Insider Master Key Attacks: Real World EoP

Matt Burrough

@mattburrough

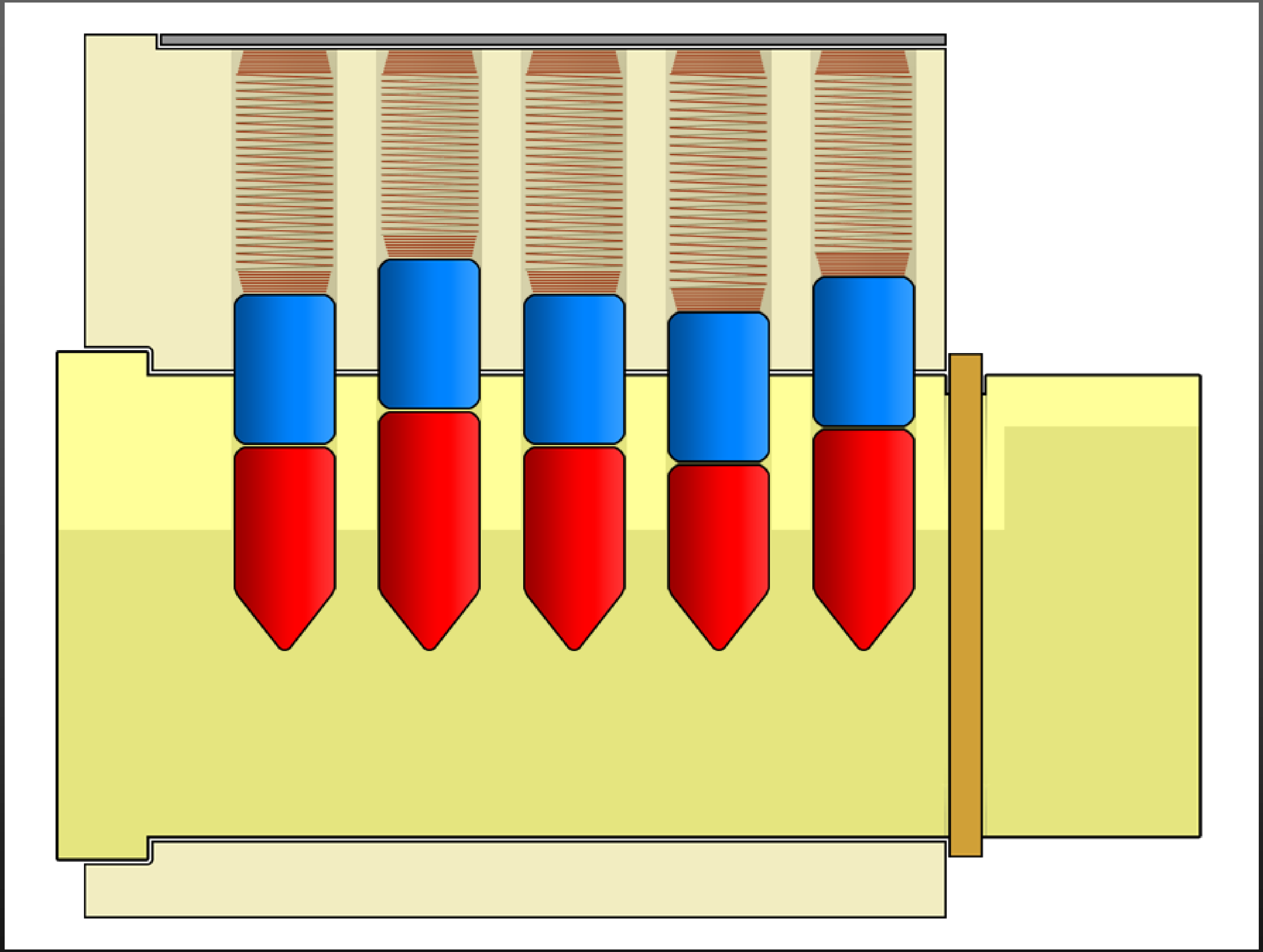
Who is Matt?

- Corporate Pen. Tester/Red Team
- Lock Sport Hobbyist
- Author: Pentesting Azure Applications, No Starch Press, 2018
  https://tinyurl.com/nspazure

How Master Keys Work

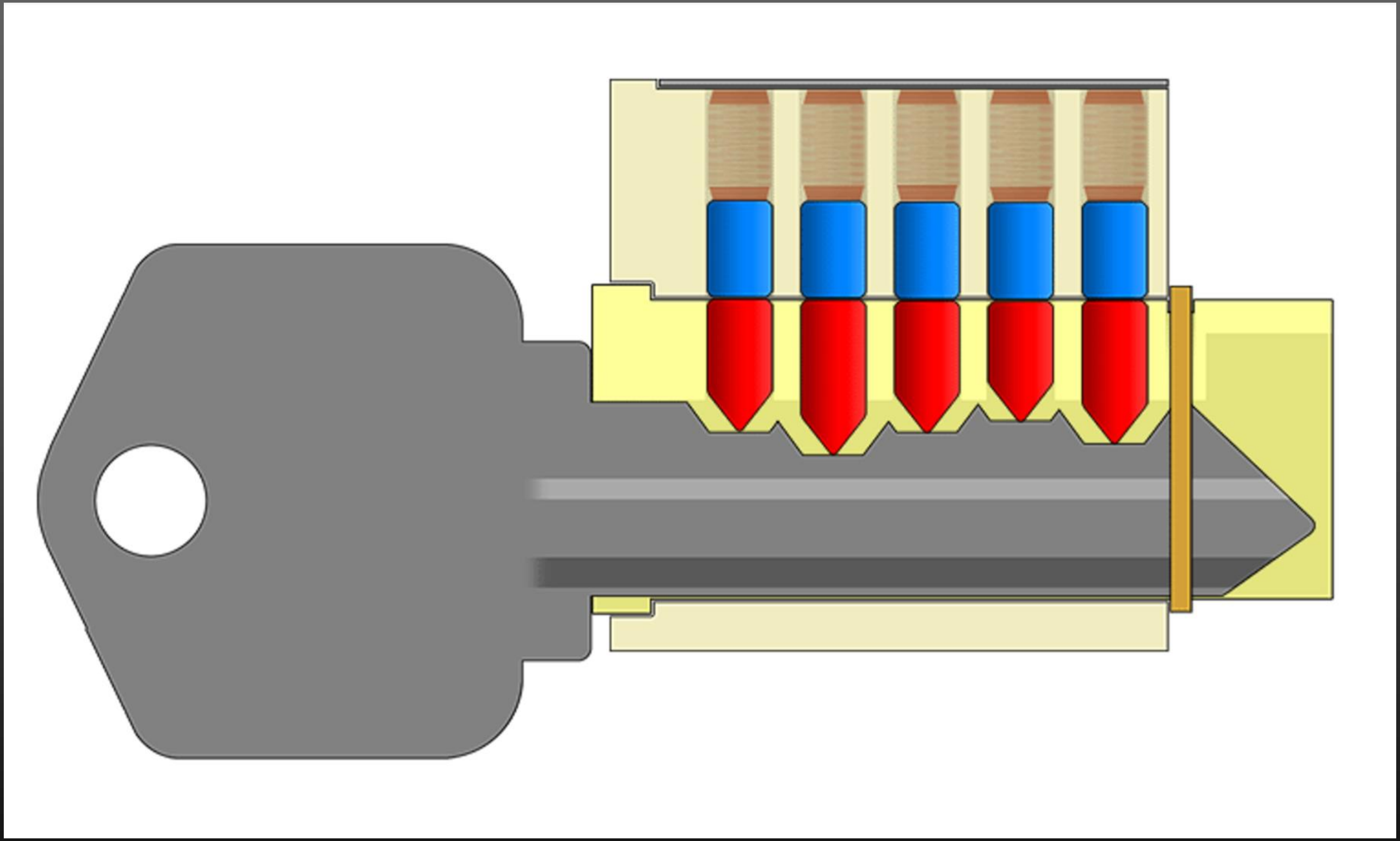
A Brief Overview

Pin Stacks



Slide courtesy Deviant Ollam
https://deviating.net/lockpicking/slides/keys_to_the_kingdom.pptx

