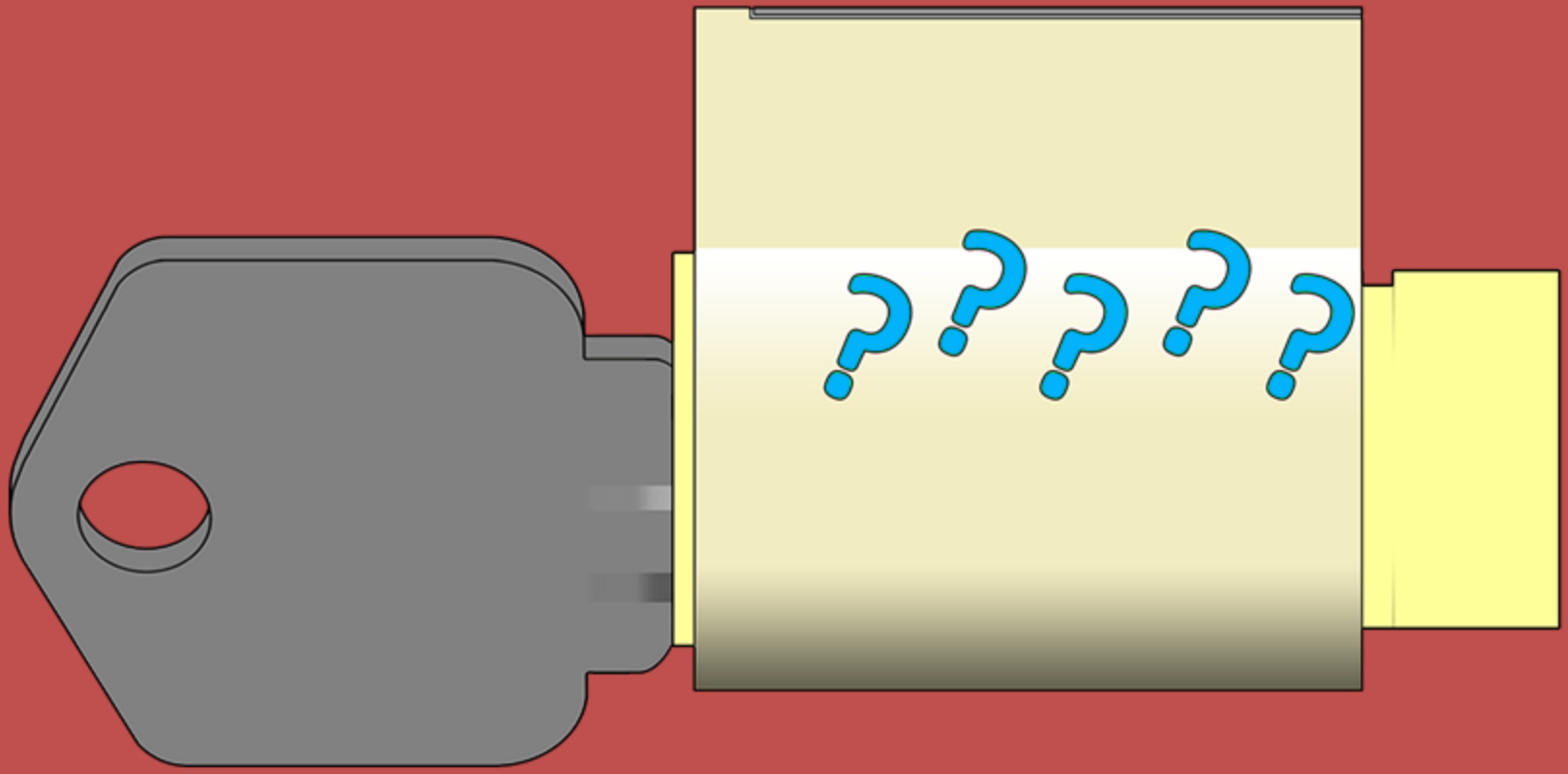
Keys to the Kingdom



Deviant Ollam

Who am i ?

Who am i ?

Who am i ?

THE CORE GROUP

TOOOL
The Open Organisation Of Lockpickers

Who am i ?

THE CORE GROUP

auditing
assessments
research
trainings

TOOOL
The Open Organisation Of Lockpickers

workshops
public lectures
lockpick village
contests & games

The Open Organisation Of Lockpicking

The Open Organisation Of Lockpickers

Lockpicking is Fun, Fun, Fun!

First, a word about rules…

Yes, we have rules. ☺

1. Do not pick locks which you do not own.

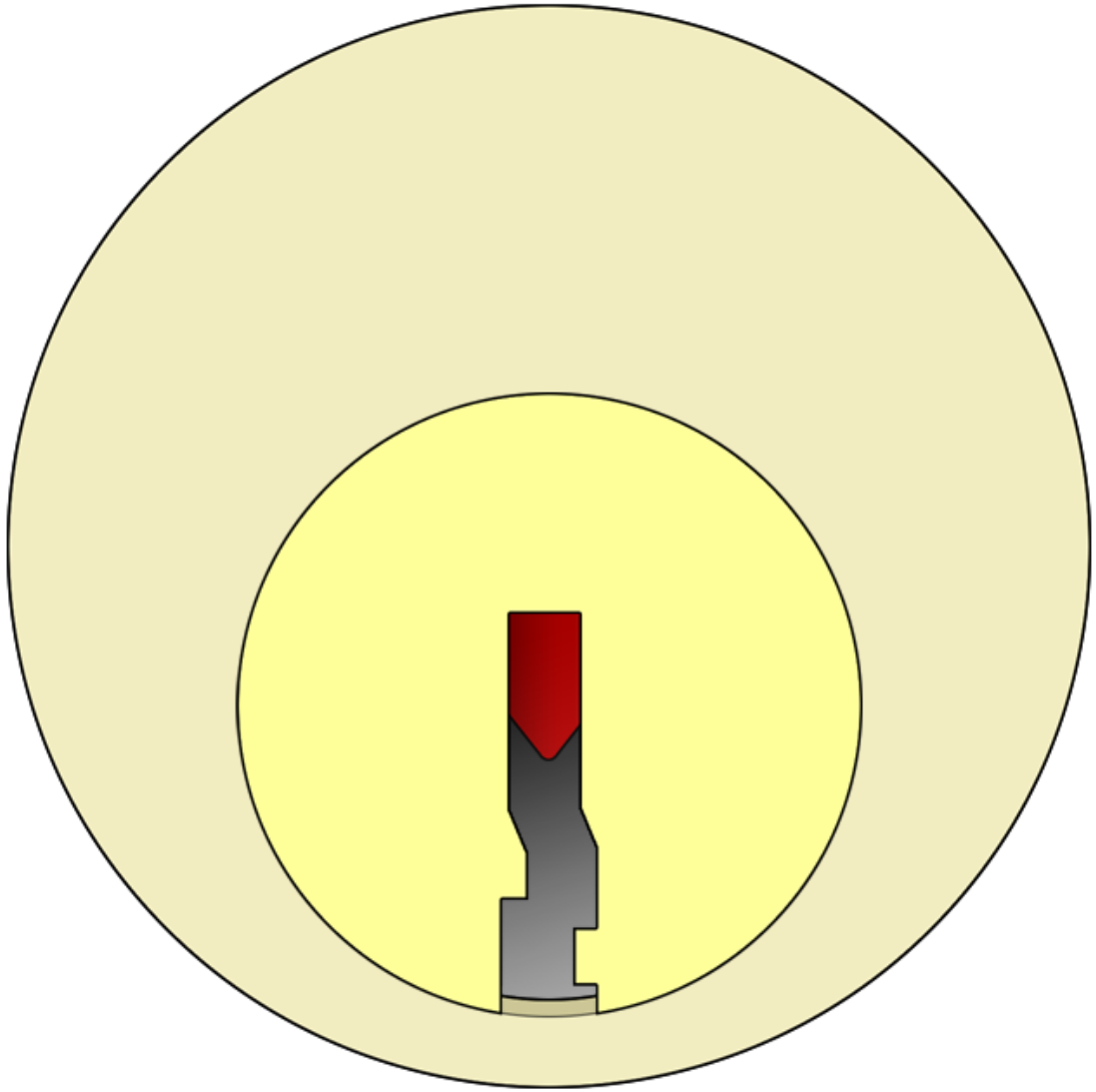
2. Do not pick locks which you rely on.

