusion...

Who's Behind Your Security?



Do Your Users Undermine Security?



Does Your Security Allow for Failure?



Does Your Security Allow for Failure?



Fail Happens



Fail Happens



Fail Happens



Fail Happens



Learn From Your Fail



Other Ways of Attacking the Pins

So really...what about...



?

Gerda Tytan Advertisement



Gerda Tytan ZX



Gerda Tytan ZX (Side View)



Gerda Tytan ZX (Rear View)



Gerda Tytan ZX (Removing the Shroud)



V.S.



FIGHT !!

Gerda Tytan ZX (Shroud Removed)



Vertical Mill Wins!

Gerda Tytan ZX (Has No Clothes)



Gerda Tytan ZX (Removing the Pins)

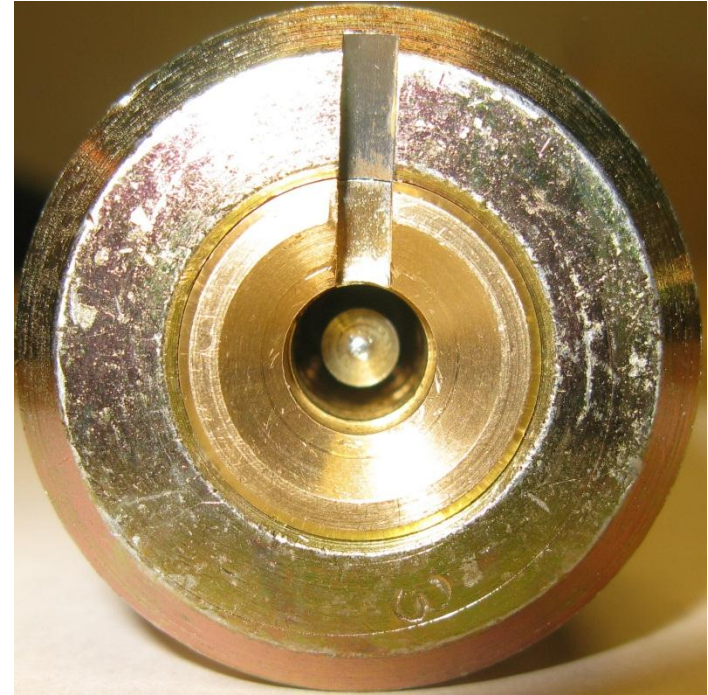


V.S.

FIGHT !!