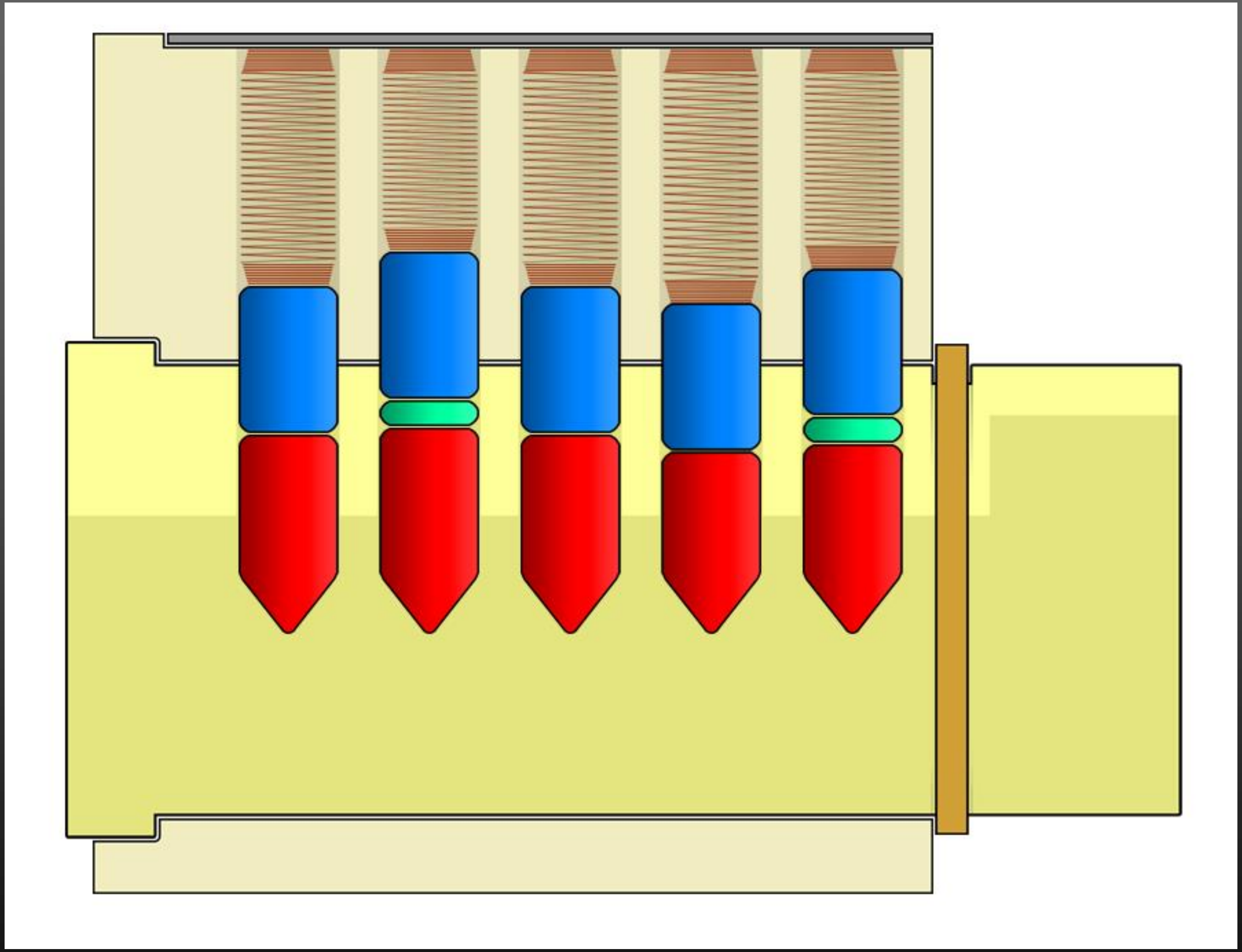
Using the Correct Key



Slide courtesy Deviant Ollam

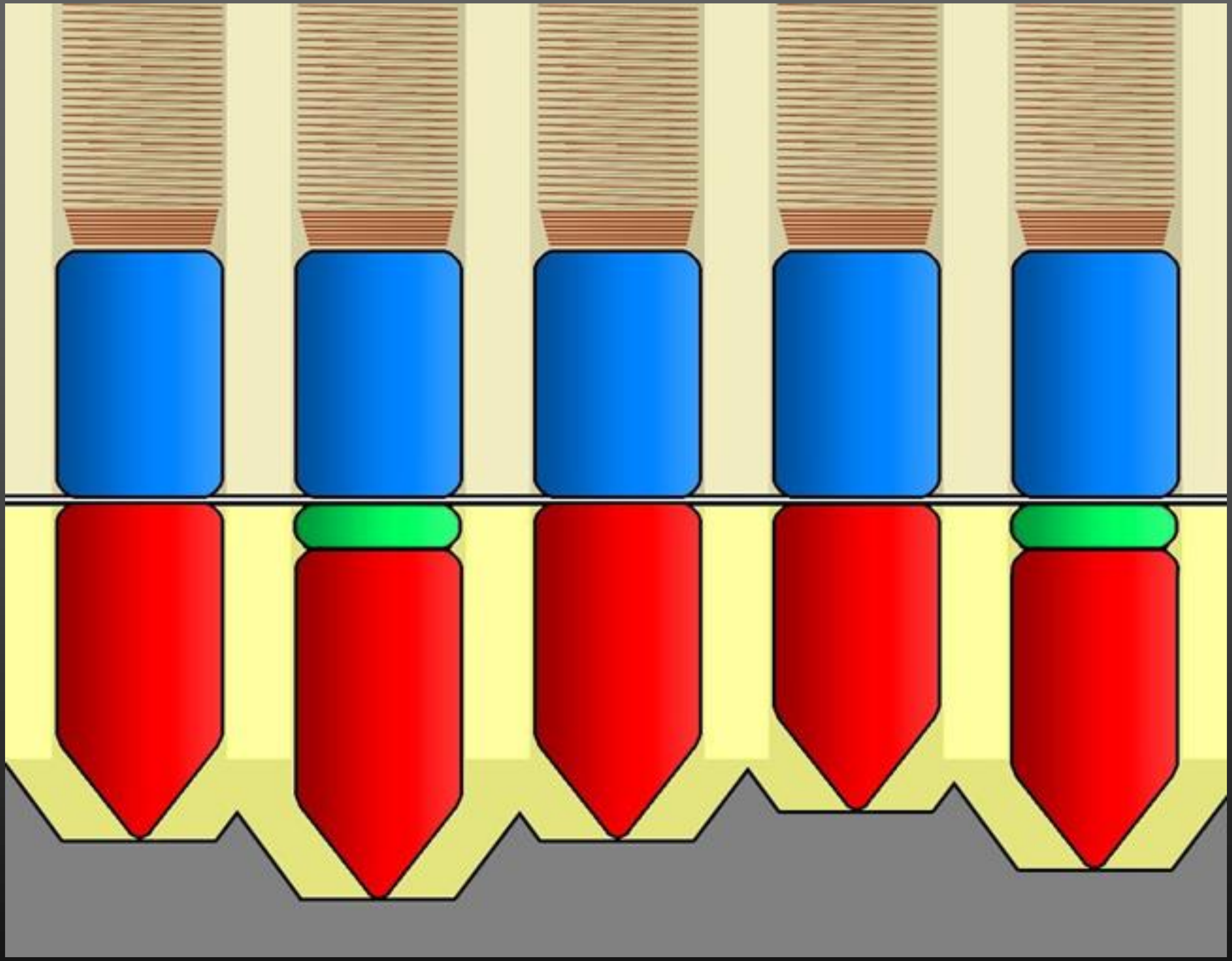
https://deviating.net/lockpicking/slides/keys_to_the_kingdom.pptx

Master-Keyed Systems



Slide courtesy Deviant Ollam
https://deviating.net/lockpicking/slides/keys_to_the_kingdom.pptx