Doorknobs…

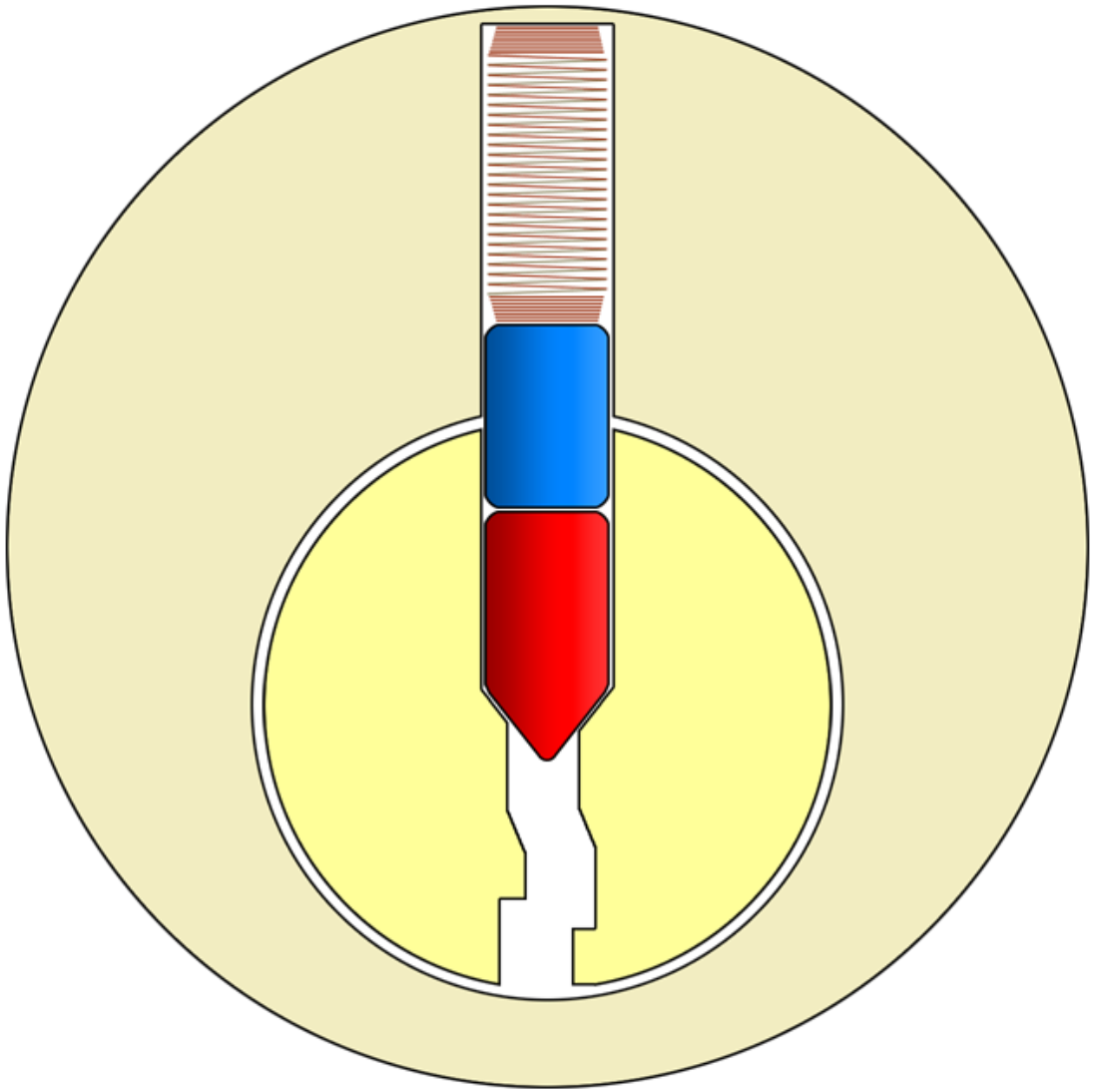
Padlocks…

Deadbolts…

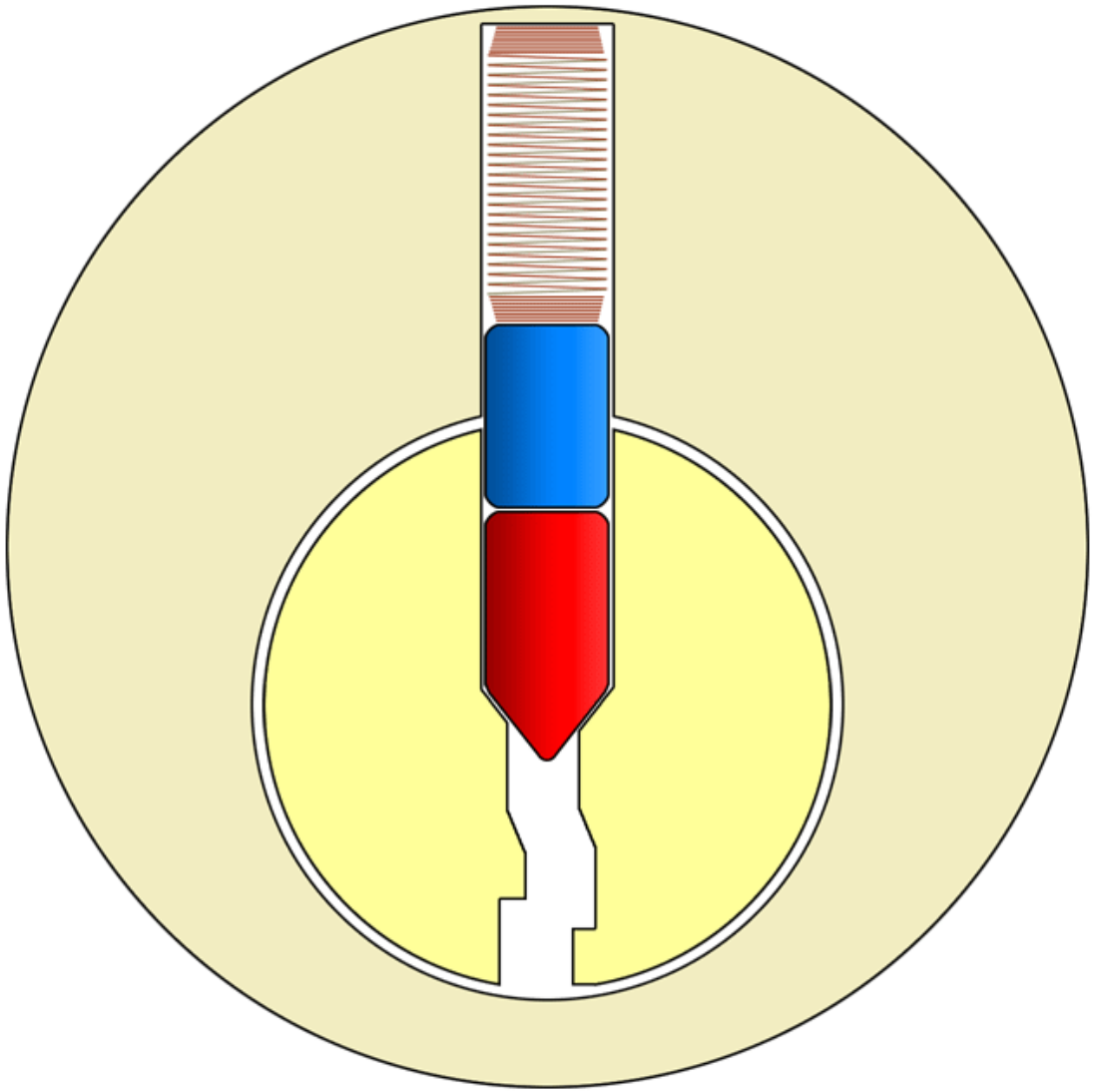
…The Mechanism Itself Is All The Same



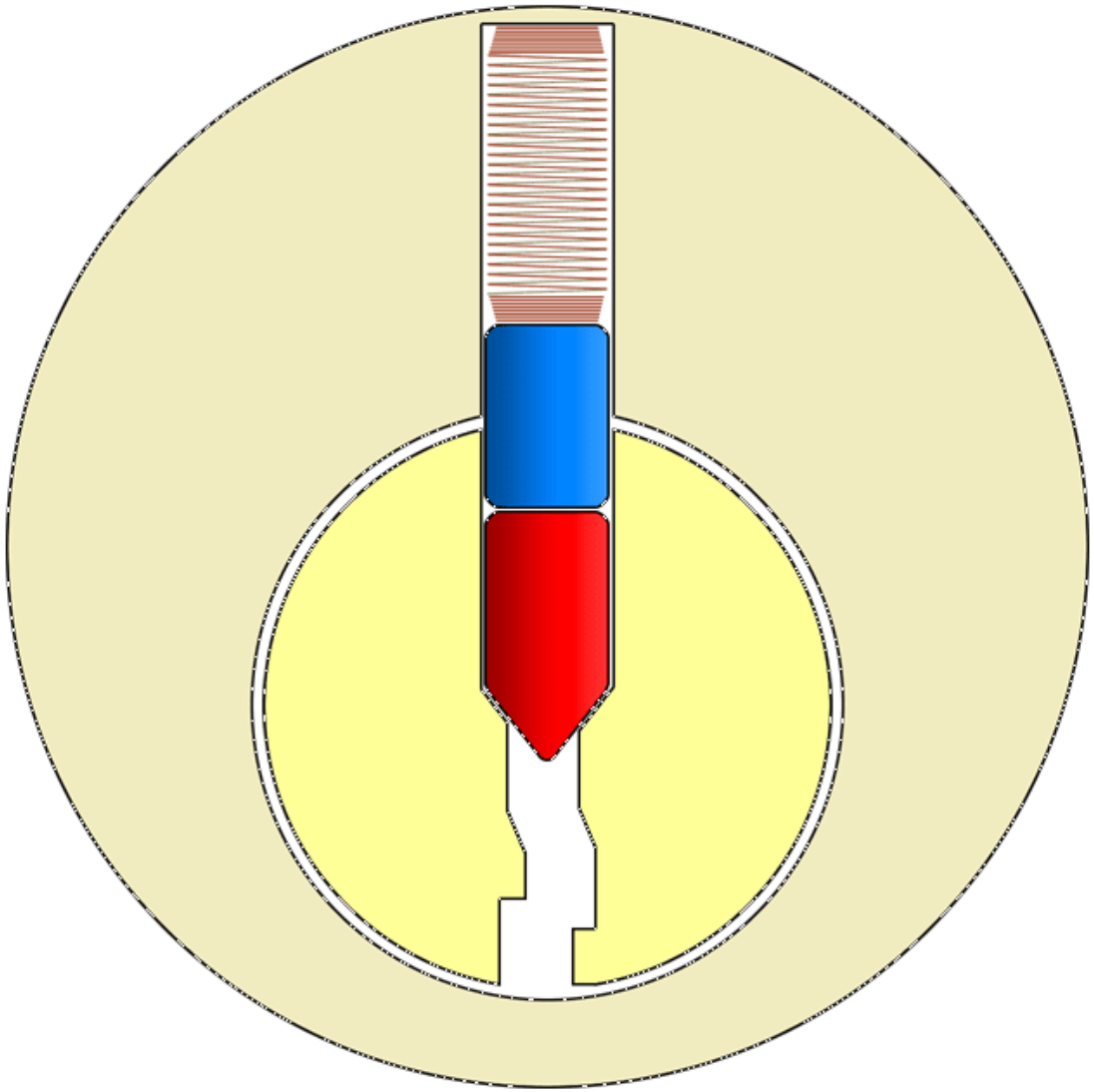
How It Looks Inside



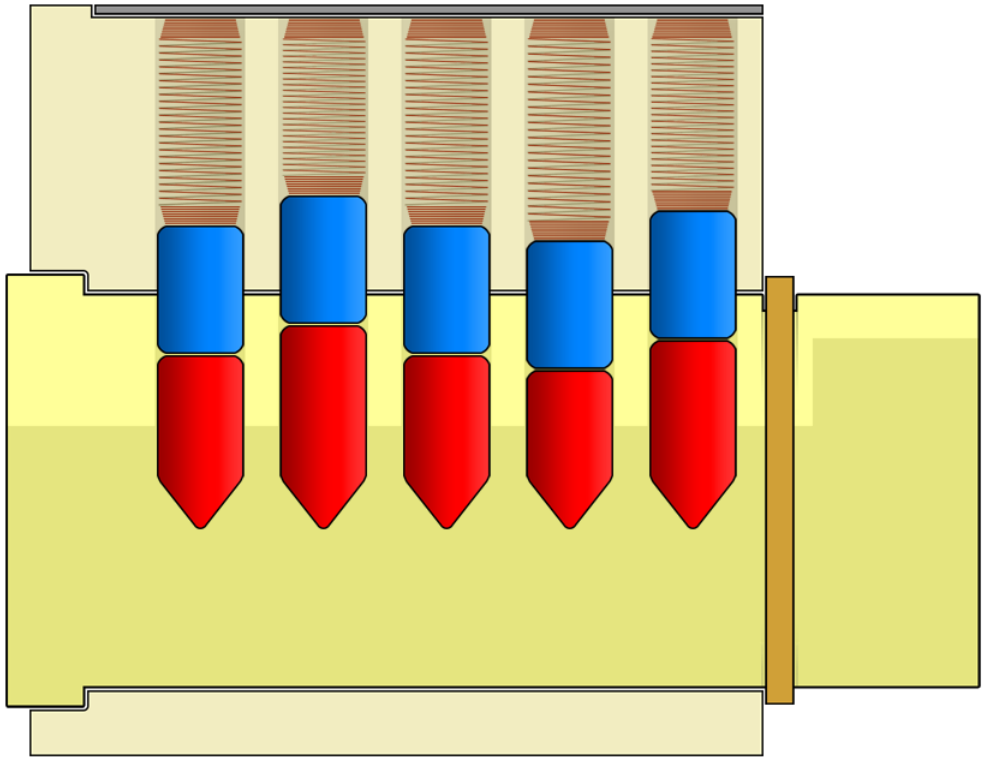
Attempt Without a Key



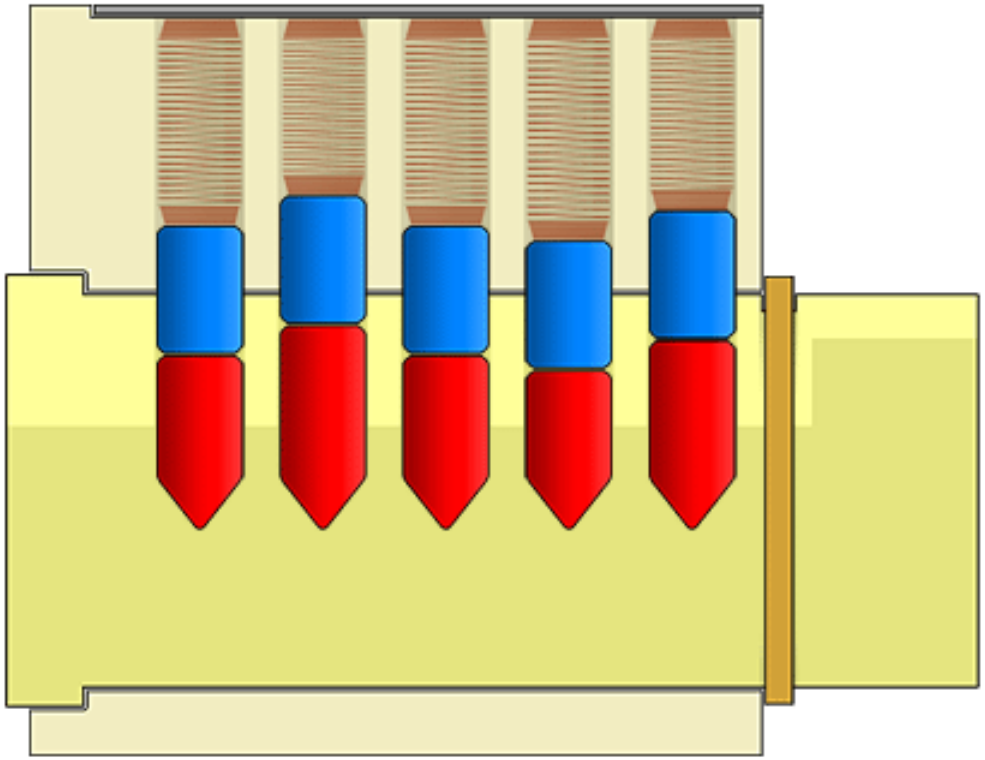
Operating With a Key



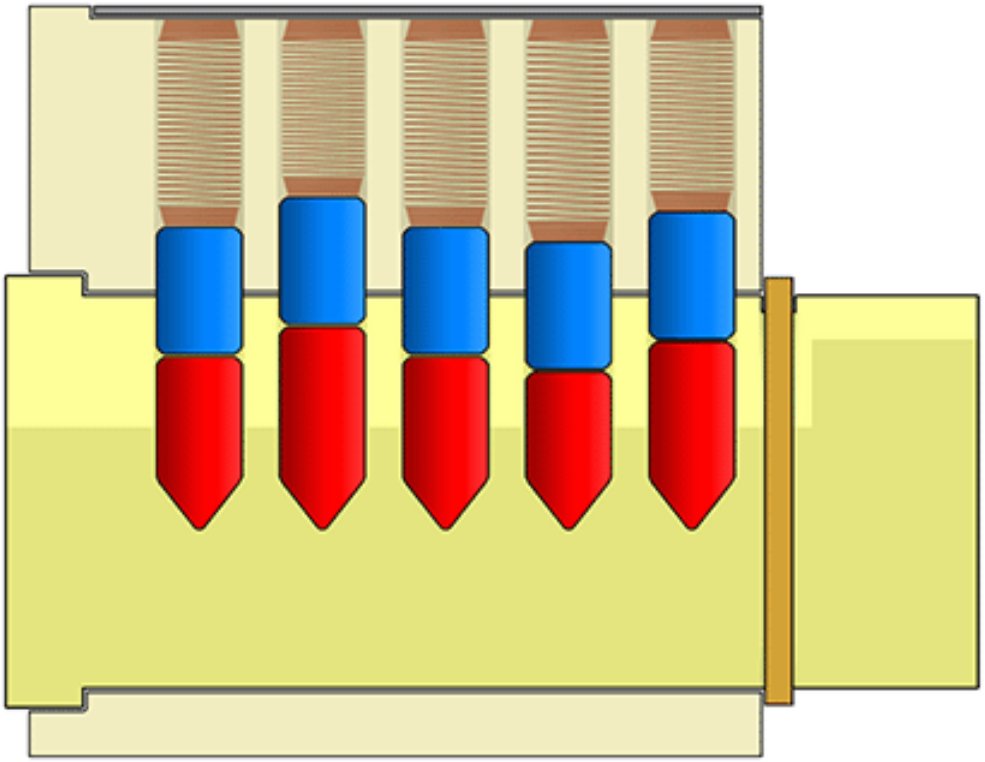
Pin Stacks



Using a Key



Using Lockpicks

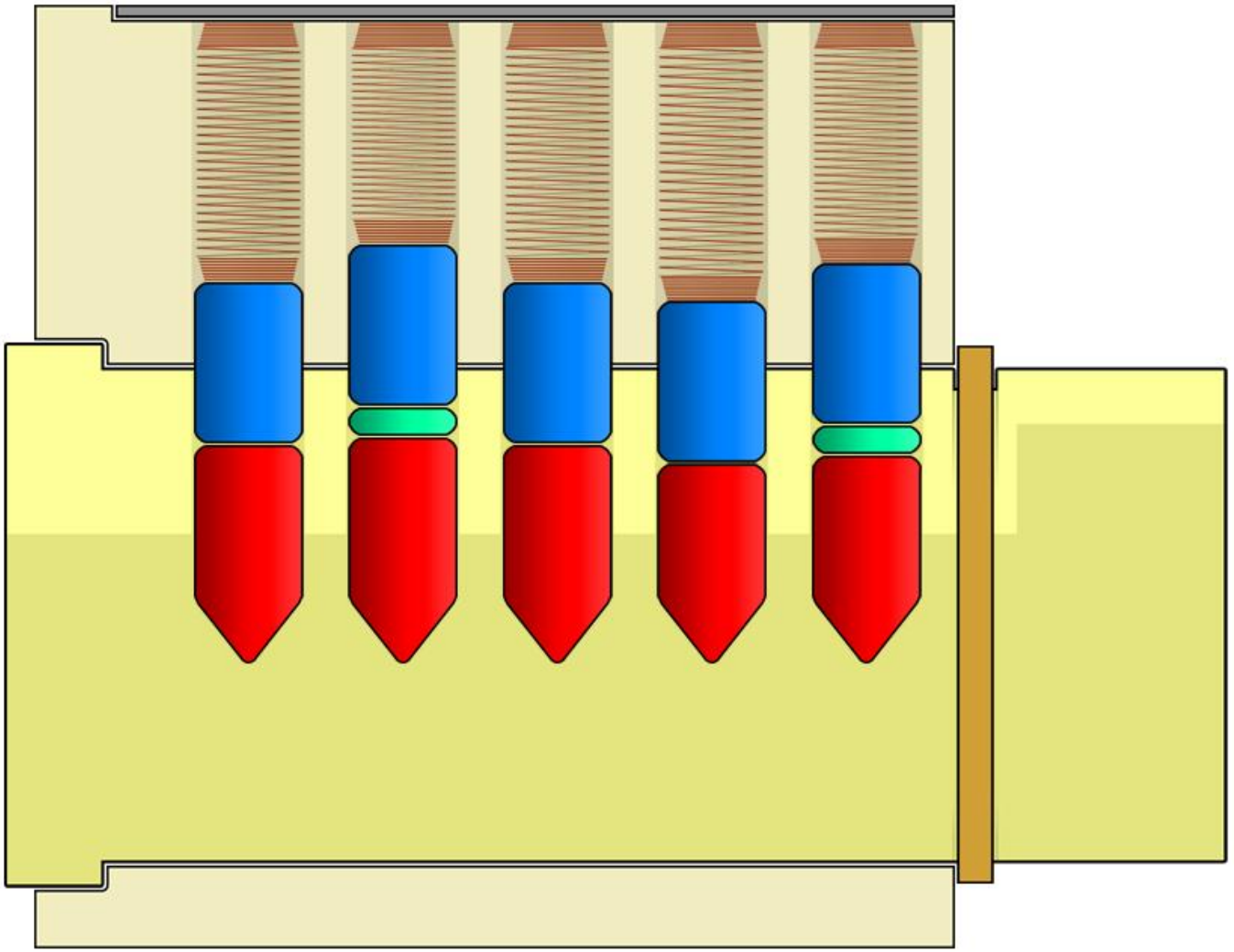


Master-Keyed Systems