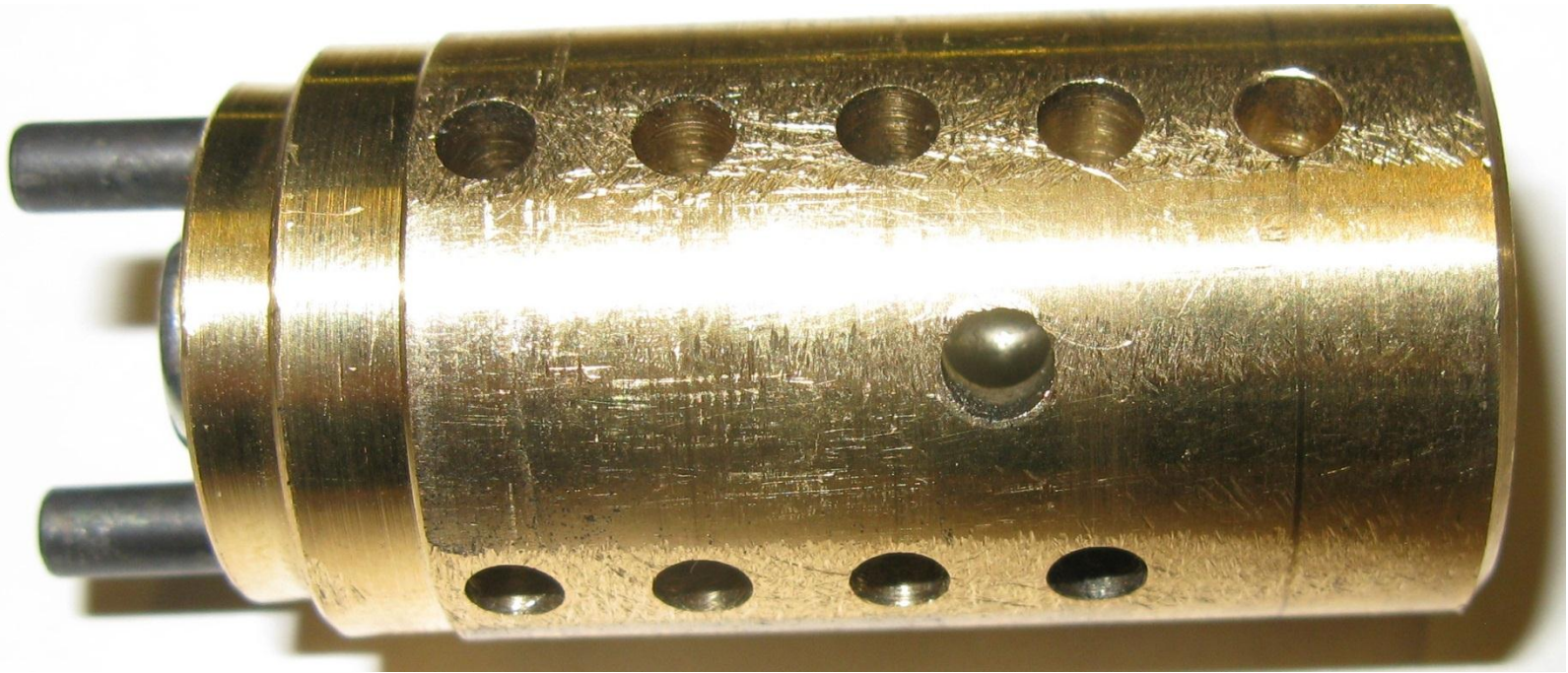


Gerda Tytan ZX (Pins Removed)