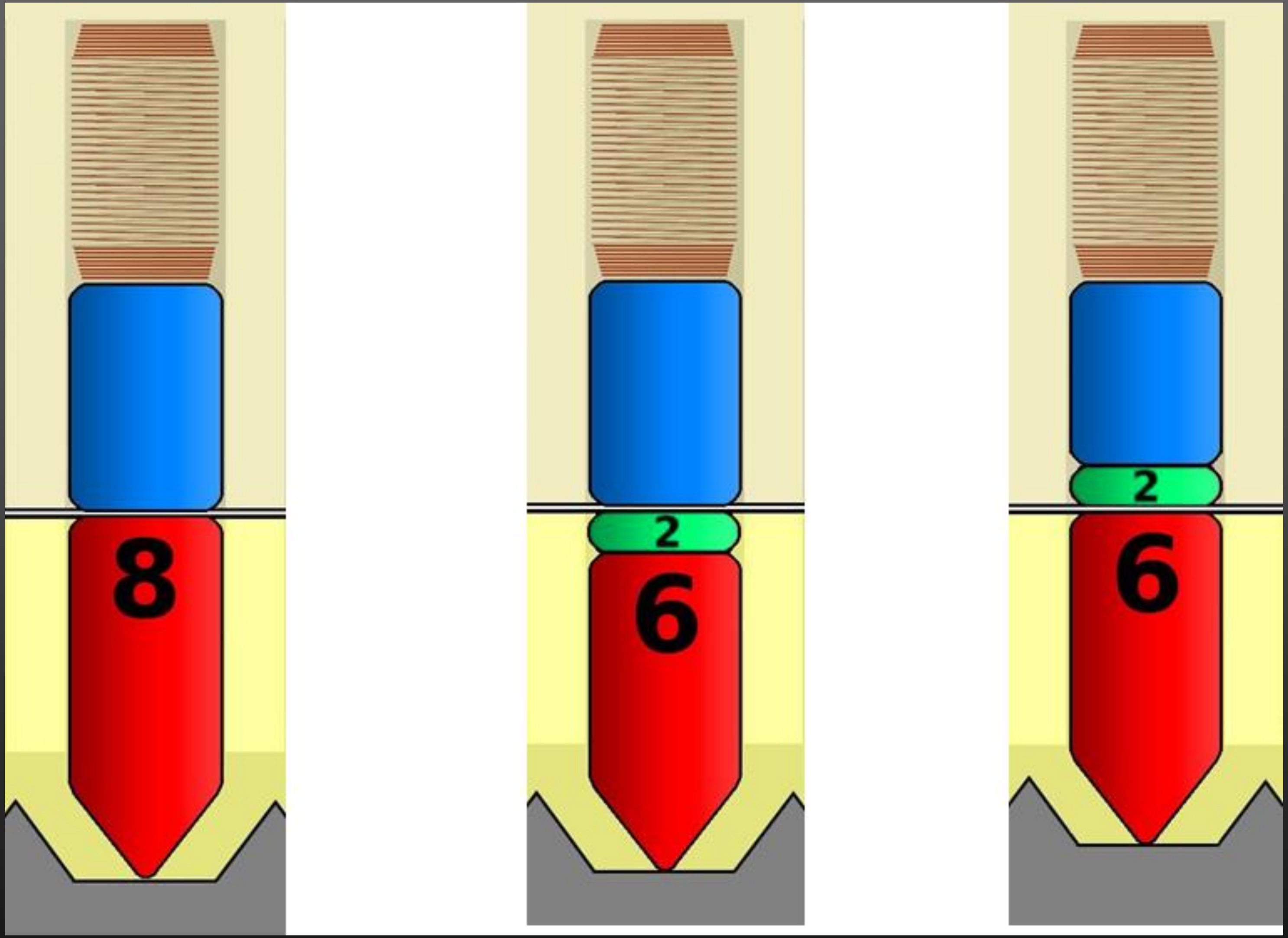
Master-Keyed Systems



Slide courtesy Deviant Ollam

https://deviating.net/lockpicking/slides/keys_to_the_kingdom.pptx

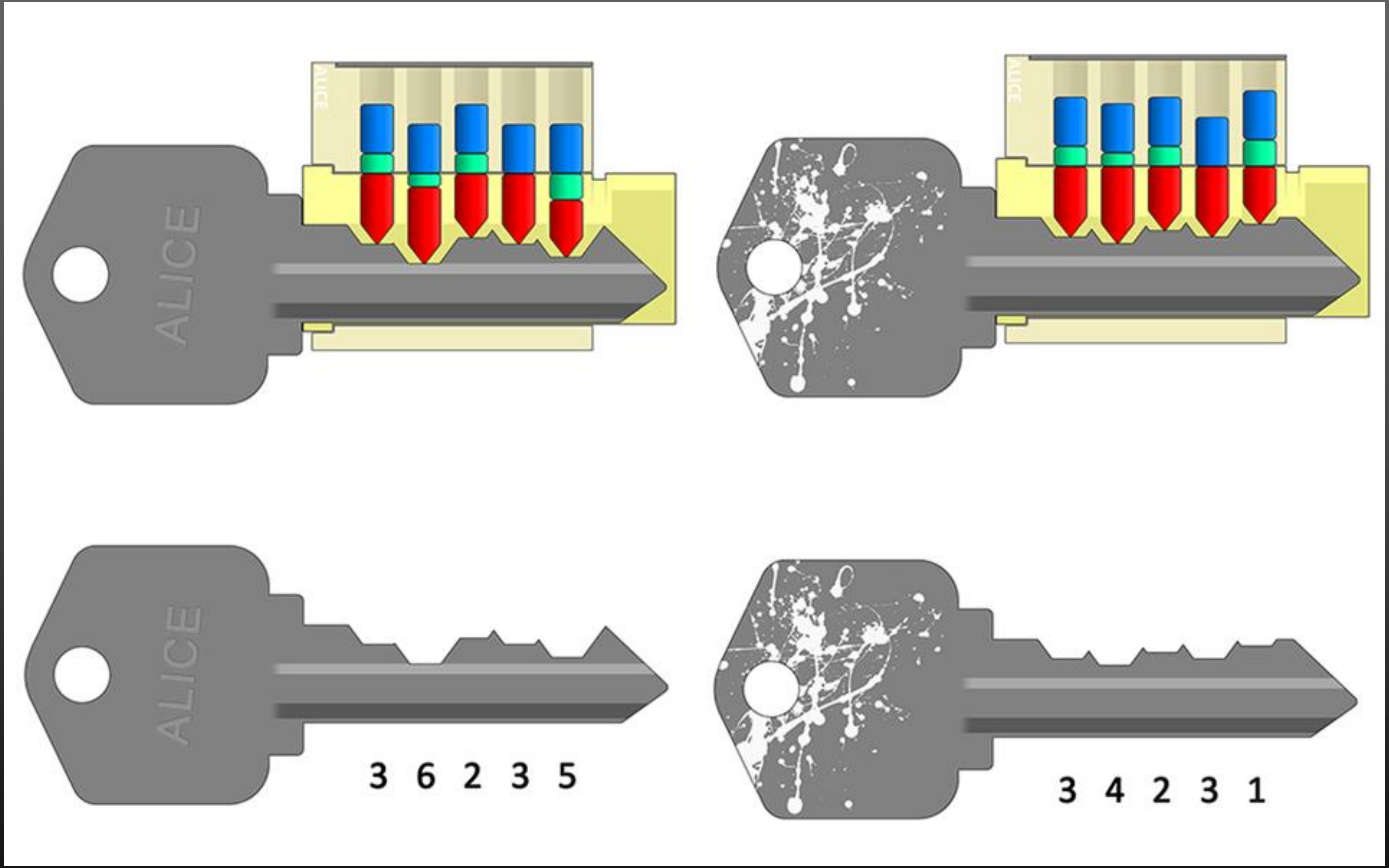
Master-Keyed Systems



Slide courtesy Deviant Ollam

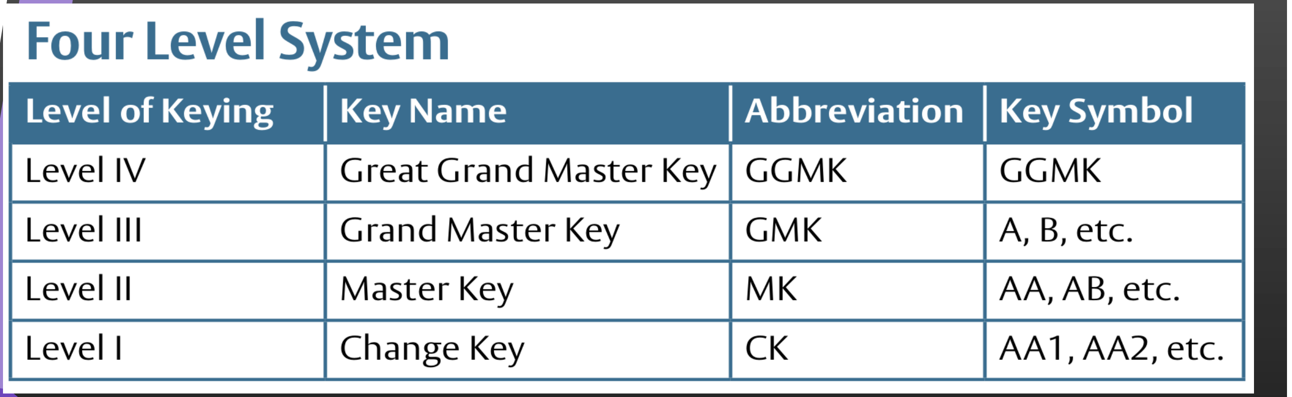
https://deviating.net/lockpicking/slides/keys_to_the_kingdom.pptx

Two Keys Opening the Same Lock



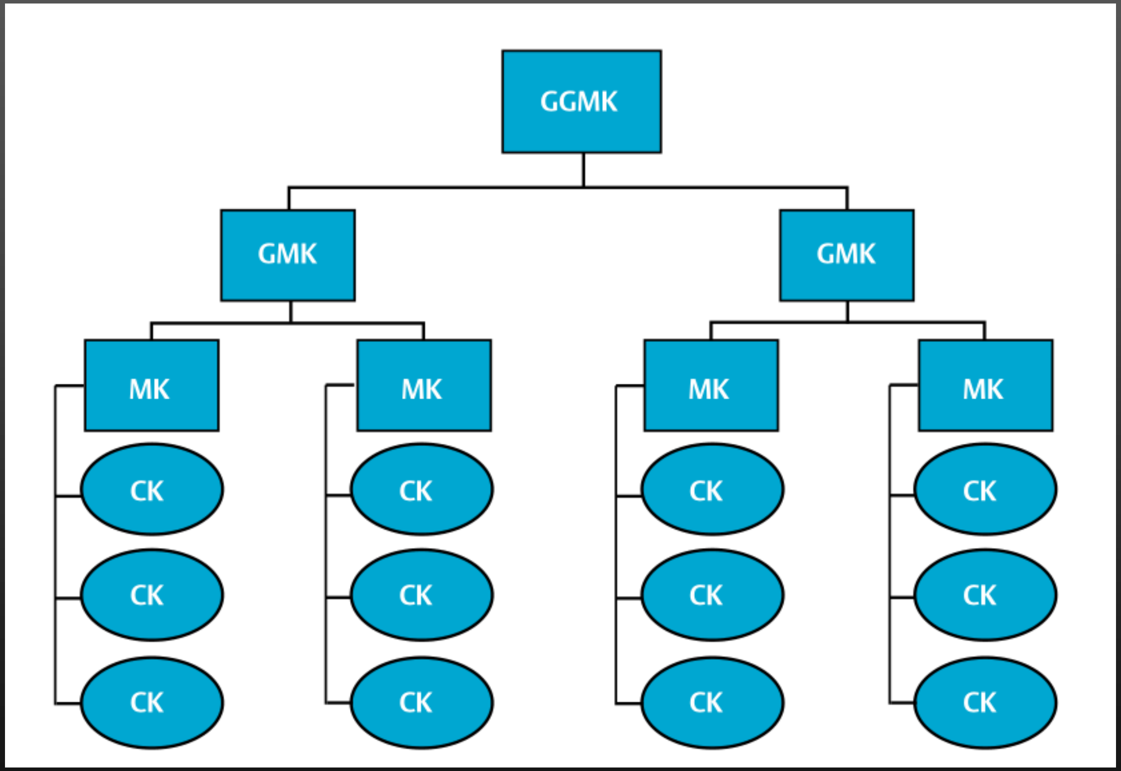
Slide courtesy Deviant Ollam
https://deviating.net/lockpicking/slides/keys_to_the_kingdom.pptx

Master Key Hierarchy



Four Level System

Level of Keying	Key Name	Abbreviation	Key Symbol
Level IV	Great Grand Master Key	GGMK	GGMK
Level III	Grand Master Key	GMK	A, B, etc.
Level II	Master Key	MK	AA, AB, etc.
Level I	Change Key	CK	AA1, AA2, etc.



“Master Key System Design Guide”

Master Key Example

Key	Bitting
Grand Master	8 3 0 1 8 3 6
Master B	6 7 0 1 8 3 6
SubMaster BA	6 7 8 3 8 3 6
Operator BA18	6 7 8 3 2 5 0
Operator BA23	6 7 8 3 4 7 0

Insider Attacks

Attack 1: Pick?

Advantages:

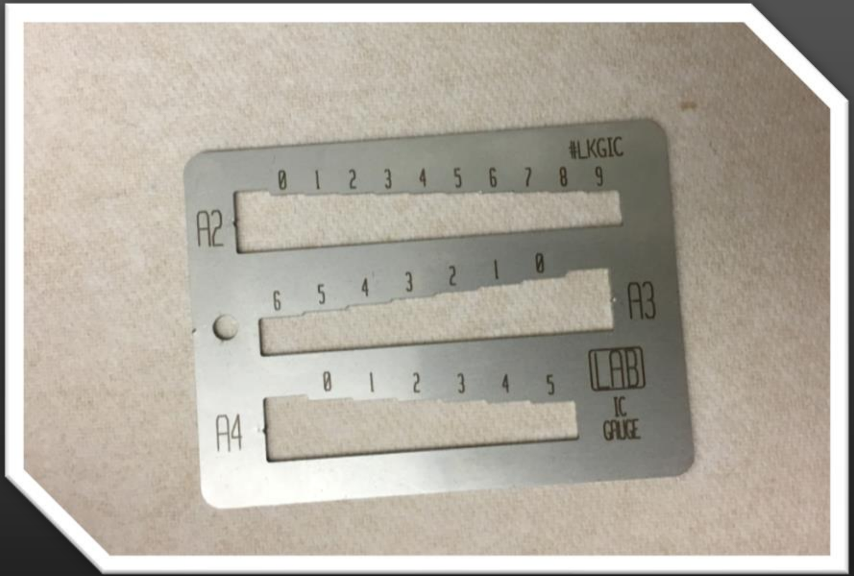
- The lock will open with any combination of master and operator positions being set
- SFICs often lack security pins
- Special turning tools to help pick to control…

Disadvantages:

- Setting pins to a mix of control positions and [master | operator] means the lock won't open
- SFICs often have 6 or even 7 pins
- Some have other security features, like additional pins on a different plane