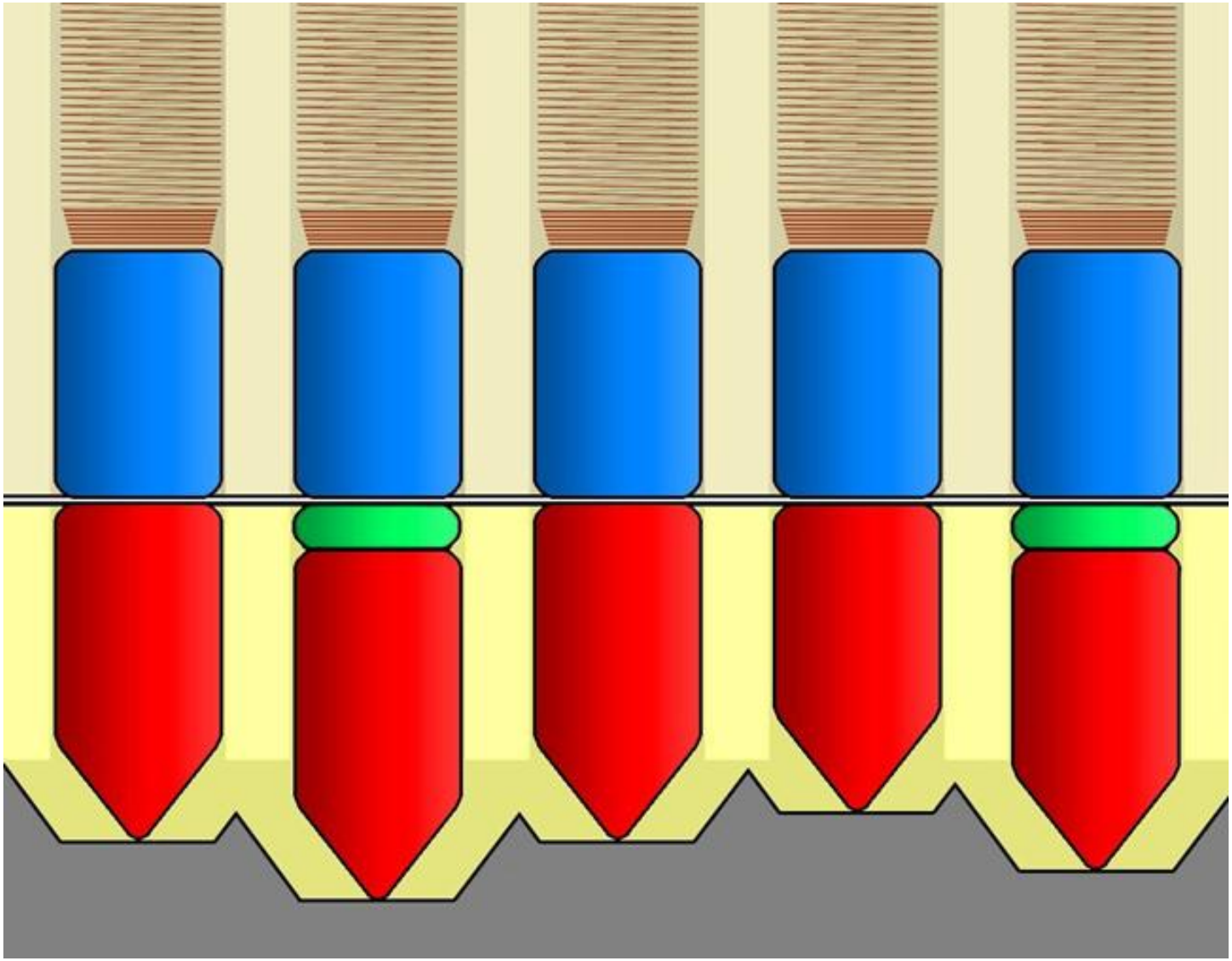
Master-Keyed Systems

Master-Keyed Systems

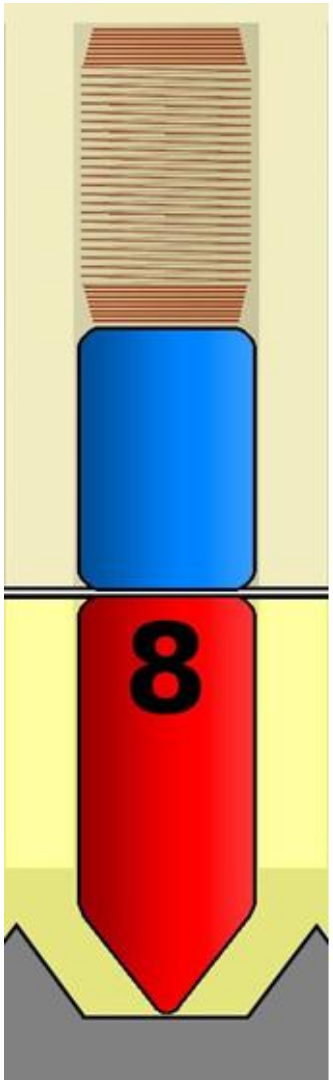
Master-Keyed Systems

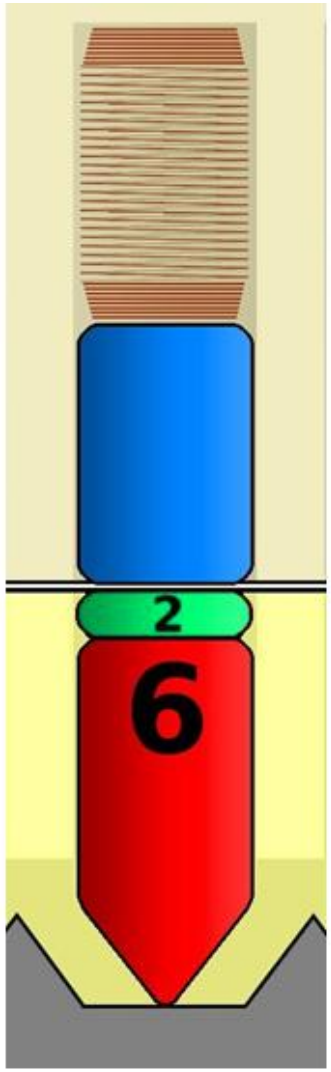


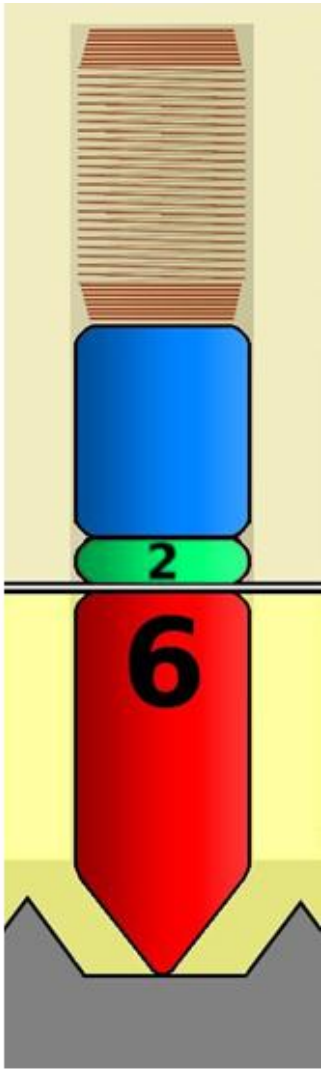
Master-Keyed Systems



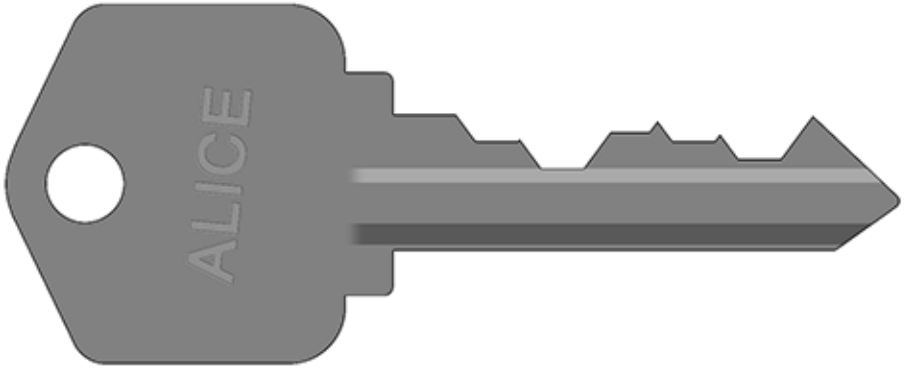
Master-Keyed Systems



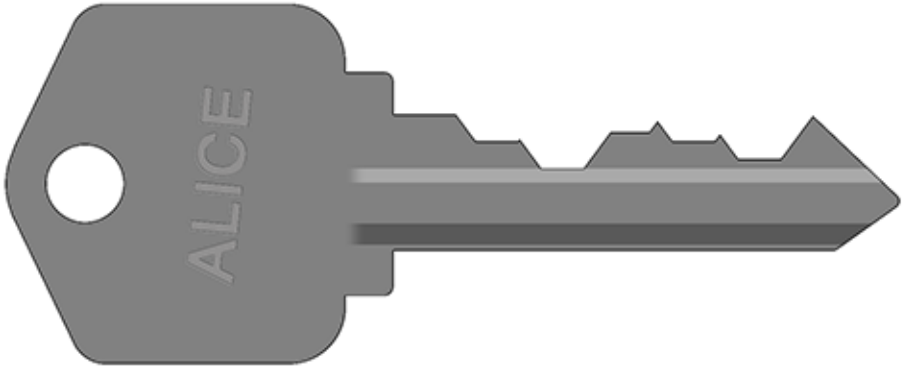


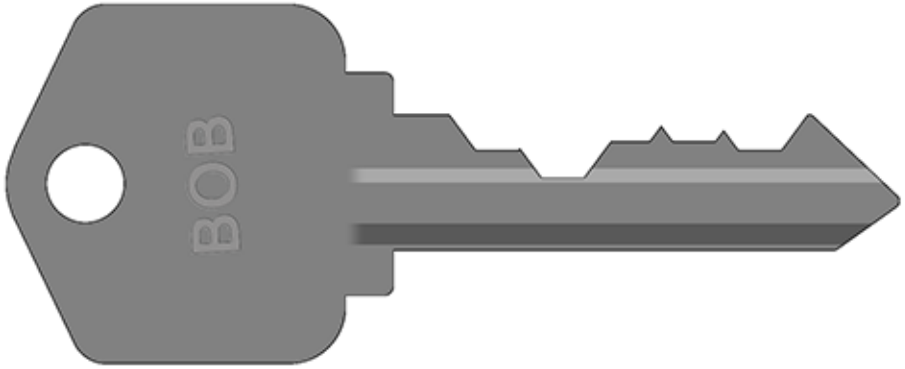


Master-Keyed Systems

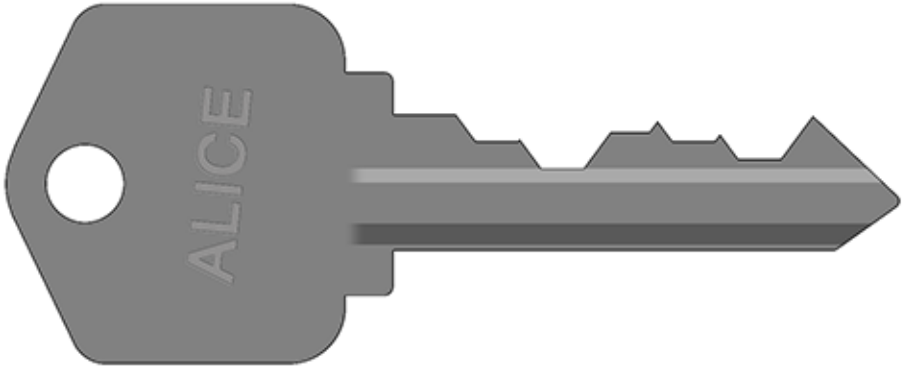


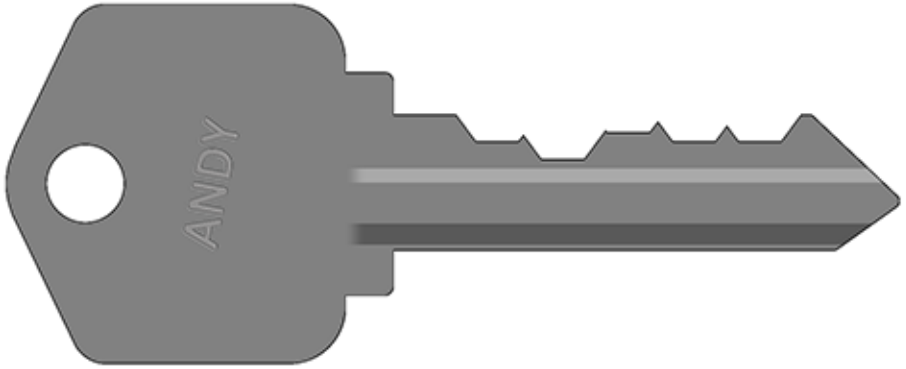