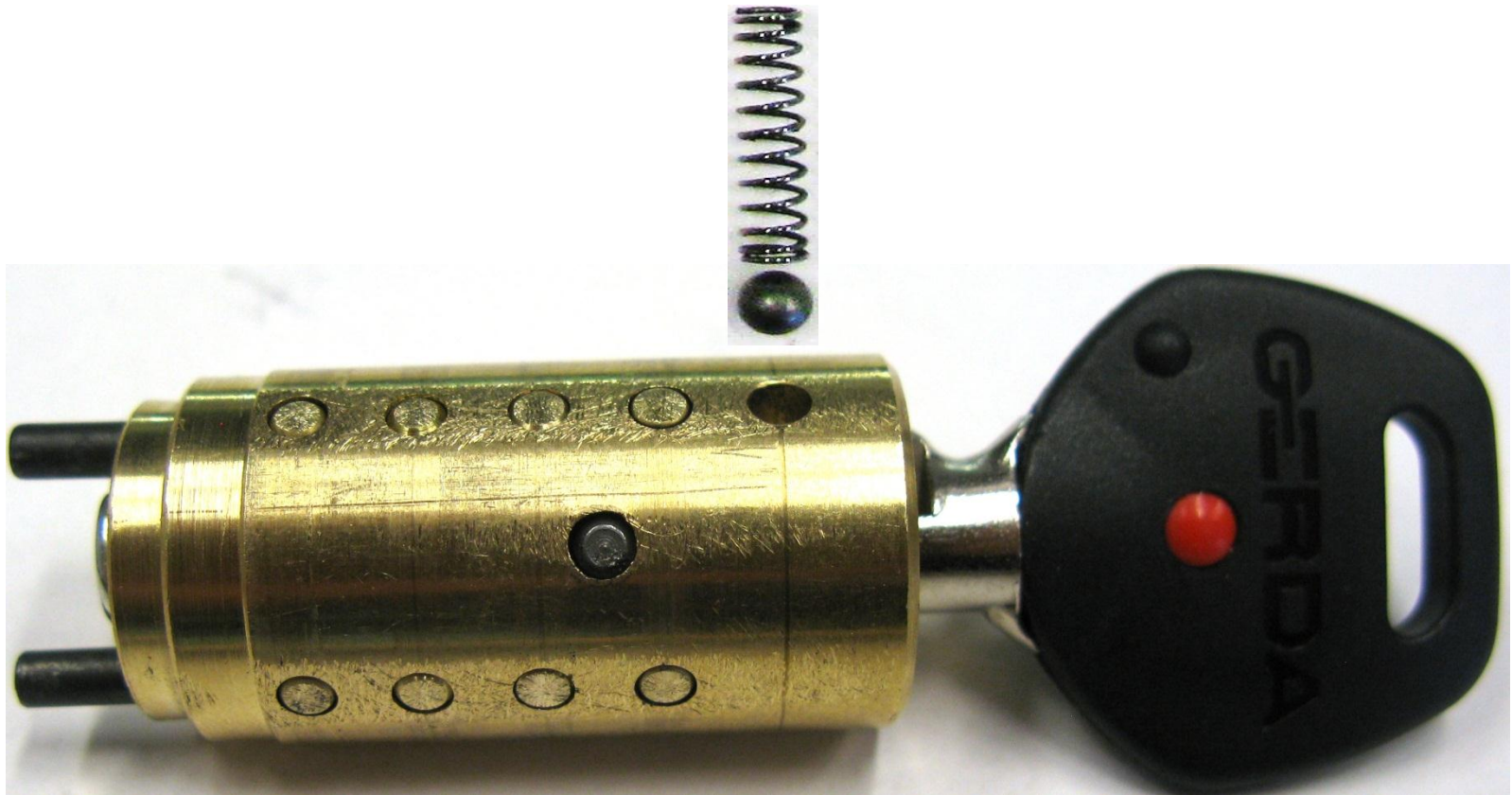


Drill Press Wins!

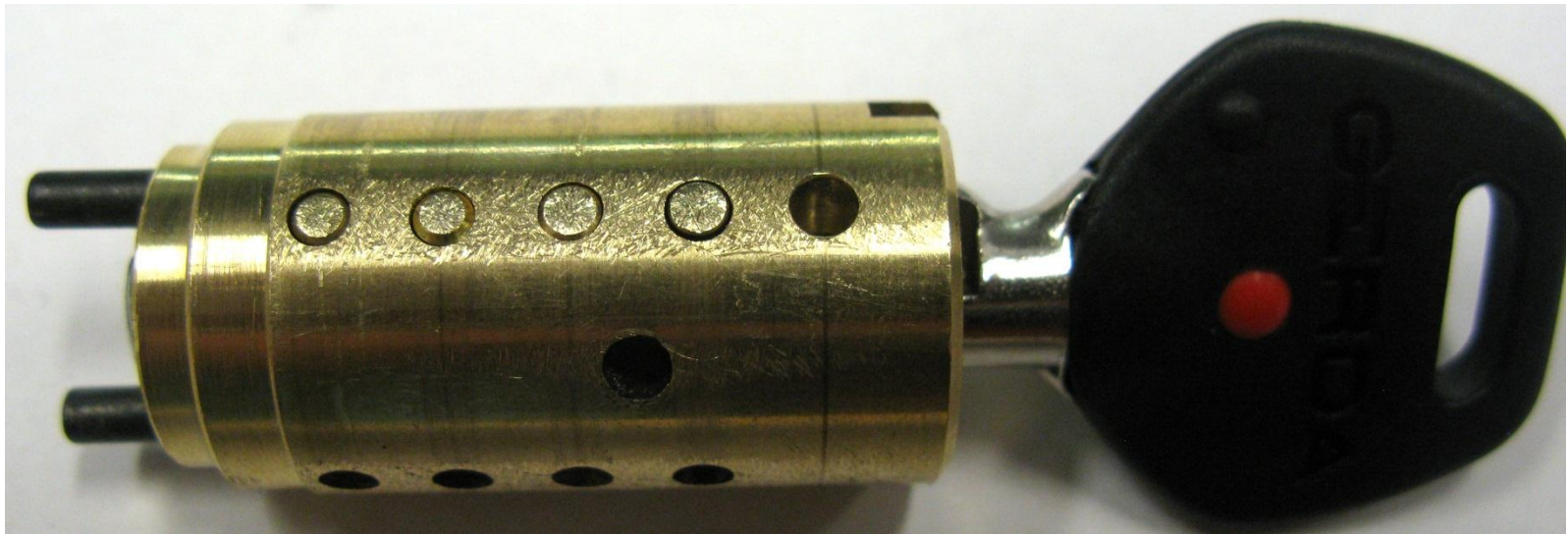
Gerda Tytan ZX Plug (No Pins)