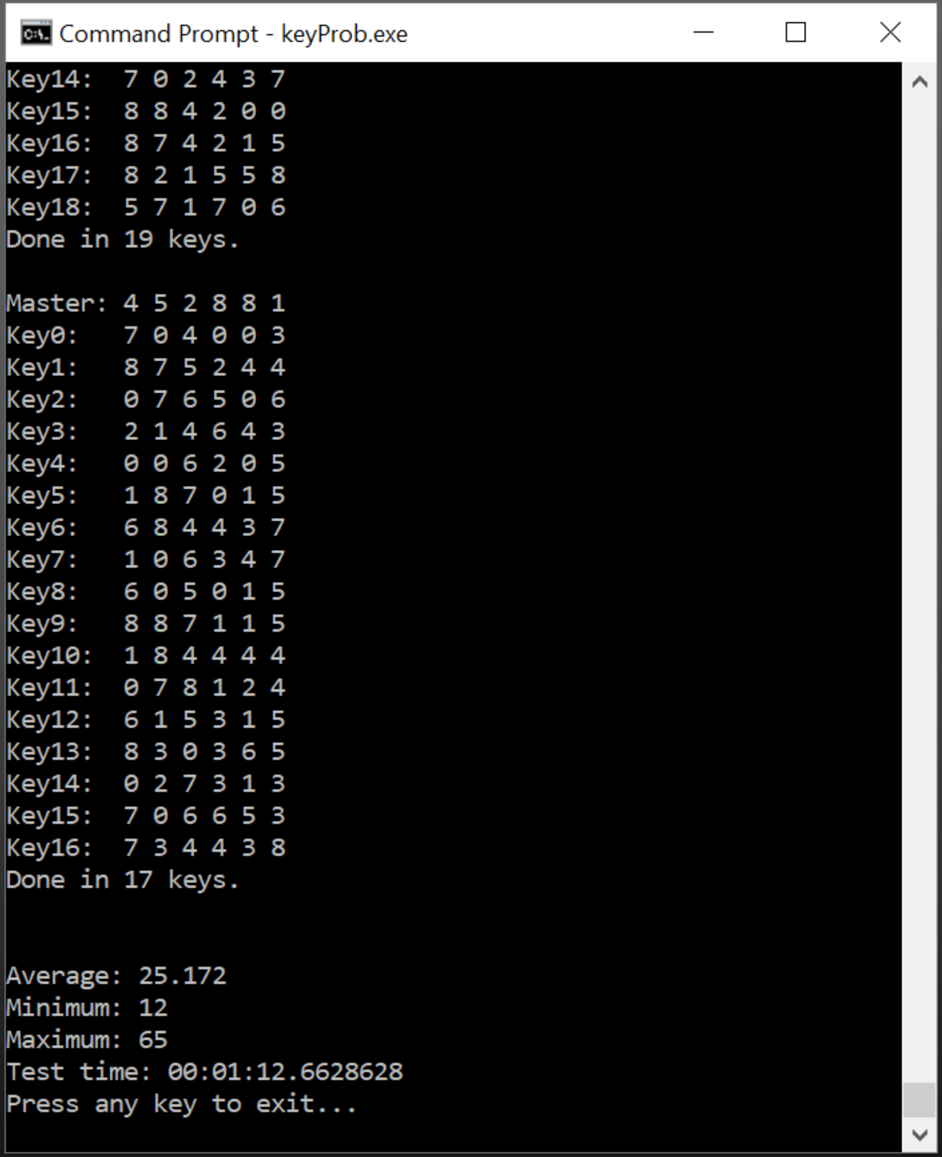
In practice, even skilled pickers can get hung up on SFICs.

Attack 2: Social Engineer / Co-Conspirators



- Per spec: No cut on an operator key should collide with master key bitting!

How many keys do we need?



```
Key14:  7 0 2 4 3 7
Key15:  8 8 4 2 0 0
Key16:  8 7 4 2 1 5
Key17:  8 2 1 5 5 8
Key18:  5 7 1 7 0 6
Done in 19 keys.

Master: 4 5 2 8 8 1
Key0:   7 0 4 0 0 3
Key1:   8 7 5 2 4 4
Key2:   0 7 6 5 0 6
Key3:   2 1 4 6 4 3
Key4:   0 0 6 2 0 5
Key5:   1 8 7 0 1 5
Key6:   6 8 4 4 3 7
Key7:   1 0 6 3 4 7
Key8:   6 0 5 0 1 5
Key9:   8 8 7 1 1 5
Key10:  1 8 4 4 4 4
Key11:  0 7 8 1 2 4
Key12:  6 1 5 3 1 5
Key13:  8 3 0 3 6 5
Key14:  0 2 7 3 1 3
Key15:  7 0 6 6 5 3
Key16:  7 3 4 4 3 8
Done in 17 keys.


Average: 25.172
Minimum: 12
Maximum: 65
Test time: 00:01:12.6628628
Press any key to exit...
```

- Per spec: No cut on an operator key should collide with Master key bitting
- So we just need enough keys to eliminate all other positions for each pin stack
- https://burrough.org/archives/66
  - https://github.com/mburrough/MasterKeySim

How would we ever see that many keys?

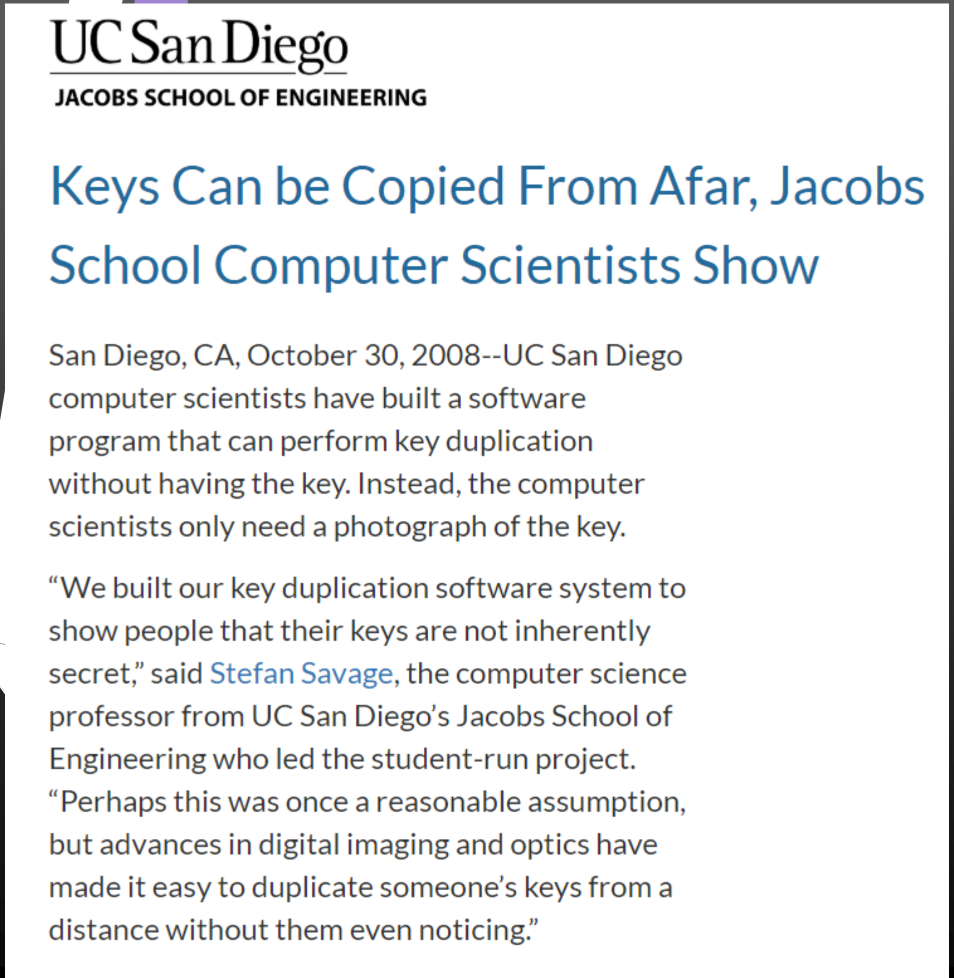
Land a Semi-Privileged Role

- Is everyone who handles multiple keys highly trusted?
- Think about key management:
  - New Employees
  - Office Moves
  - Broken/Lost Key Replacement
  - Departing Employees

Social Engineering

- “I left my key at home. I heard that some of our offices use the same key. Can I see if yours works in my door?”
- “Did you ever notice that mark on our keys?”
- “You’re busy, let me help carry that stuff.”