Master-Keyed Systems

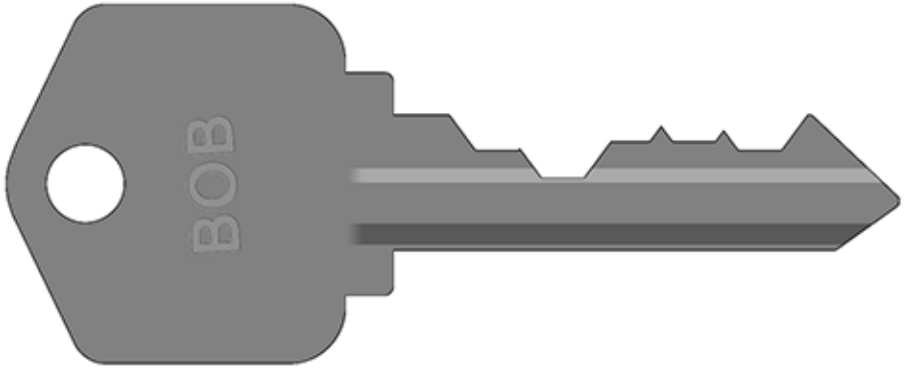




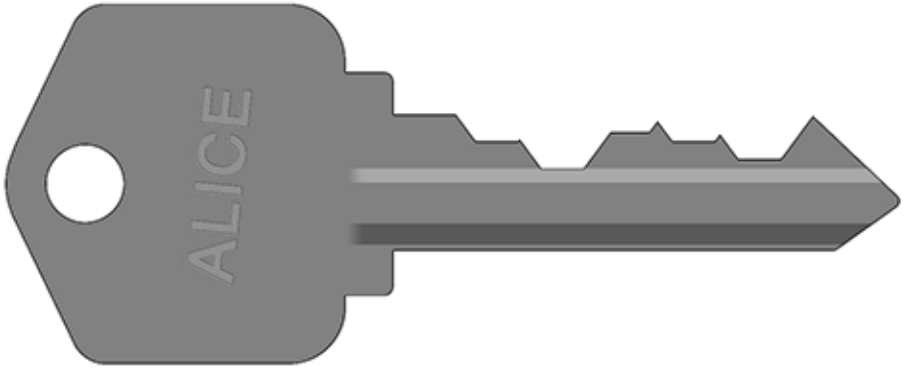
Master-Keyed Systems

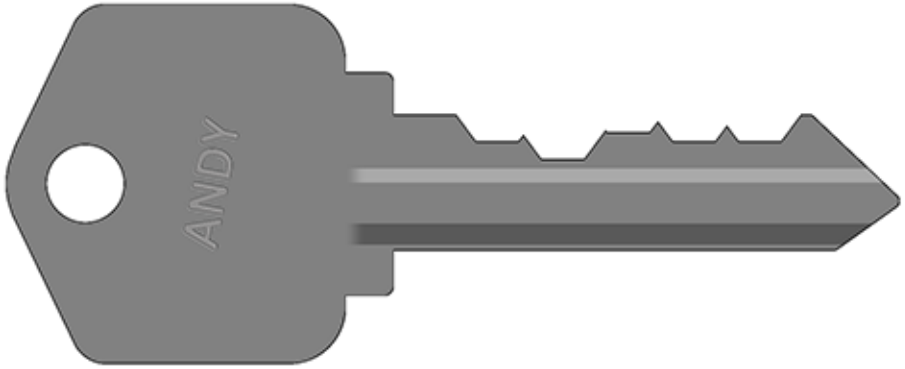


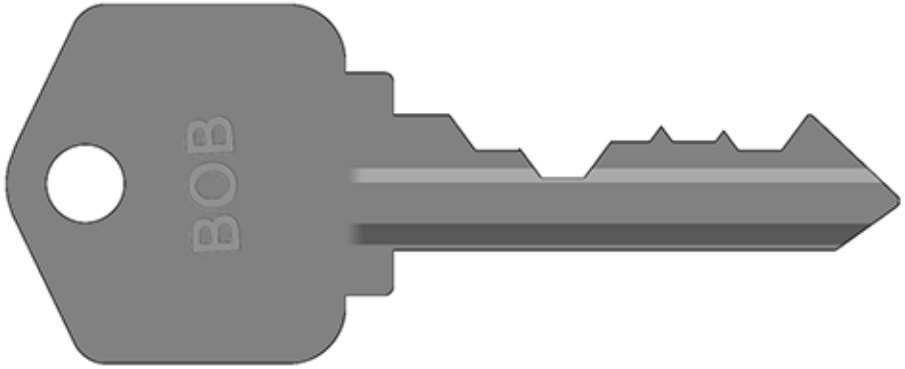


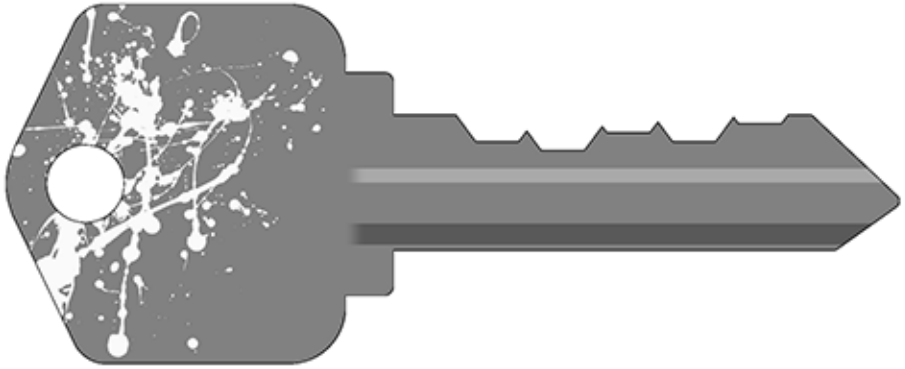


Master-Keyed Systems

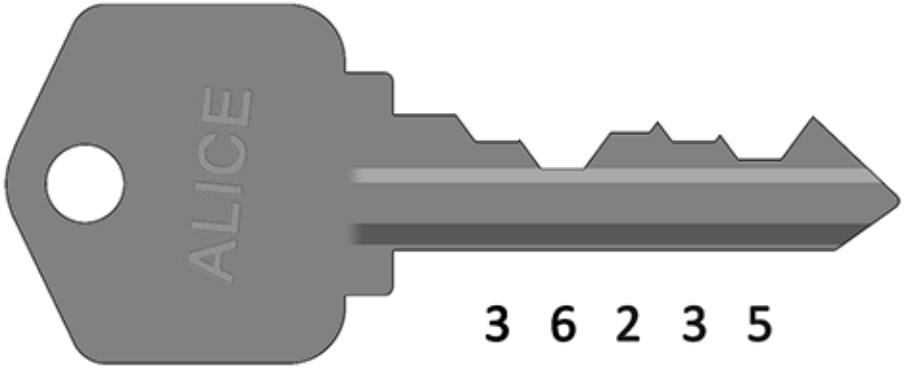


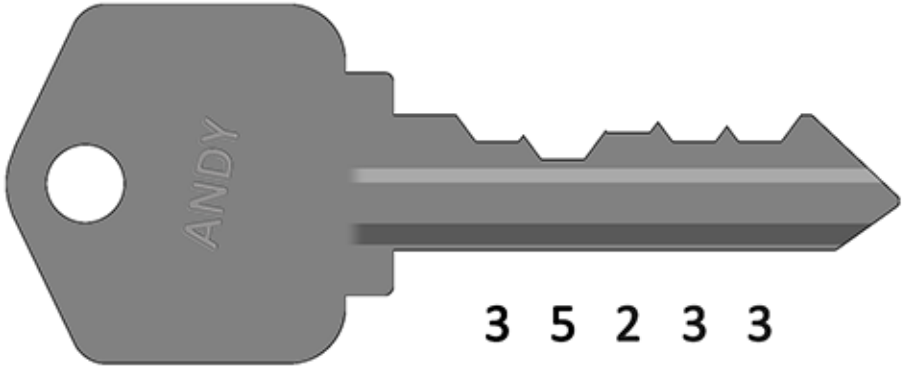


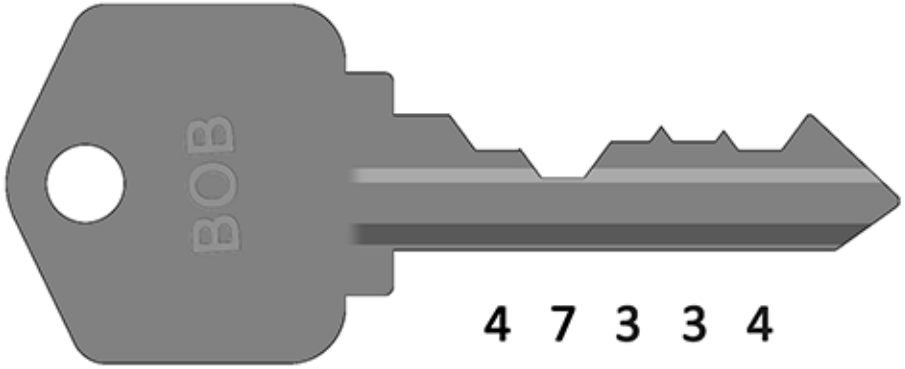


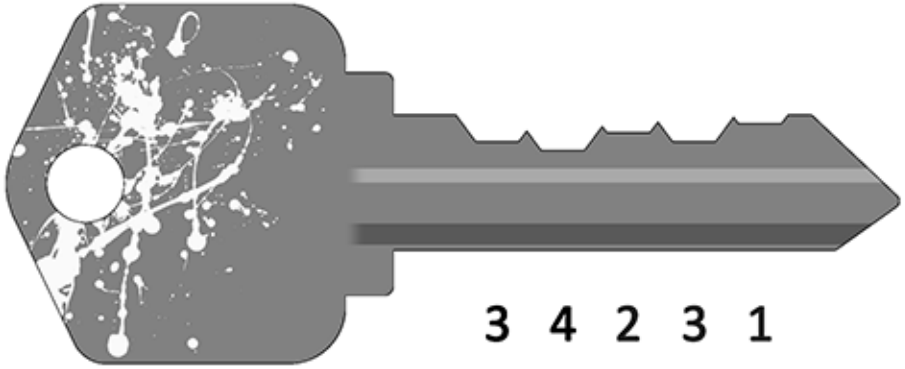


Master-Keyed Systems