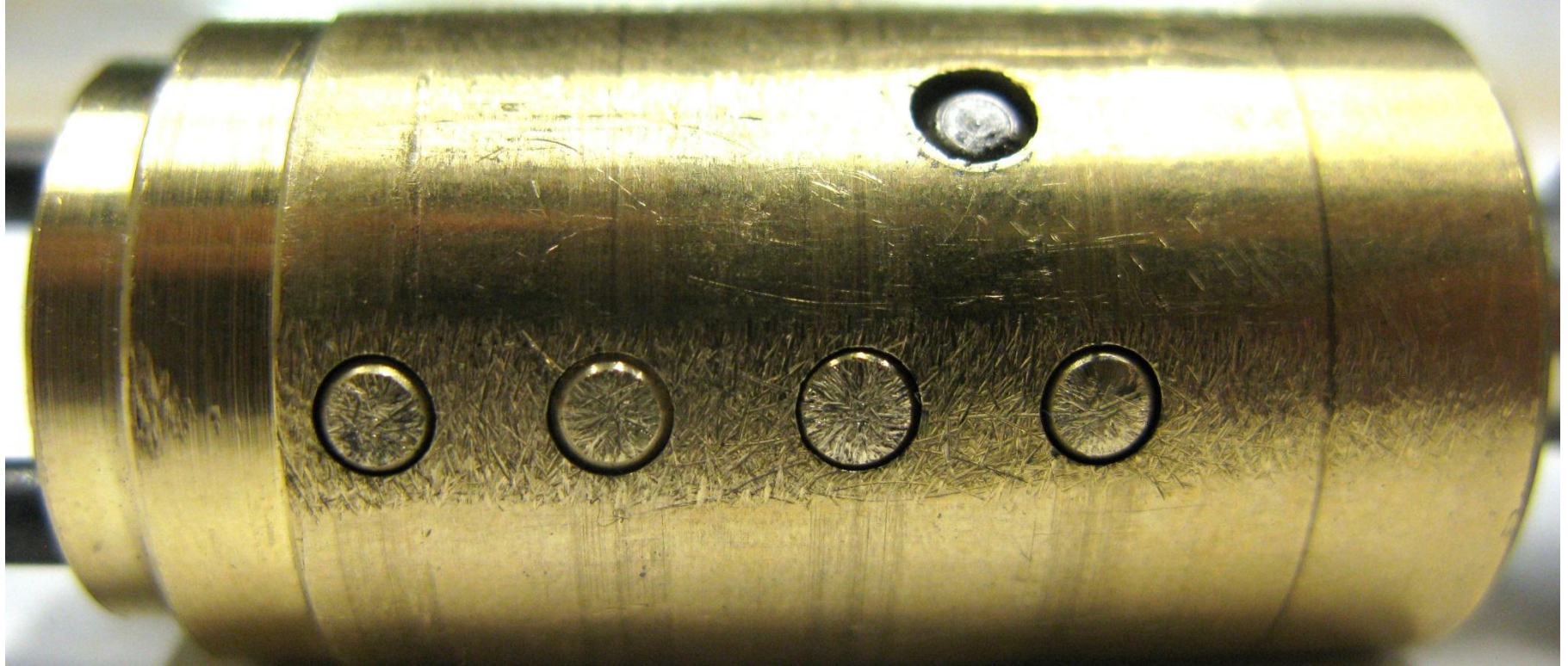
Gerda Tytan ZX Plug (With Pins)



Gerda Tytan ZX Plug (With Pins)



Gerda Tytan ZX Plug (???)