Long Distance Photography

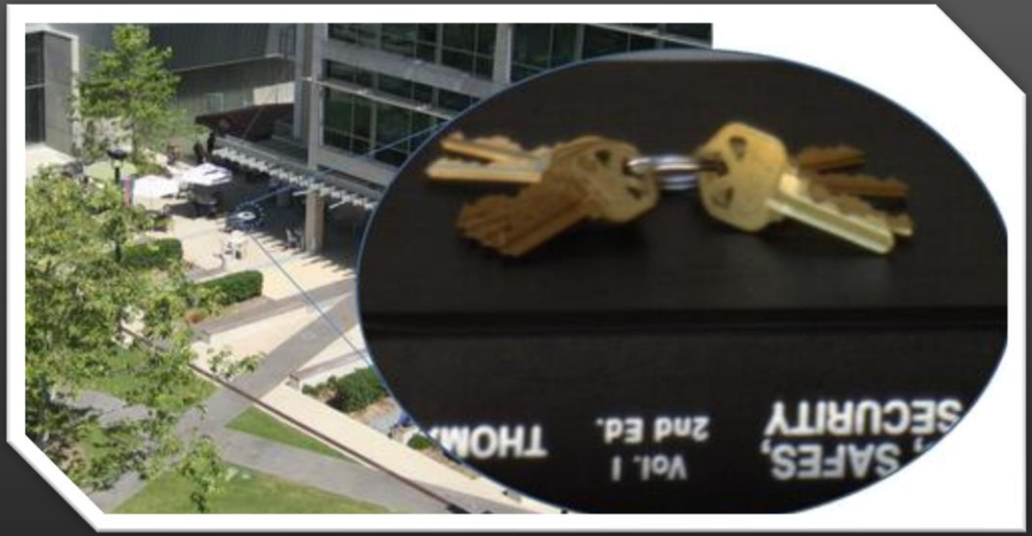


UC San Diego
JACOBS SCHOOL OF ENGINEERING

Keys Can be Copied From Afar, Jacobs School Computer Scientists Show

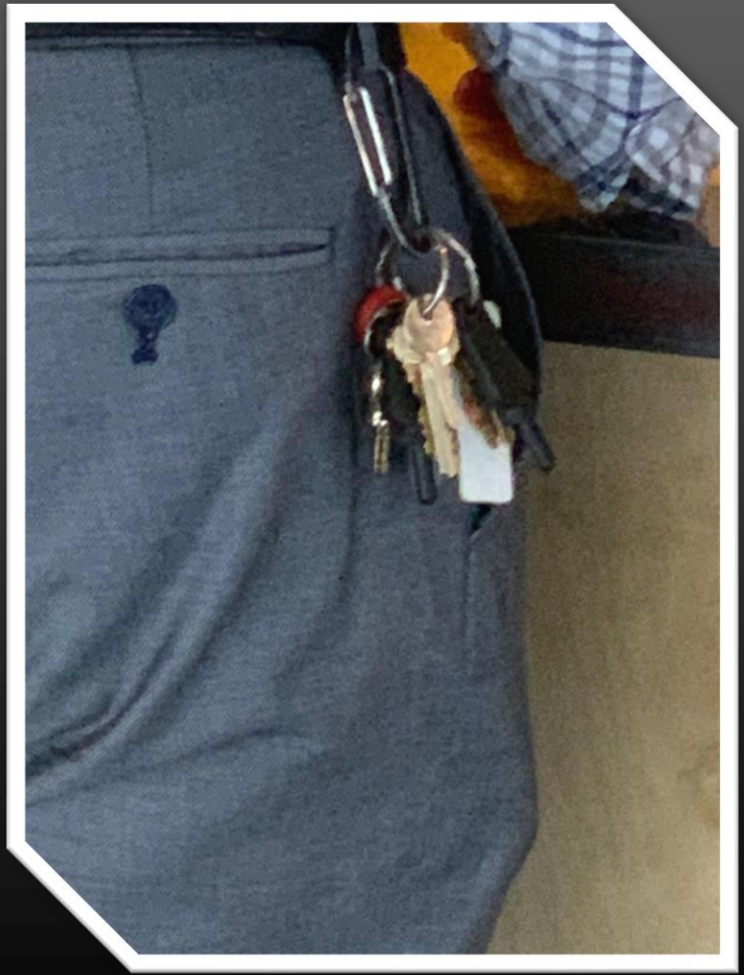
San Diego, CA, October 30, 2008--UC San Diego computer scientists have built a software program that can perform key duplication without having the key. Instead, the computer scientists only need a photograph of the key.

"We built our key duplication software system to show people that their keys are not inherently secret," said Stefan Savage, the computer science professor from UC San Diego's Jacobs School of Engineering who led the student-run project. "Perhaps this was once a reasonable assumption, but advances in digital imaging and optics have made it easy to duplicate someone's keys from a distance without them even noticing."



https://www.jacobsschool.ucsd.edu/news/news_releases/release.sfe?id=791

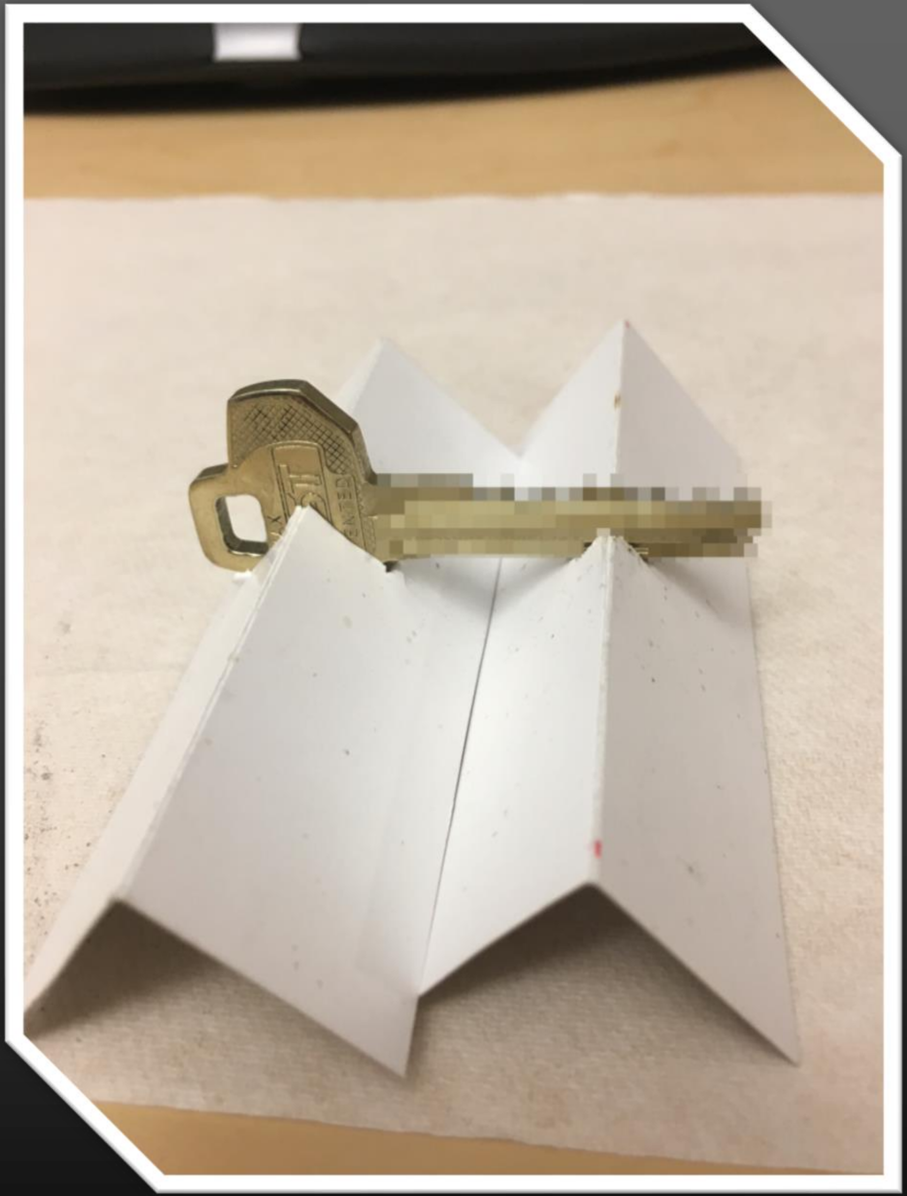
Attack 3: Hello, Security?