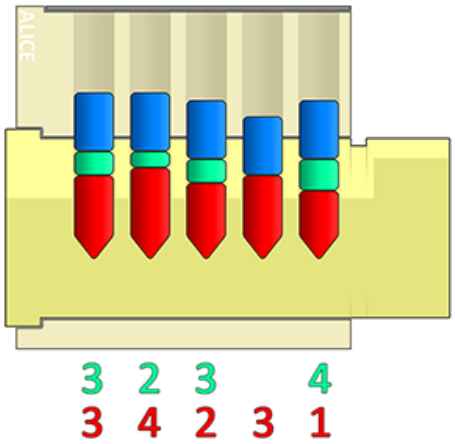


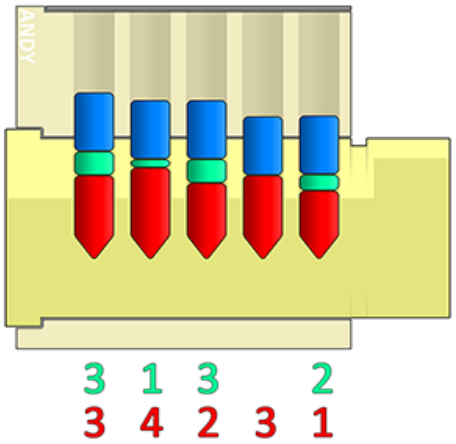


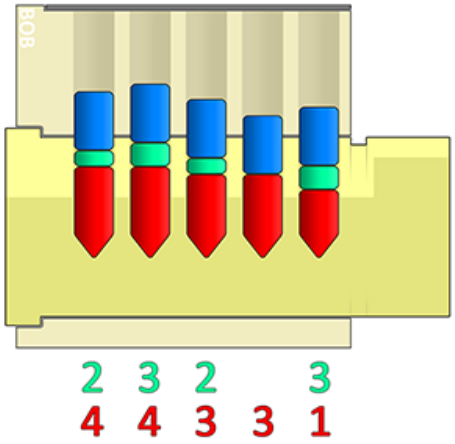




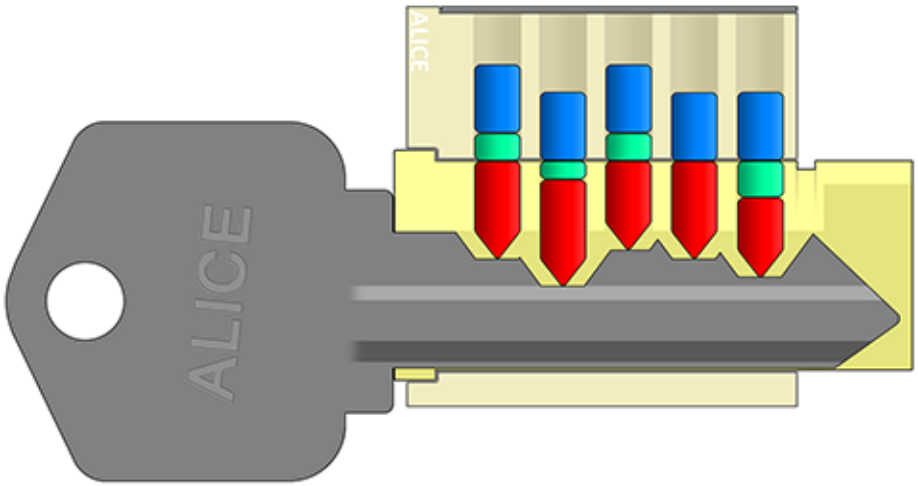
Master-Keyed Systems

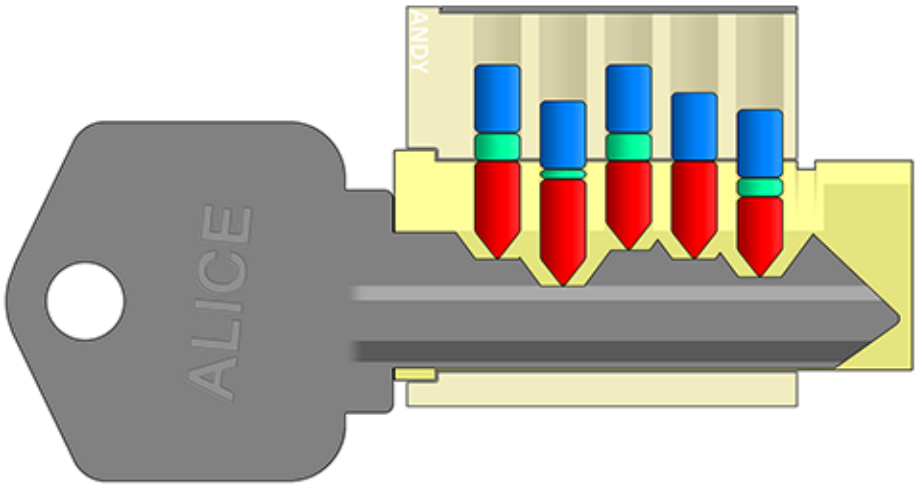


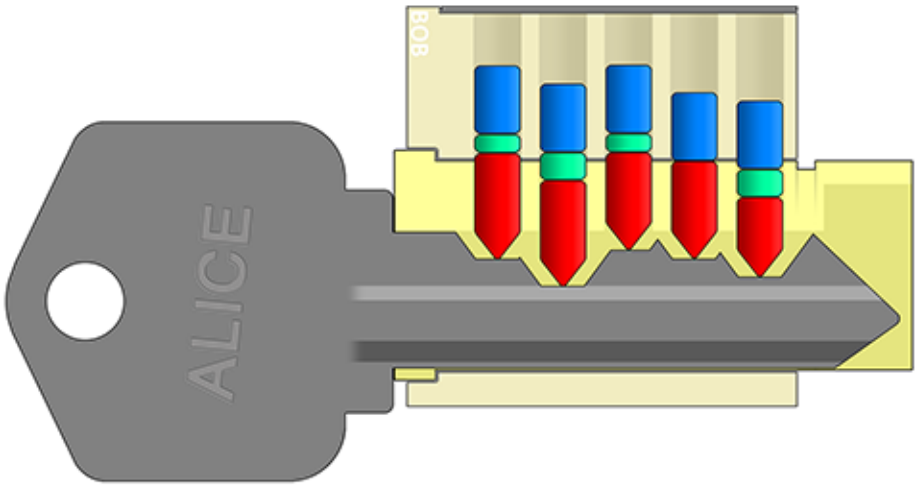


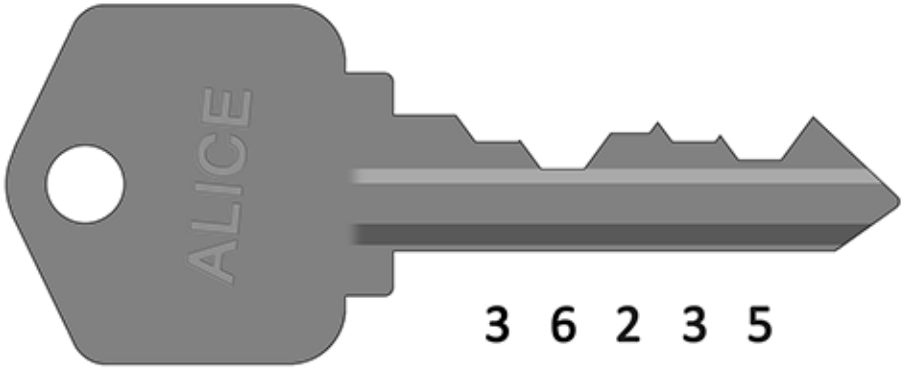


Master-Keyed Systems

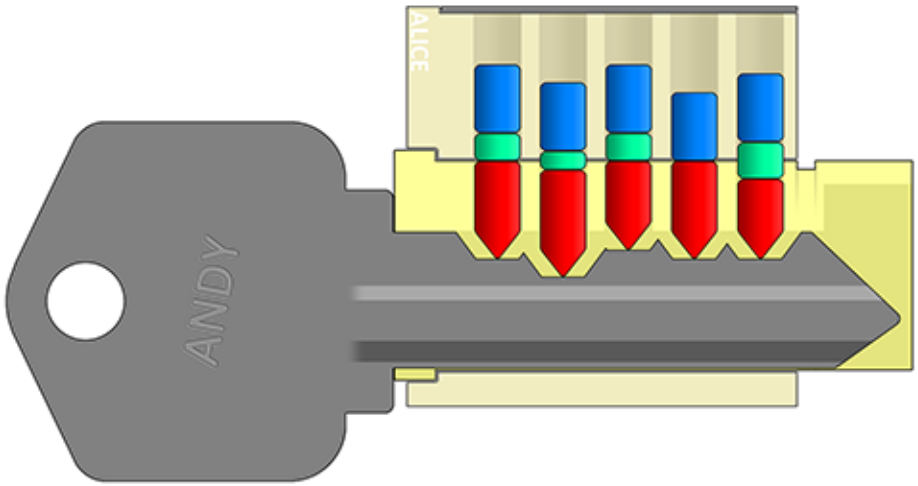


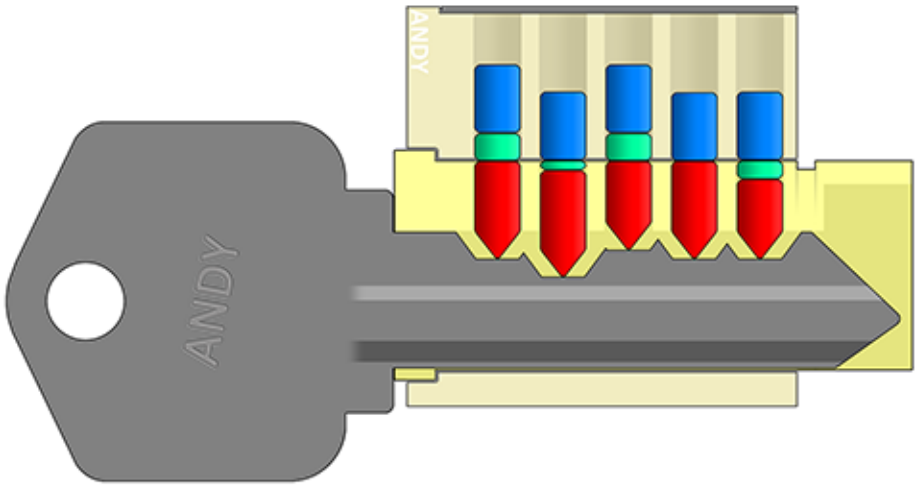


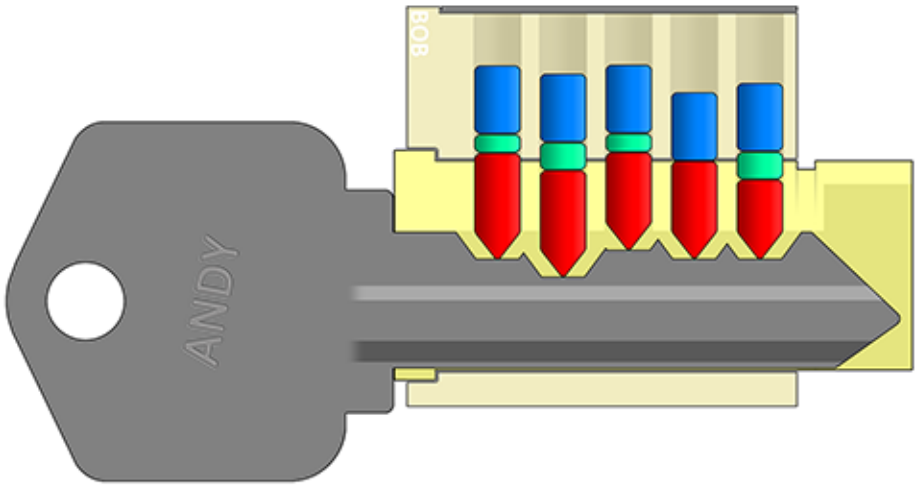


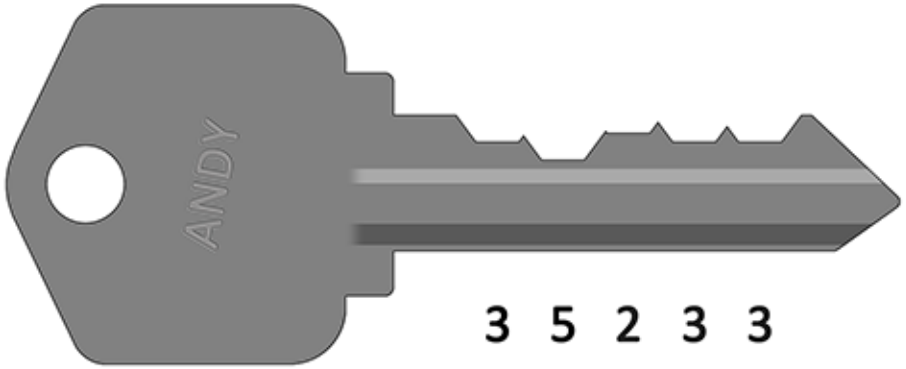