Gerda Tytan ZX Plug (Sloppy Manufacturing)



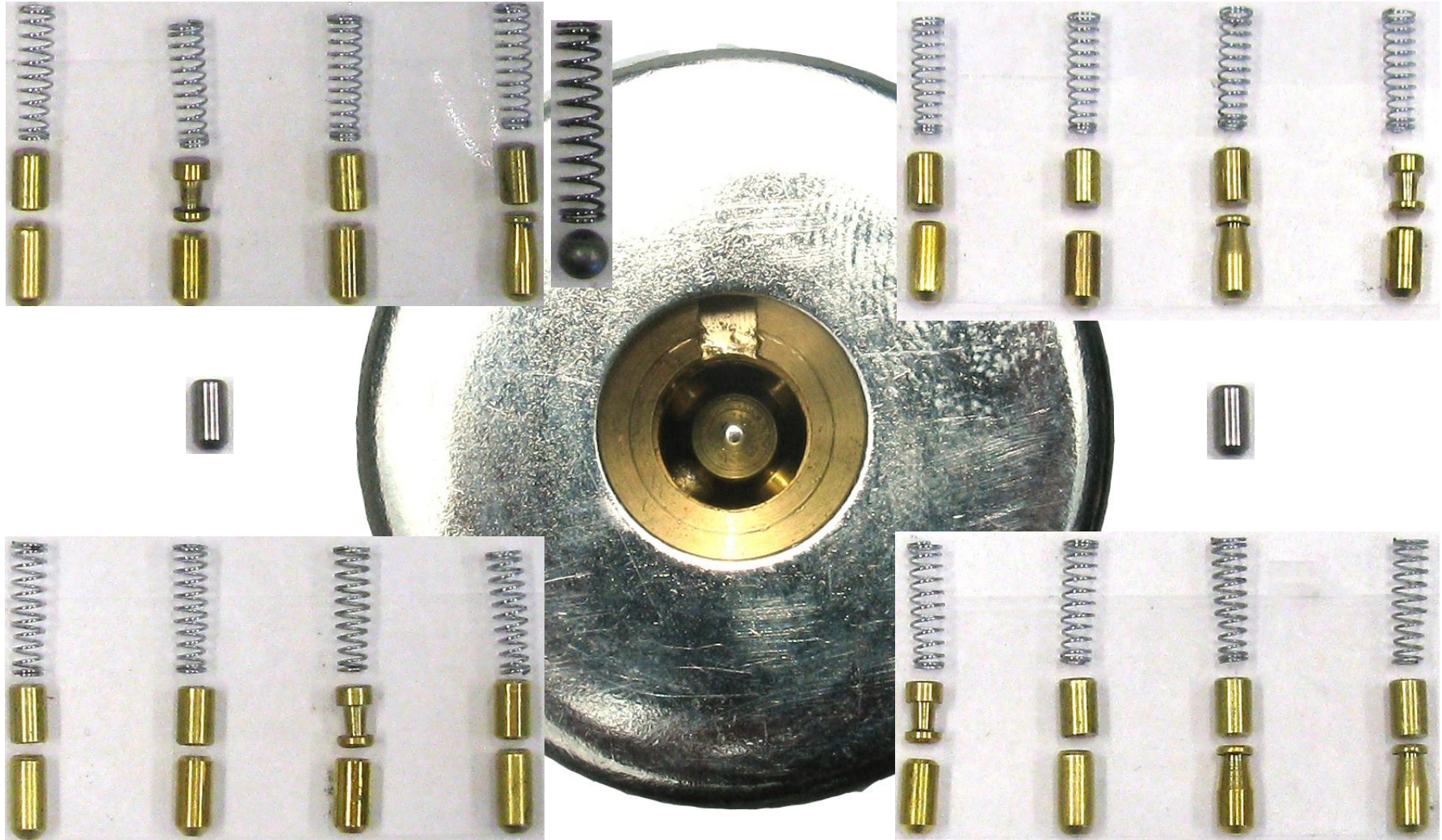
+



=



Gerda Tytan Rearranging Pins, Polish-style



Gerda Tytan ZX (Pick Tools)

So can you pick it?

Talk to me in a few months.



Thank you very much.



<http://deviating.net>

<http://enterthecore.net>

<http://toool.us>



this presentation is CopyLeft by Deviant Ollam. you are free to reuse any or all of this material as long as it is attributed and freedom for other s to do the same is maintained