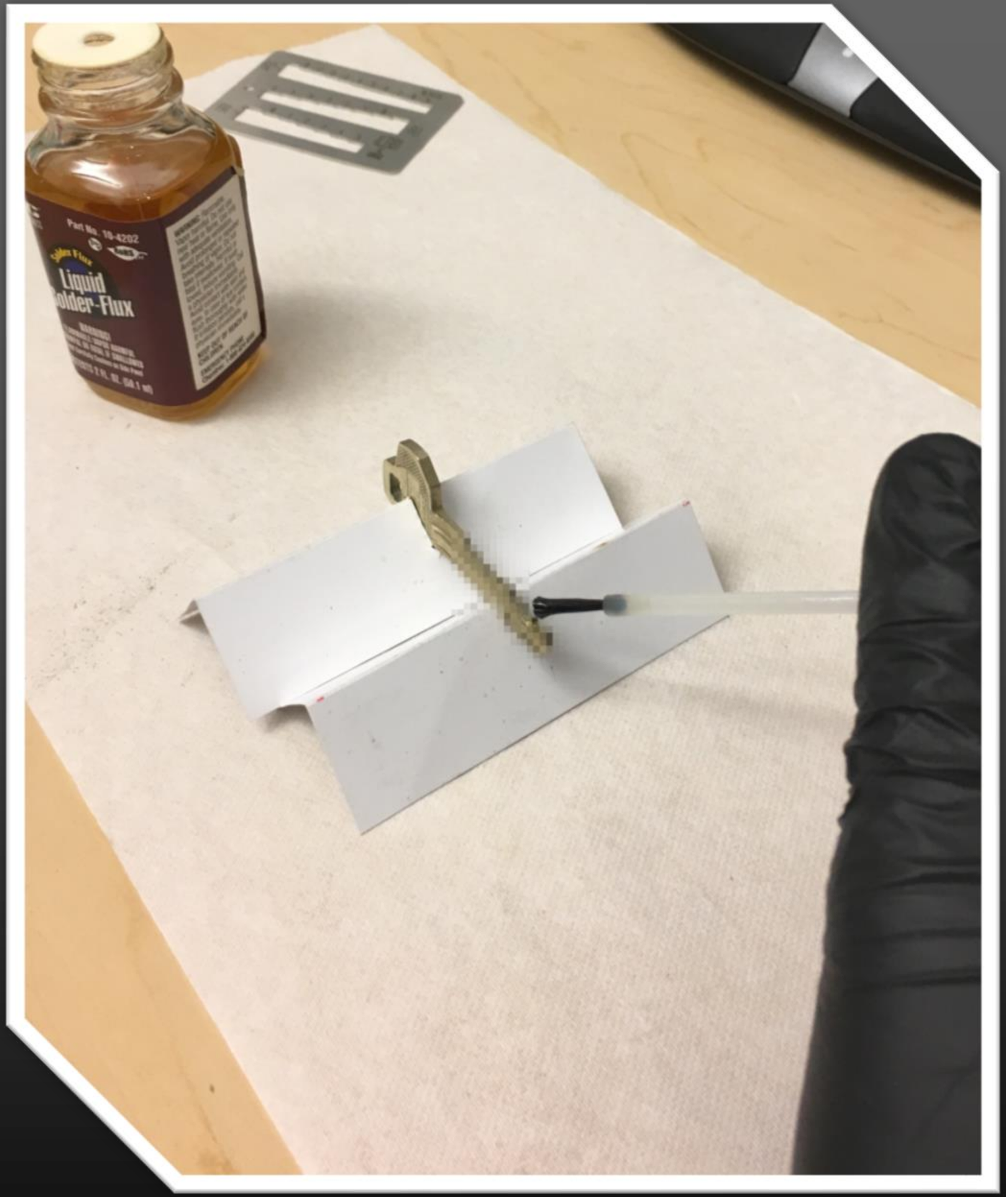
Attack 4: Fill & File

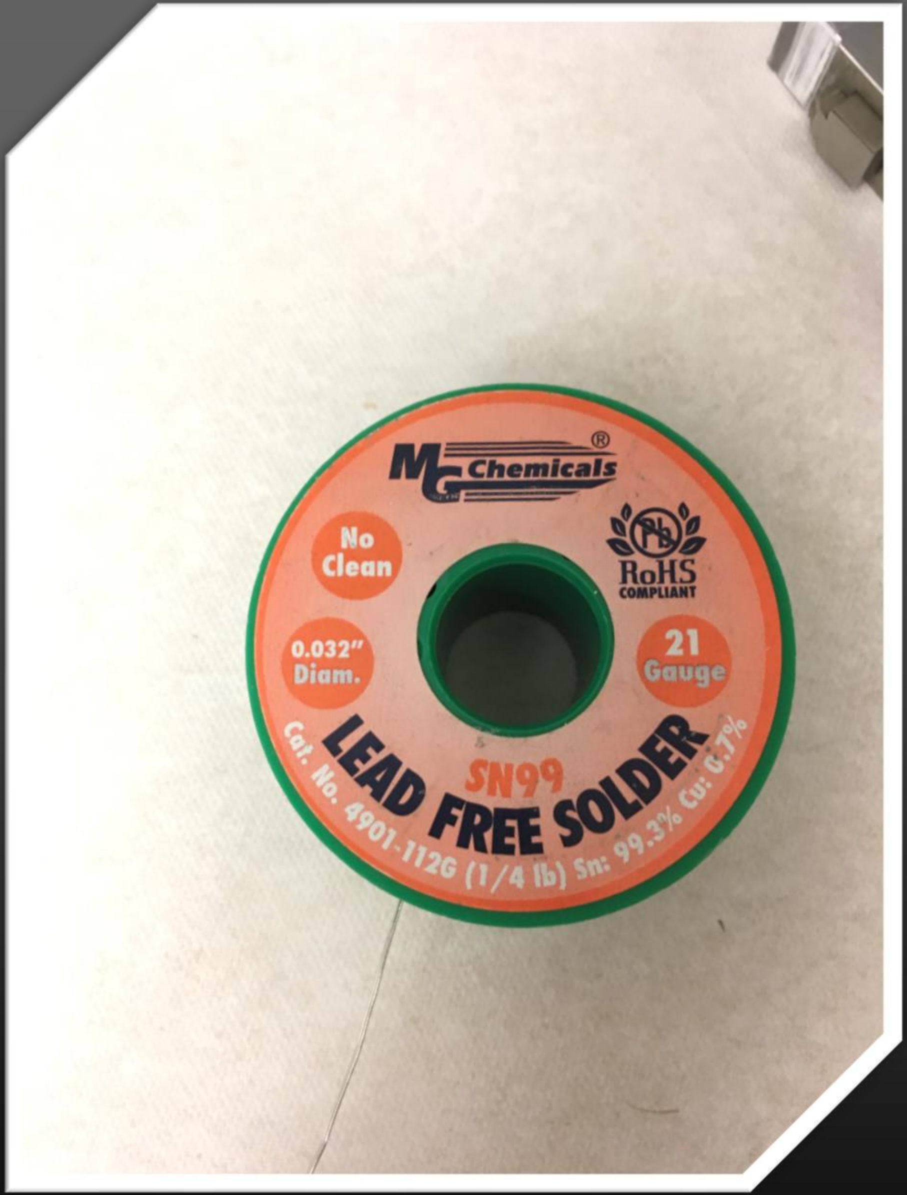
- If no operator cut can collide with a master cut – we should be able to:
  - Take a blank, cut it to all operator depths except one position
  - Test the key with that position as a 0 cut
  - Cut/file to a 1 and retry…
  - Repeat for each depth
  - Repeat for each pin
  - Just need as many blanks as positions on the key (5, 6, maybe 7)

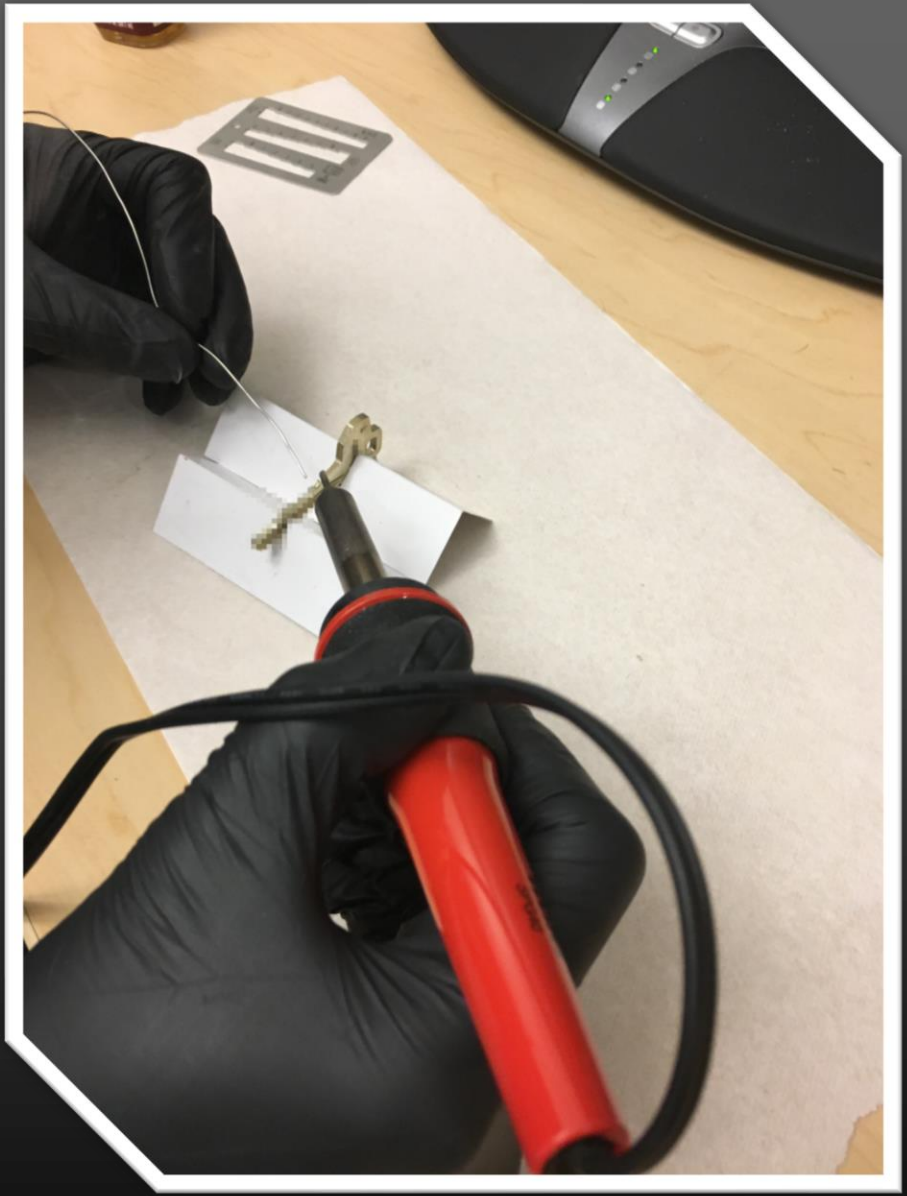
- *But*, what if we can't get blanks?!
- We could use an operator key…
  - What about positions where the operator key is cut deeper than the master?
  - **Solder!**



GC ELECTRONICS
Part No. 10-4202
Pb
RoHS
Solder Flux
Liquid Solder-Flux
WARNING!
FLAMMABLE/VAPOR HARMFUL
HARMFUL OR FATAL IF SWALLOWED
Read Carefully Cautions on Side Panel
CONTENTS 2 FL. OZ. (59.1 ml)


Part No. 10-4202
Solder Flux
Liquid
older-Flux


MG Chemicals®
No Clean
RoHS COMPLIANT
Pb
0.032" Diam.
21 Gauge
SN99
LEAD FREE SOLDER
Cat. No. 4901-112G (1/4 lb) Sn: 99.3% Cu: 0.7%



BEST
PATENTED

CORMAX
BEST
PATENTED

And we have a master key!

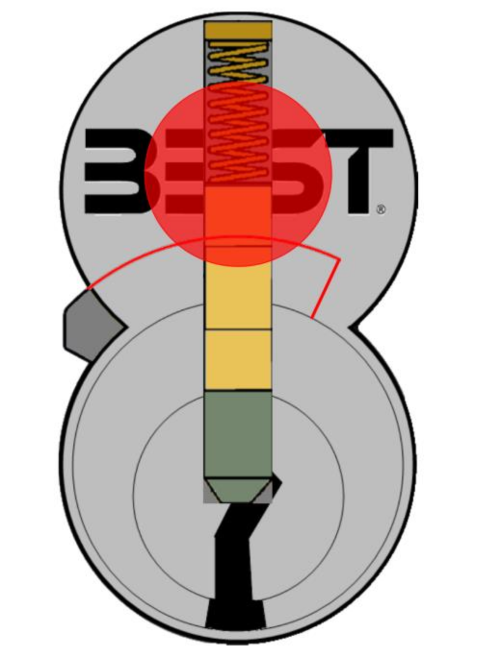
- It works!
- Looks almost as good as an impressioned key.
- Probably shouldn’t use everyday.
- Maybe carry a key extractor, too.
- This technique can’t be used to derive the control key.
    - How can we get one of those?