Master-Keyed Systems

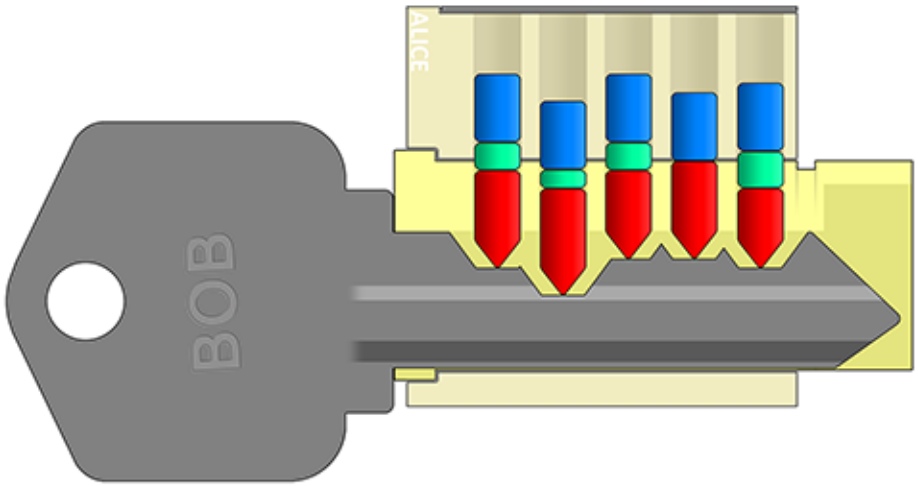


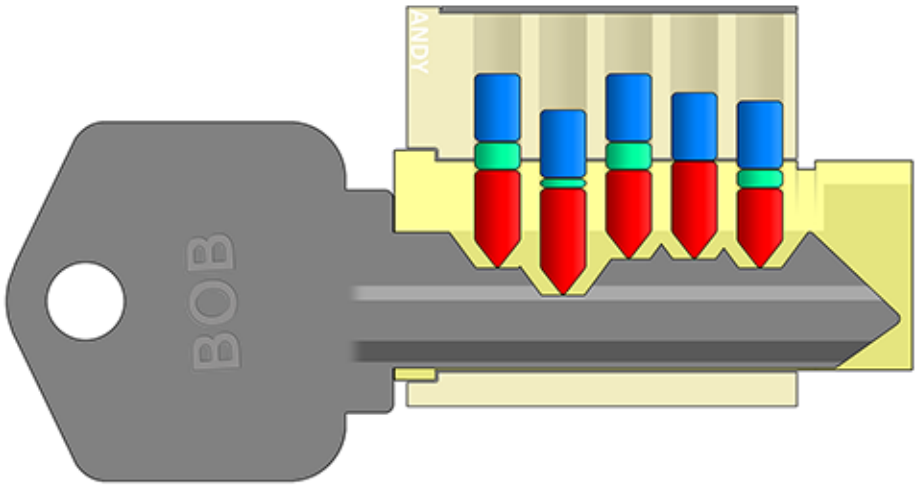


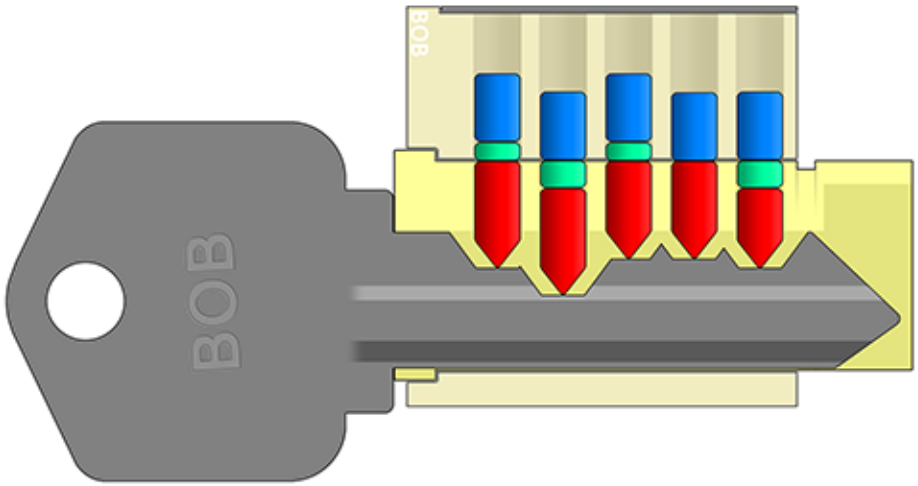


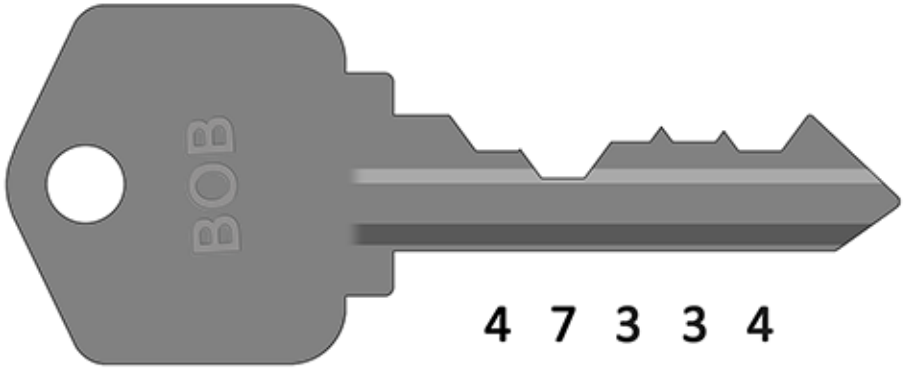


Master-Keyed Systems

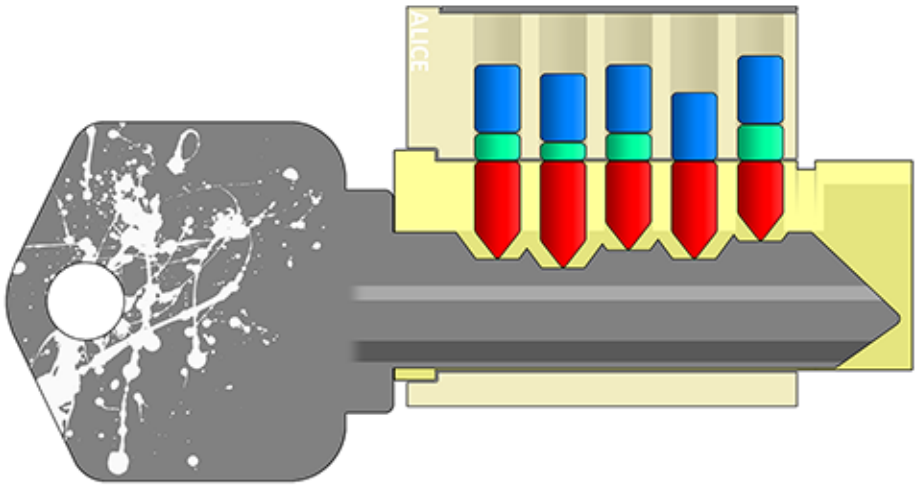


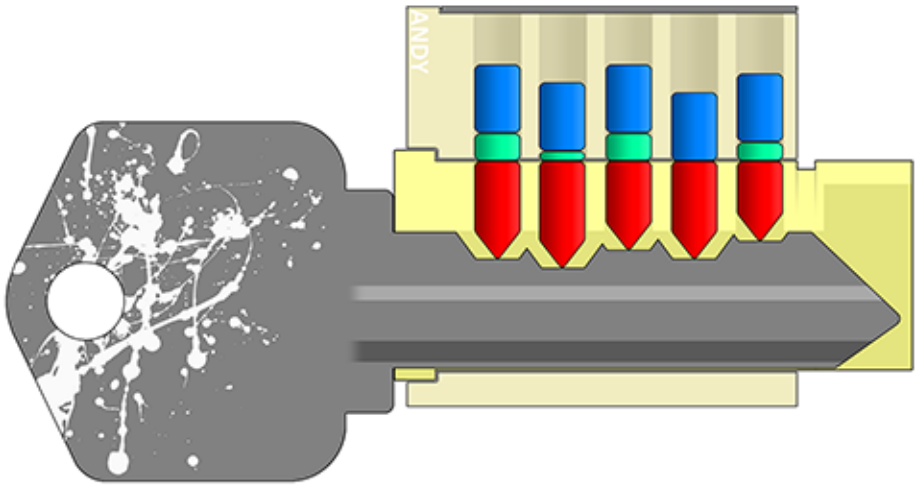


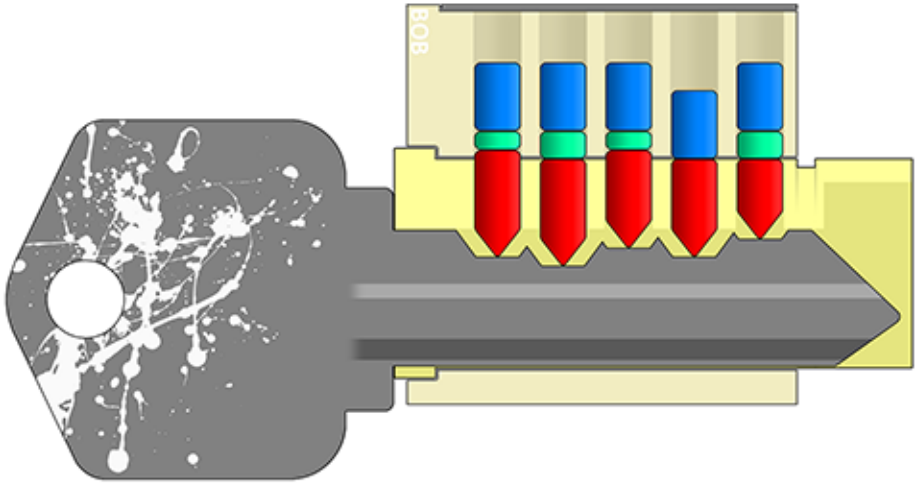


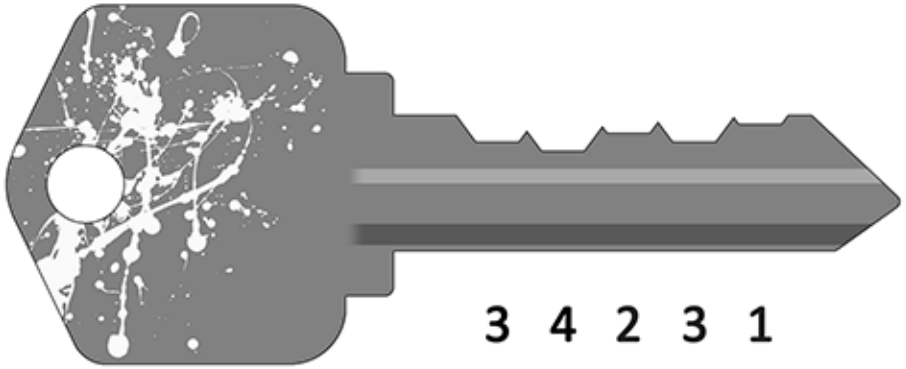


Master-Keyed Systems









Attacking Master-Keyed Systems

"Master-Keyed Lock Vulnerability"