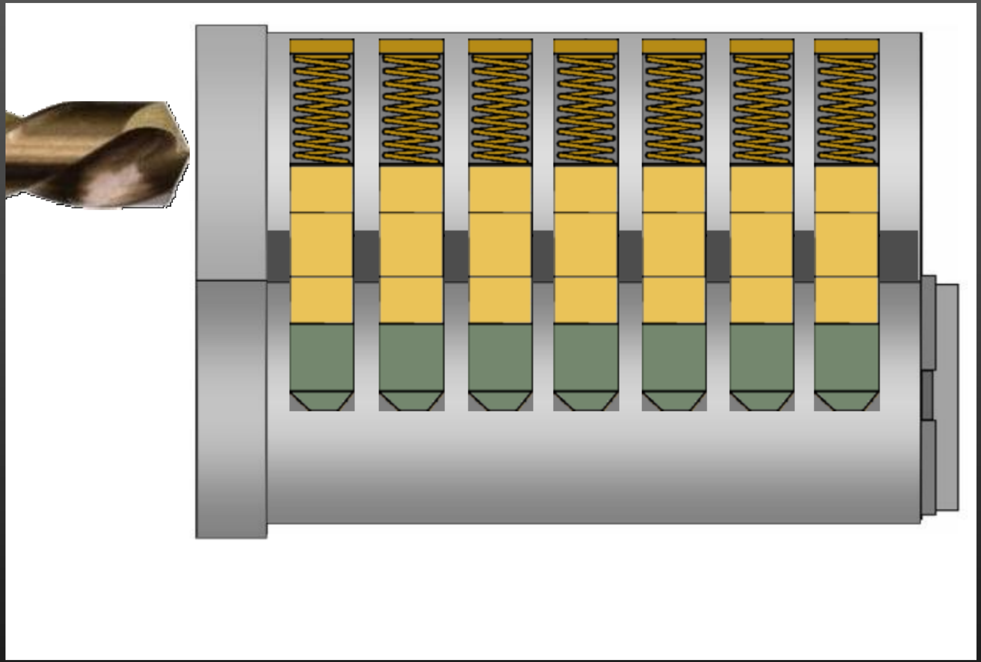
Attack 5: Steal a Lock and Measure Pins

https://majestycommercialroofing.com/junk-removal-services/
https://adelaideruralsalvage.com.au/windows-doors/#

Get access to core

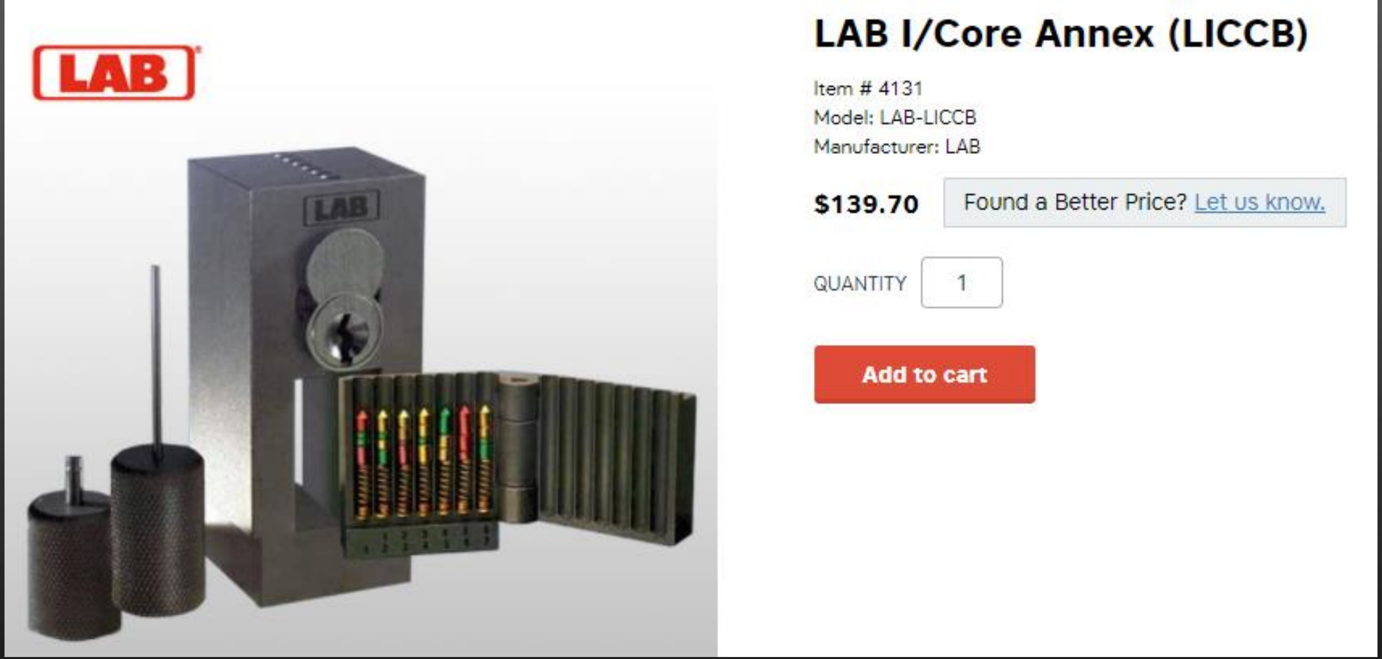
(Just don't follow the directions)





"BEST A2 & A4 Keys System Training"

Tools are expensive…



LAB I/Core Annex (LICCB)

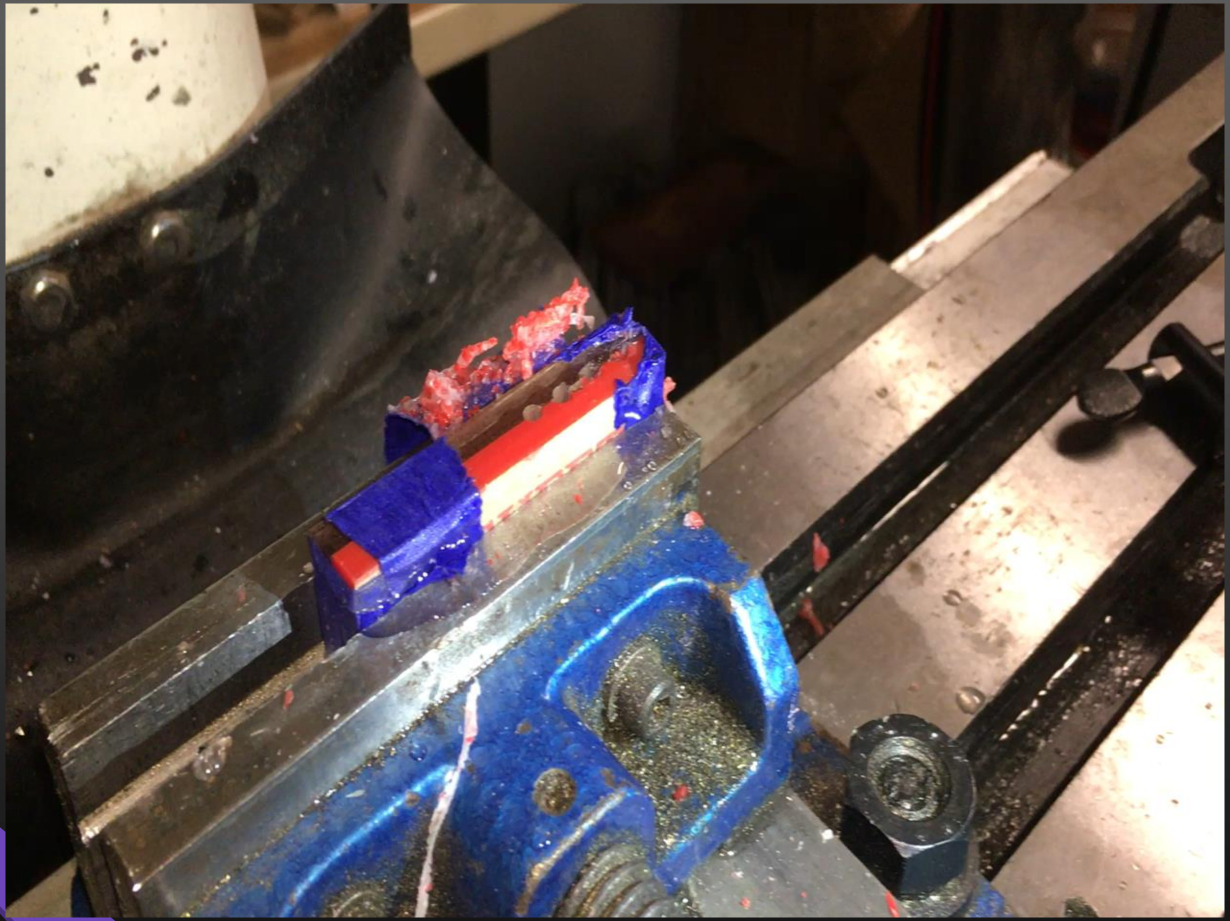
Item # 4131
Model: LAB-LICCB
Manufacturer: LAB

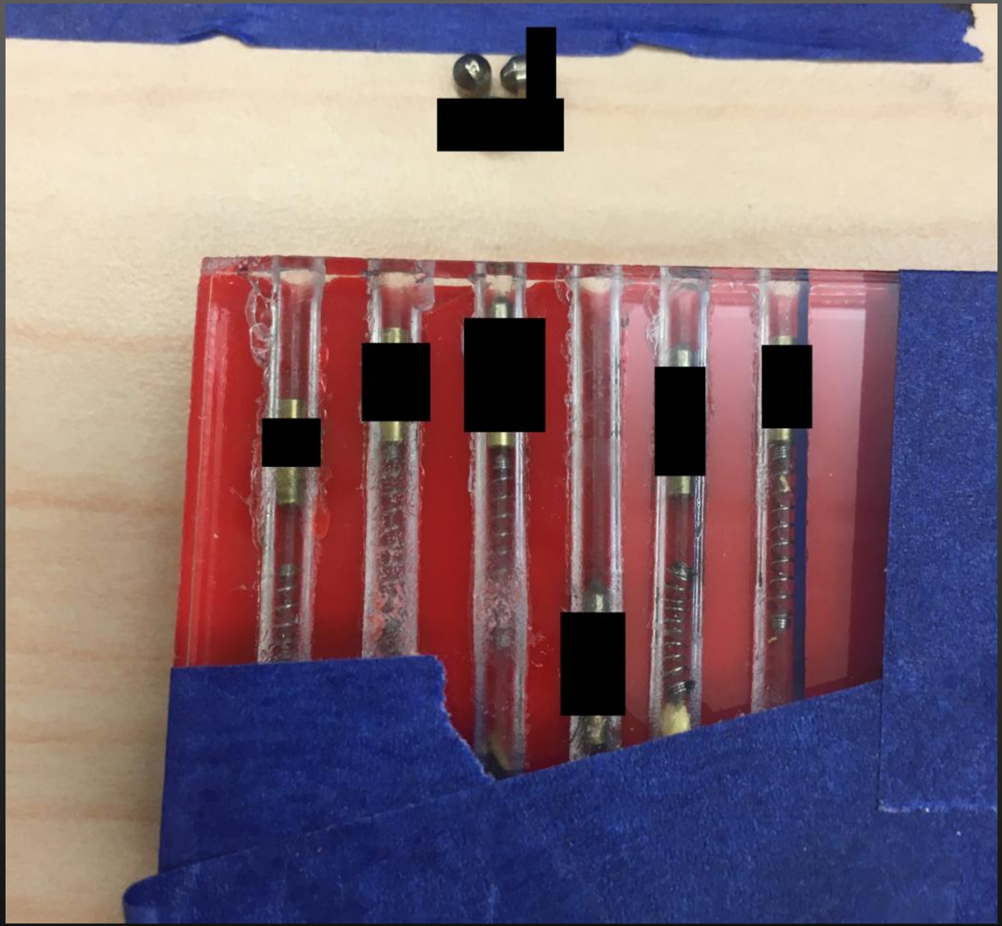
$139.70 Found a Better Price? Let us know.

QUANTITY 1

https://www.americankeysupply.com/product/lab-i-core-annex-liccb-4131

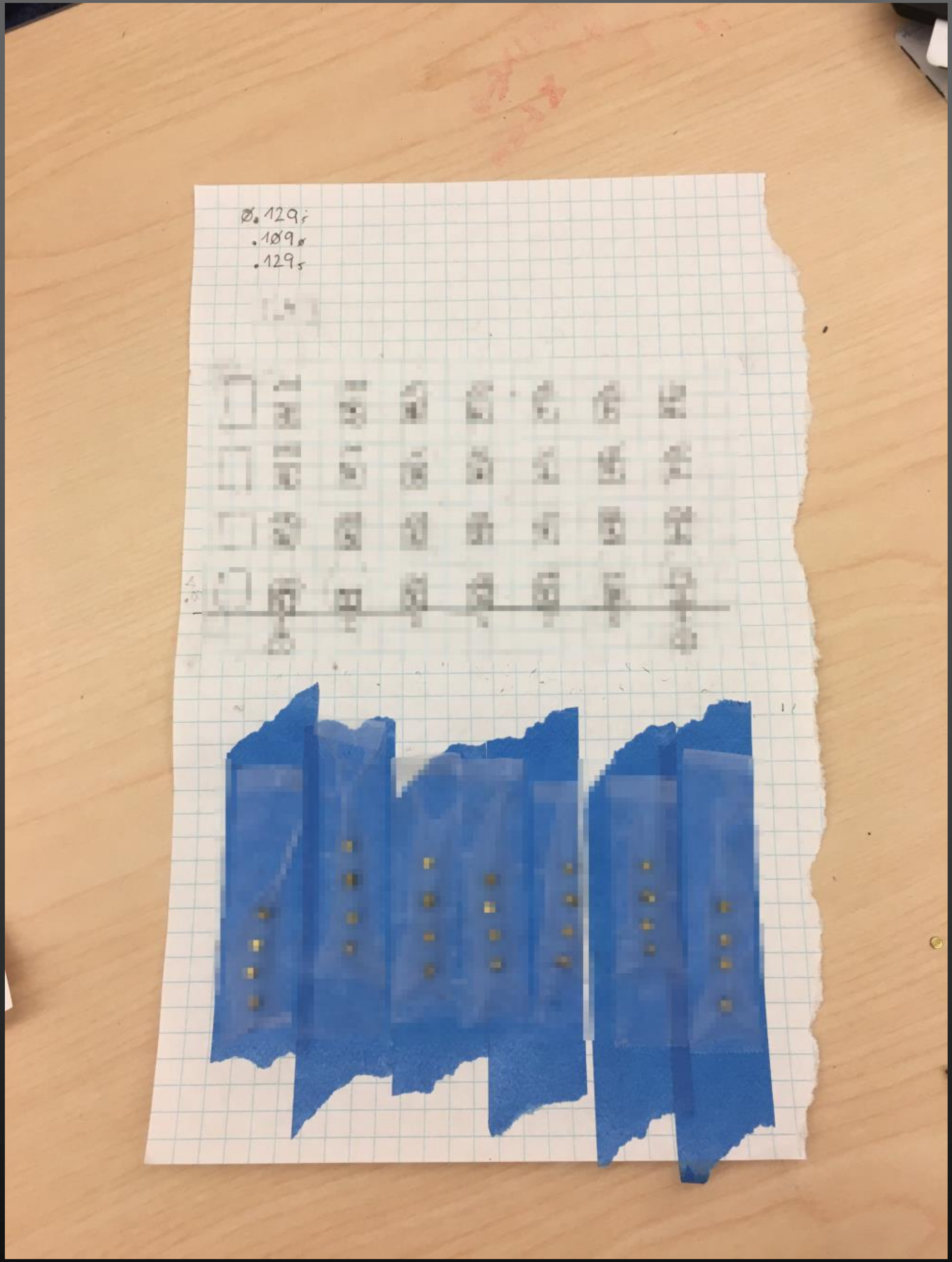
…so we made our own





[redacted] [redacted] [redacted] [redacted] [redacted] [redacted] [redacted]

Measure the pins

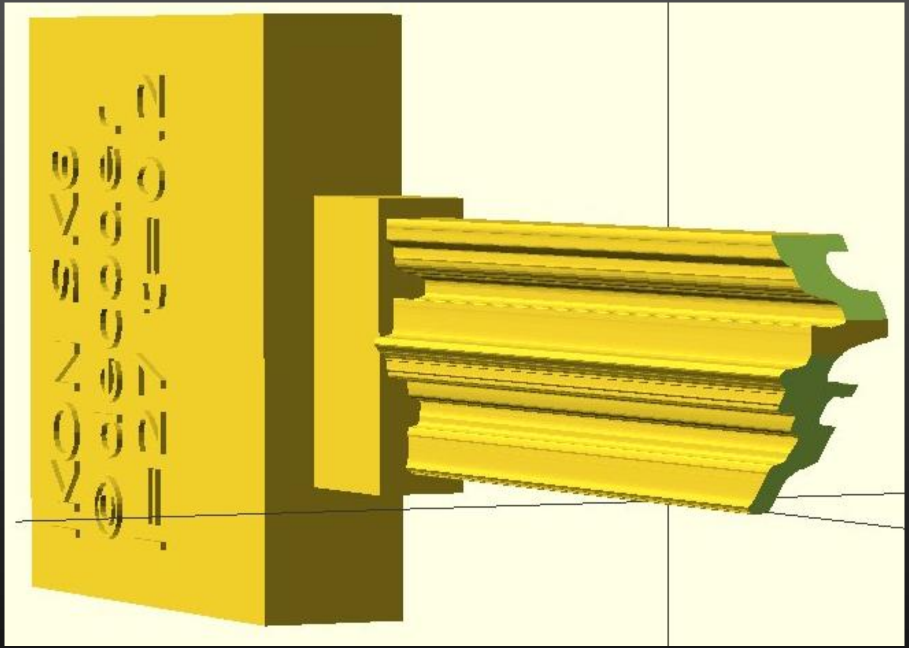


So now what?

- Fill & File
- Make a key

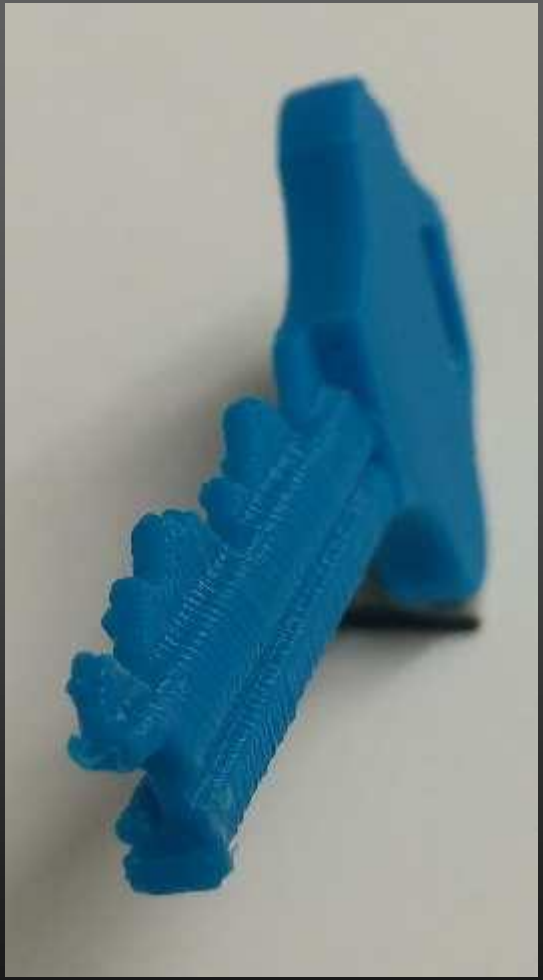
CAD Model

- Given photos of keyways, can we create a 3D model?
- Can it be made permissive for numerous keyways?



https://www.wired.com/2014/08/3d-printed-bump-keys

3D Print



“Replication Prohibited: Attacking Restricted Keyways with 3D Printing”, Burgess, et al.

CNC Mill…?

PCNC 1100
PERSONAL CNC
TORMACH
www.tormach.com

easy entrie
OK
STOP
CSI/SPECO REGULATED POWER SUPPLY
MODEL NO. PSR-4/24

Mitigations

- Use locks with restricted (patent protected) keys
- Limit the number of people who can access multiple keys
- Remind users not to display their keys
- Consider hybrid key systems that combine electronic and physical protections
- Use Defense in Depth strategies

Acknowledgements

- Volty
- Matt Blaze
- Deviant Ollam
- Rubber Banned
- Ben Golub
- Jos Weyers
- Dune
- Michael Weiner
- Rfguy
- Christian Holler (Decoder)

References

- "Master Keying", Deviant Ollam. https://deviating.net/lockpicking/slides/keys_to_the_kingdom.pptx
- "BEST A2 & A4 Keys System Training", Stanley. https://www.lsamichigan.org/Tech/BEST%20A2%20-%20A4%20Key%20Systems%20Training%20ver.%2002132015.pdf
- "Master Key System Design Guide", ASSA ABLOY Group. https://www.lsamichigan.org/Tech/Master_Key_System_Design_Guide_ASSA-ABLOY.pdf
- "Cryptology and Physical Security: Rights Amplification in Master-Keyed Mechanical Locks", Matt Blaze. 2003. https://www.mattblaze.org/papers/mk.pdf
- "Notes on SFIC (Best) Interchangeable Core Locks", Matt Blaze. 2003. https://www.mattblaze.org/photos/misc/sfic/
- "Hochsicherheits-Generalschlüssel Marke Eigenbau", Michael Weiner & RFGuy. 2016. https://github.com/muccc/akab/blob/master/33c3/Evva_3ks_33c3.pdf
- "Key Decoding", Deviant Ollam. https://deviating.net/lockpicking/slides/key_decoding.pdf
- "Replication Prohibited: Attacking Restricted Keyways with 3D Printing", Burgess, Wustrow, Halderman. https://www.usenix.org/system/files/conference/woot15/woot15-paper-burgess.pdf