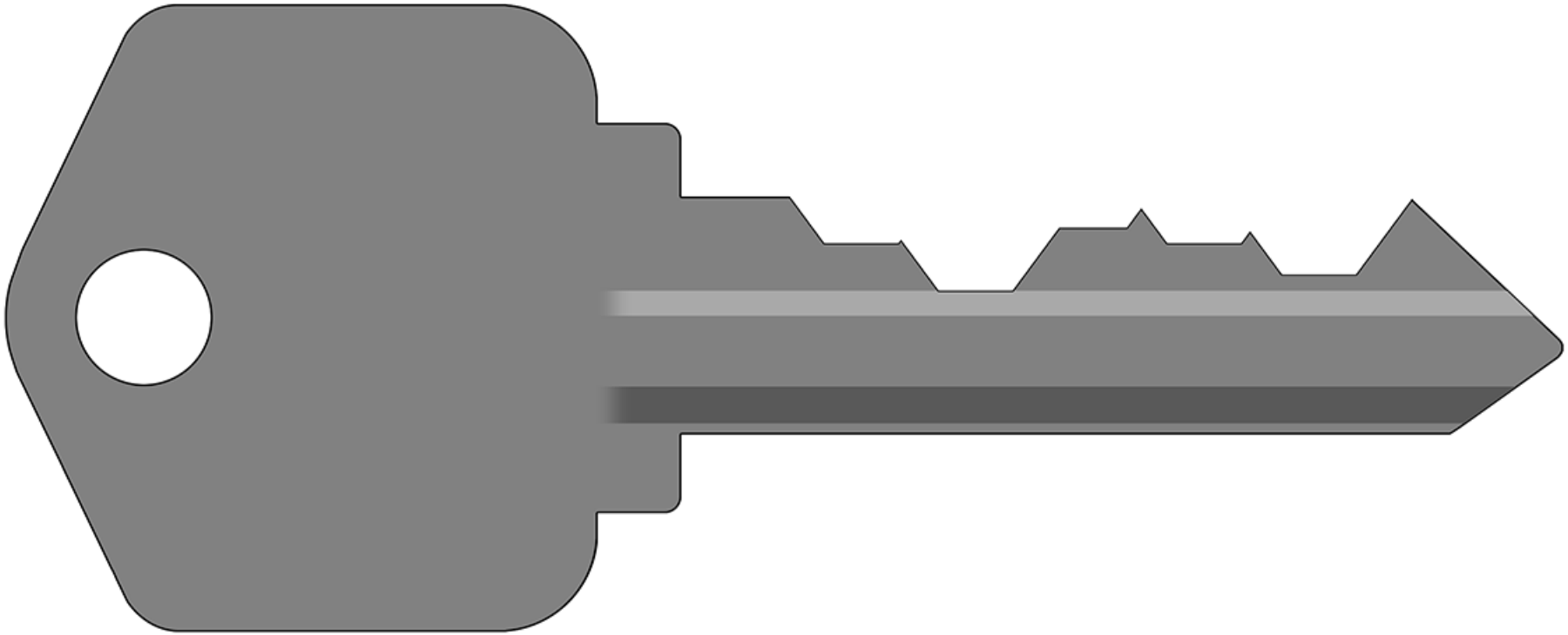
by Matt Blaze

2003-01-27

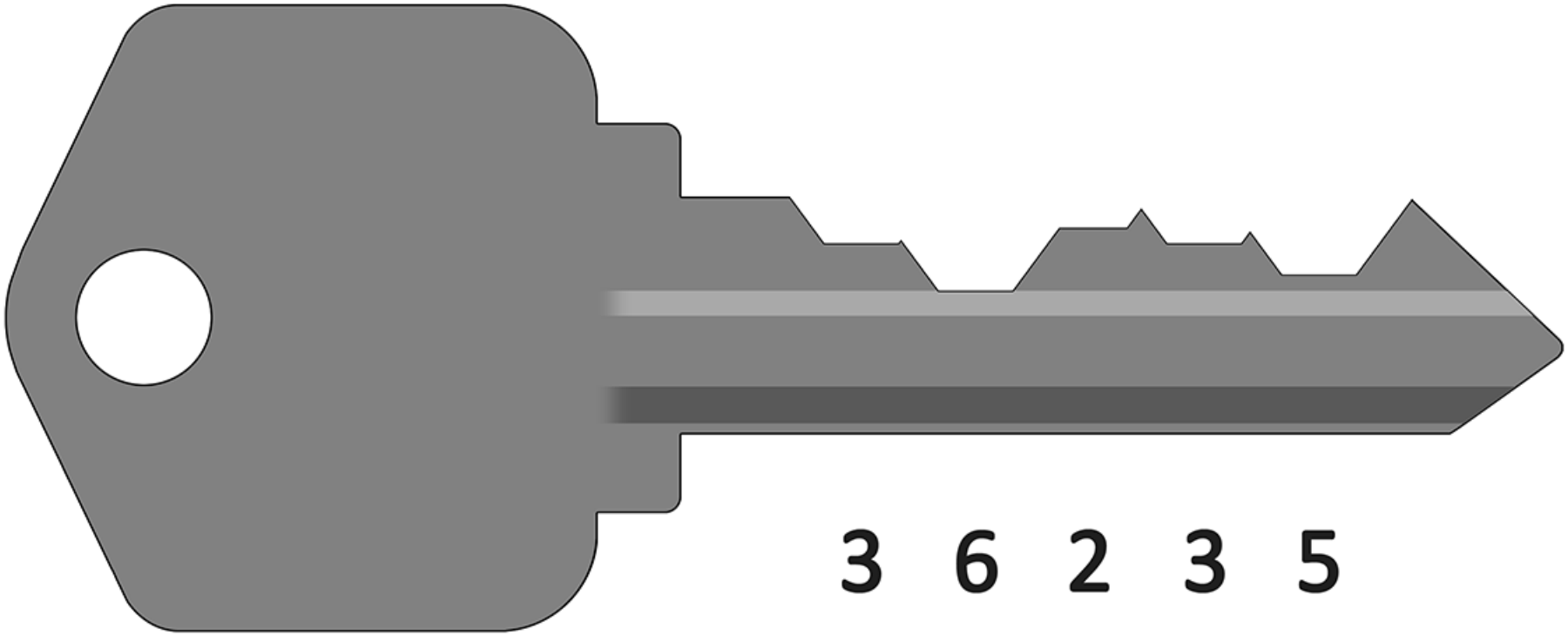
http://www.crypto.com/papers/mk.pdf

http://www.crypto.com/masterkey.html

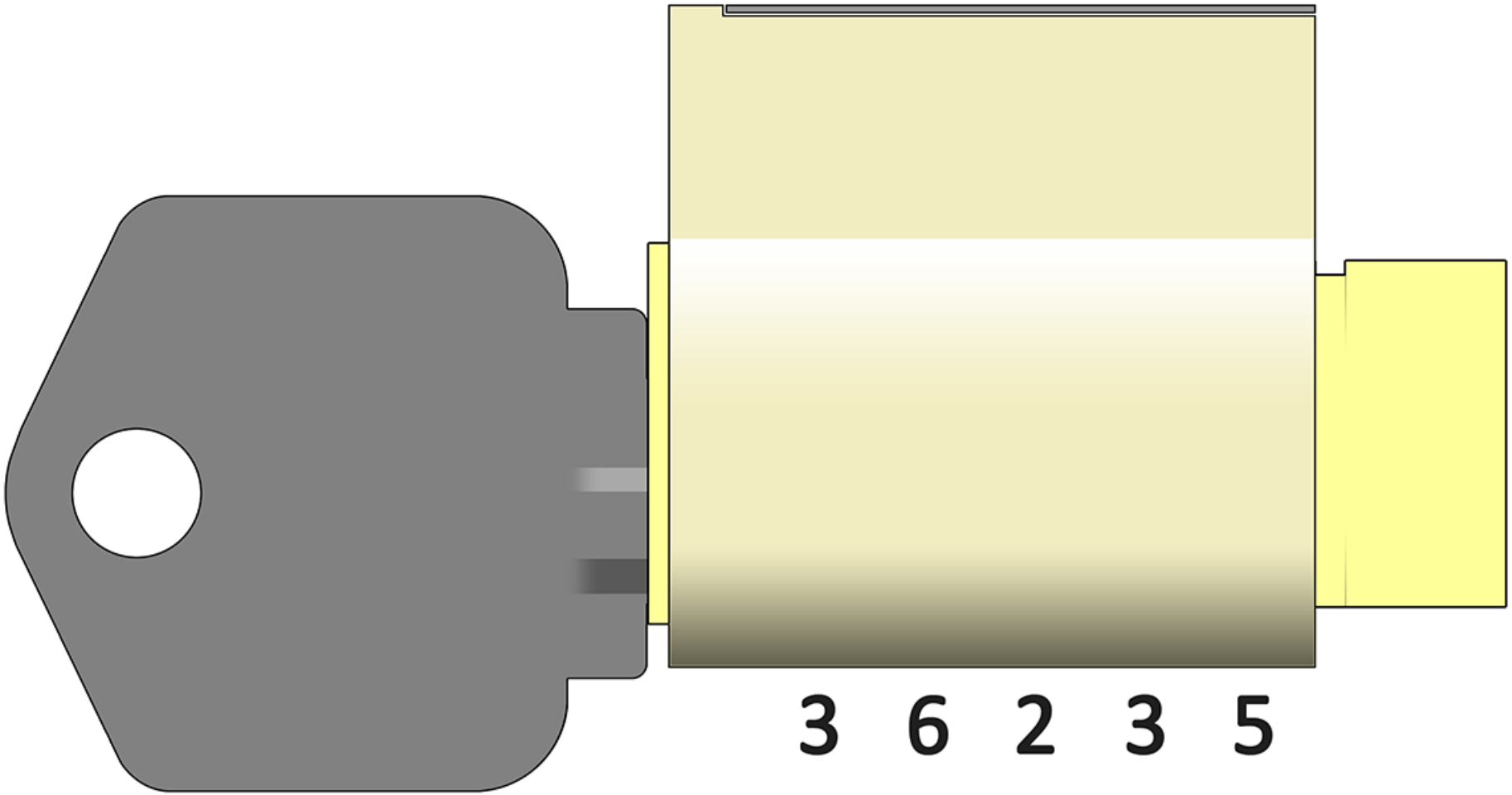
Consider Alice's key… for a lock



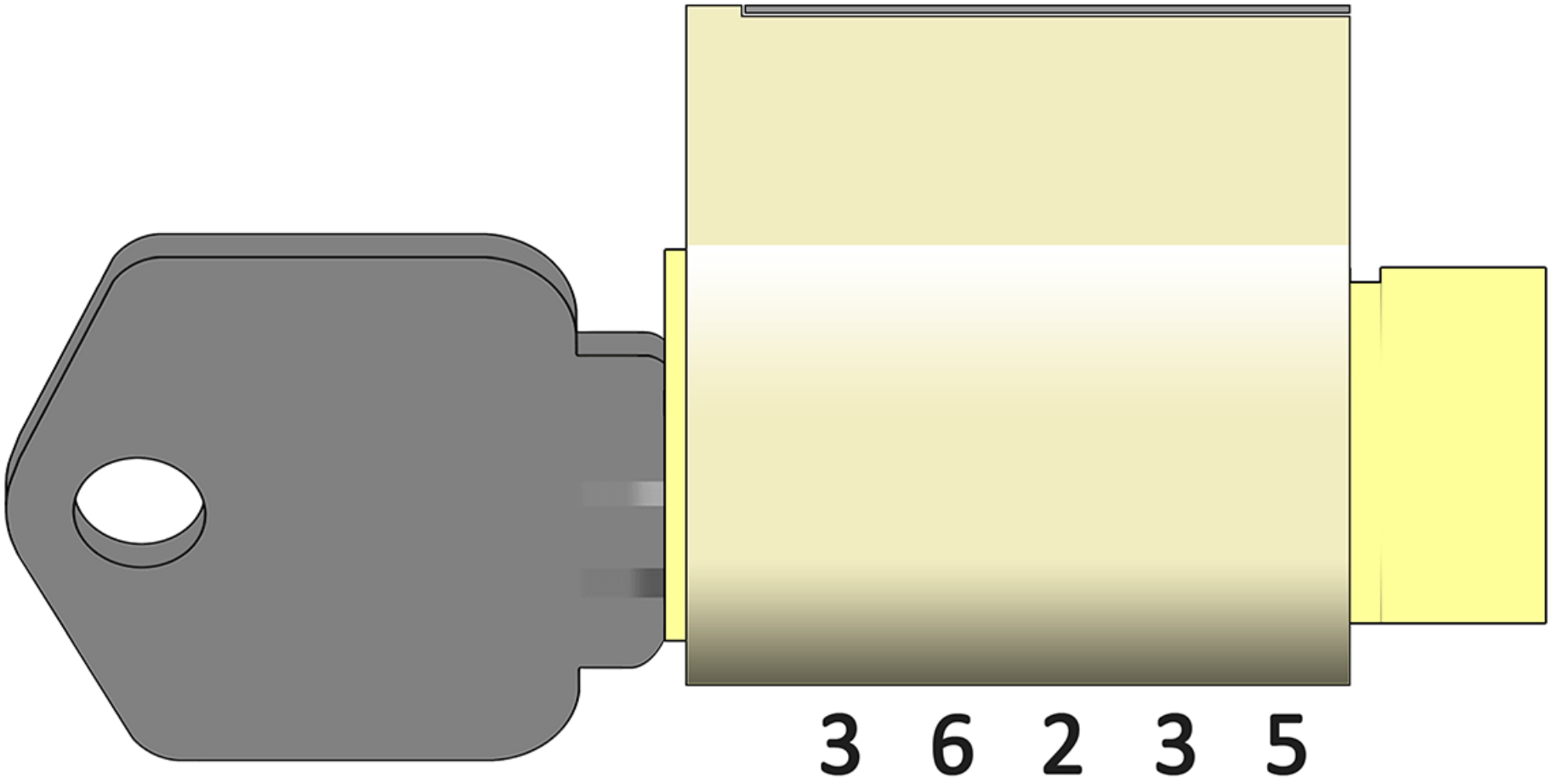
Change Key Bitting Depths



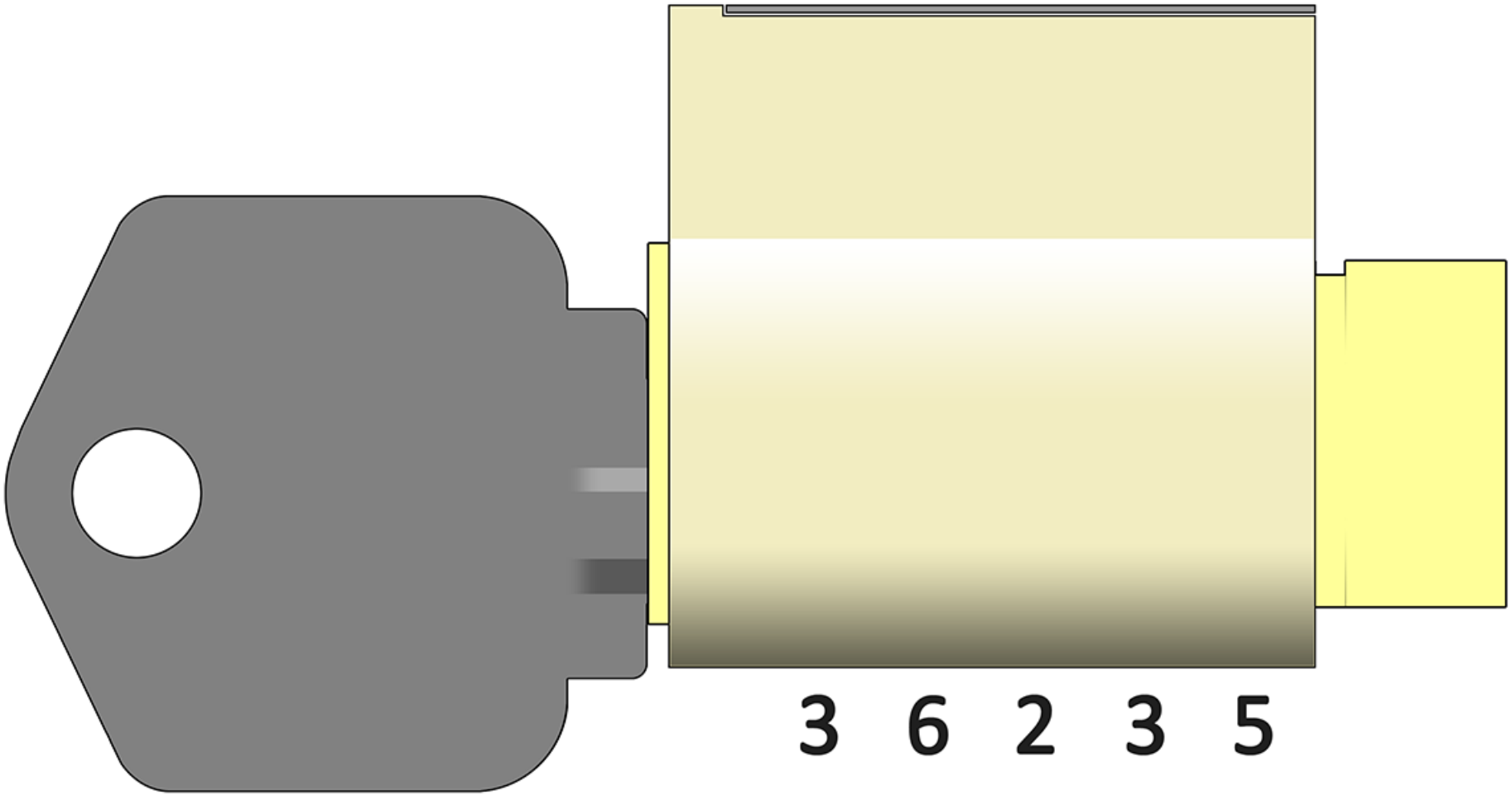
Obviously, it Works in the Lock…



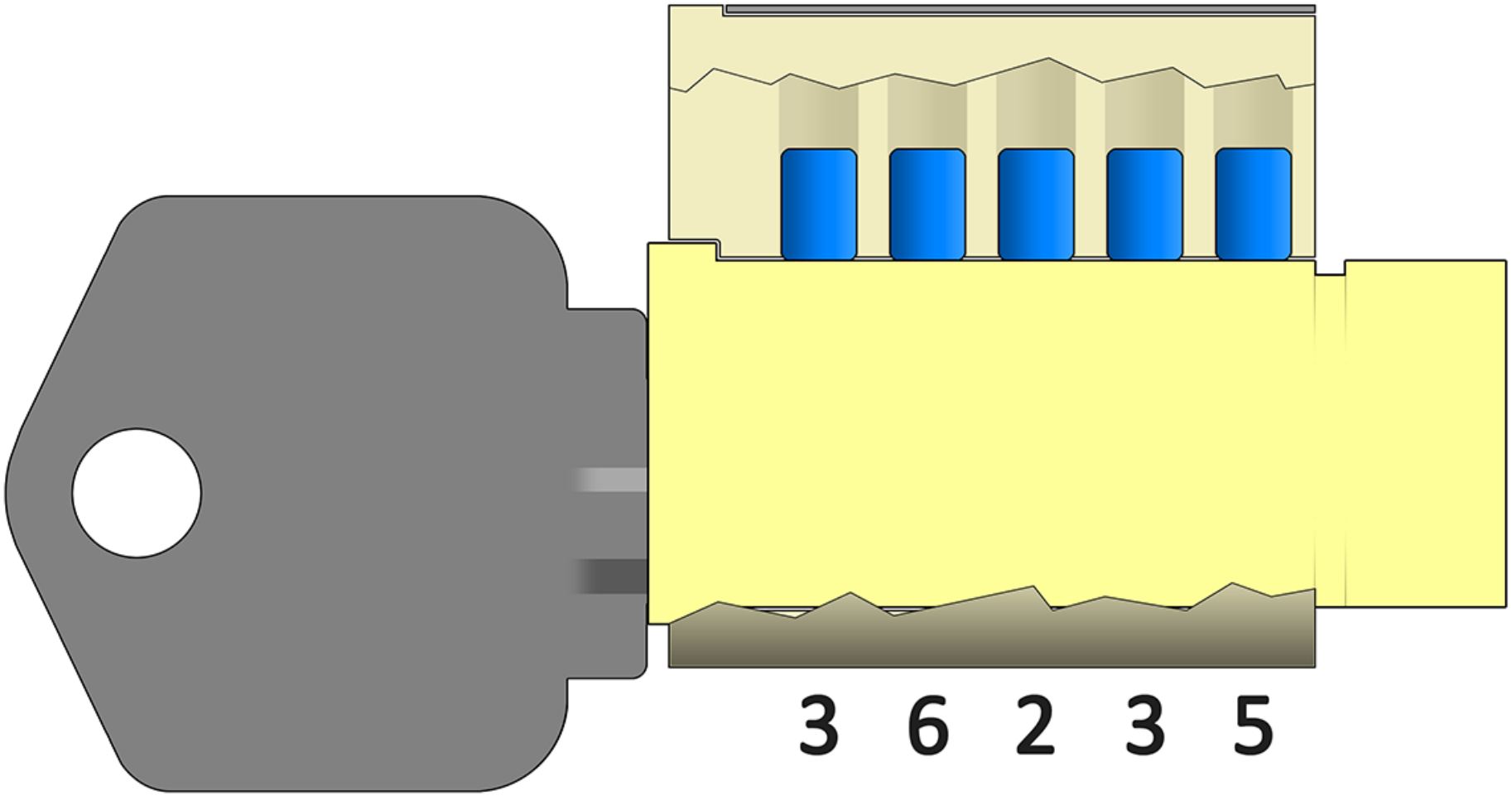
Obviously, it Works in the Lock…



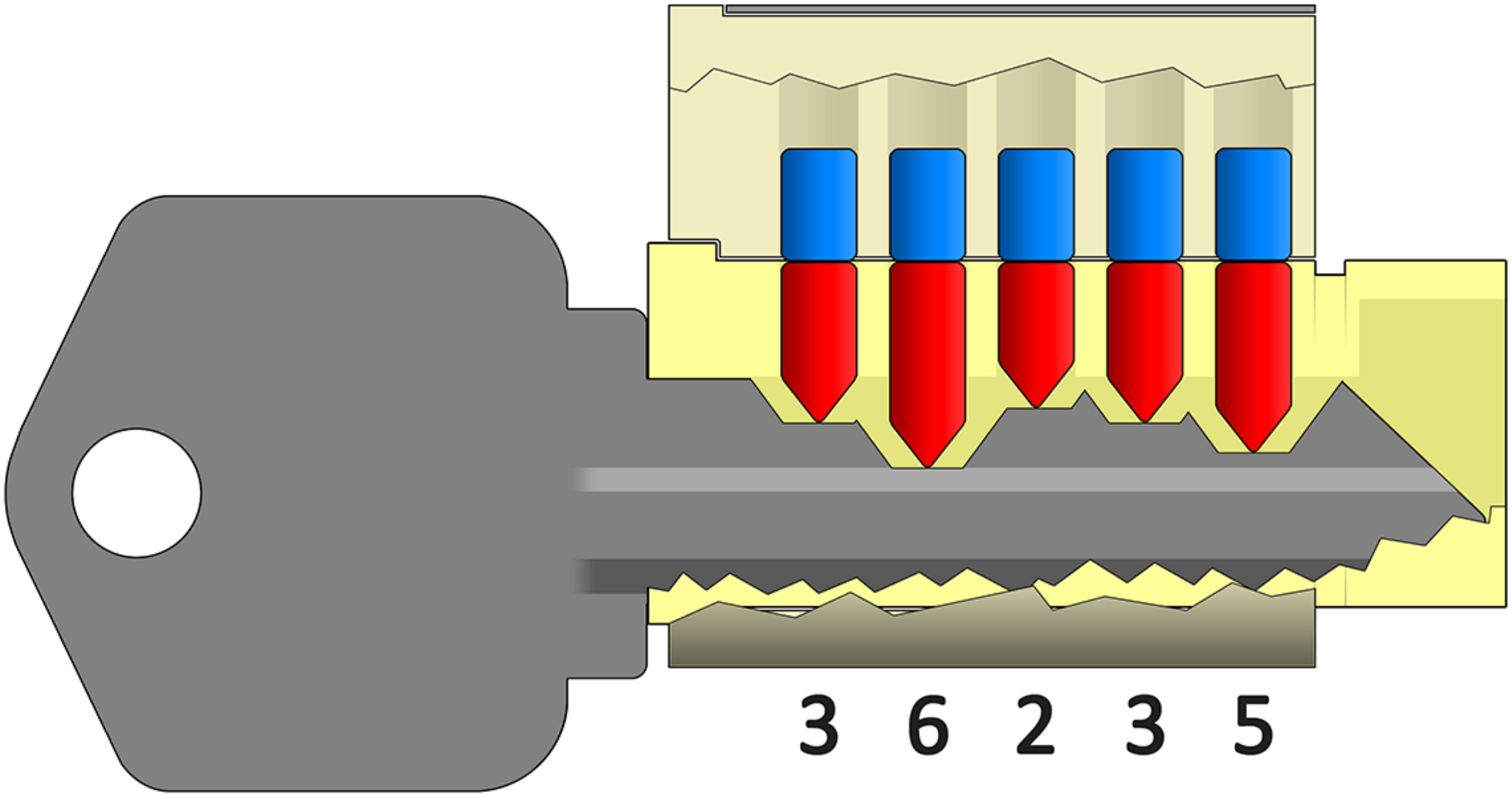
So, What Can We Infer About the



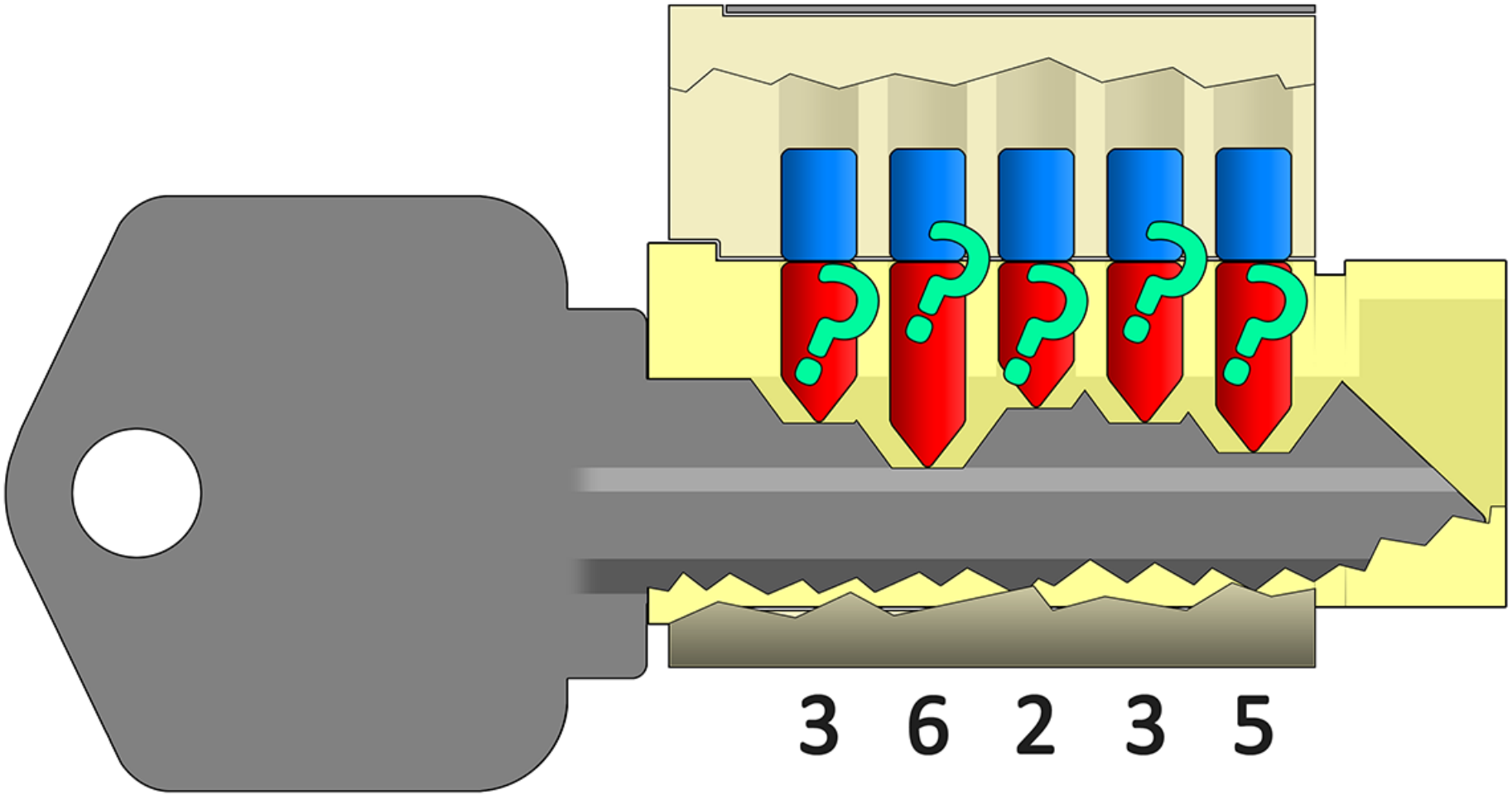
Pins Must Be At the Edge of the



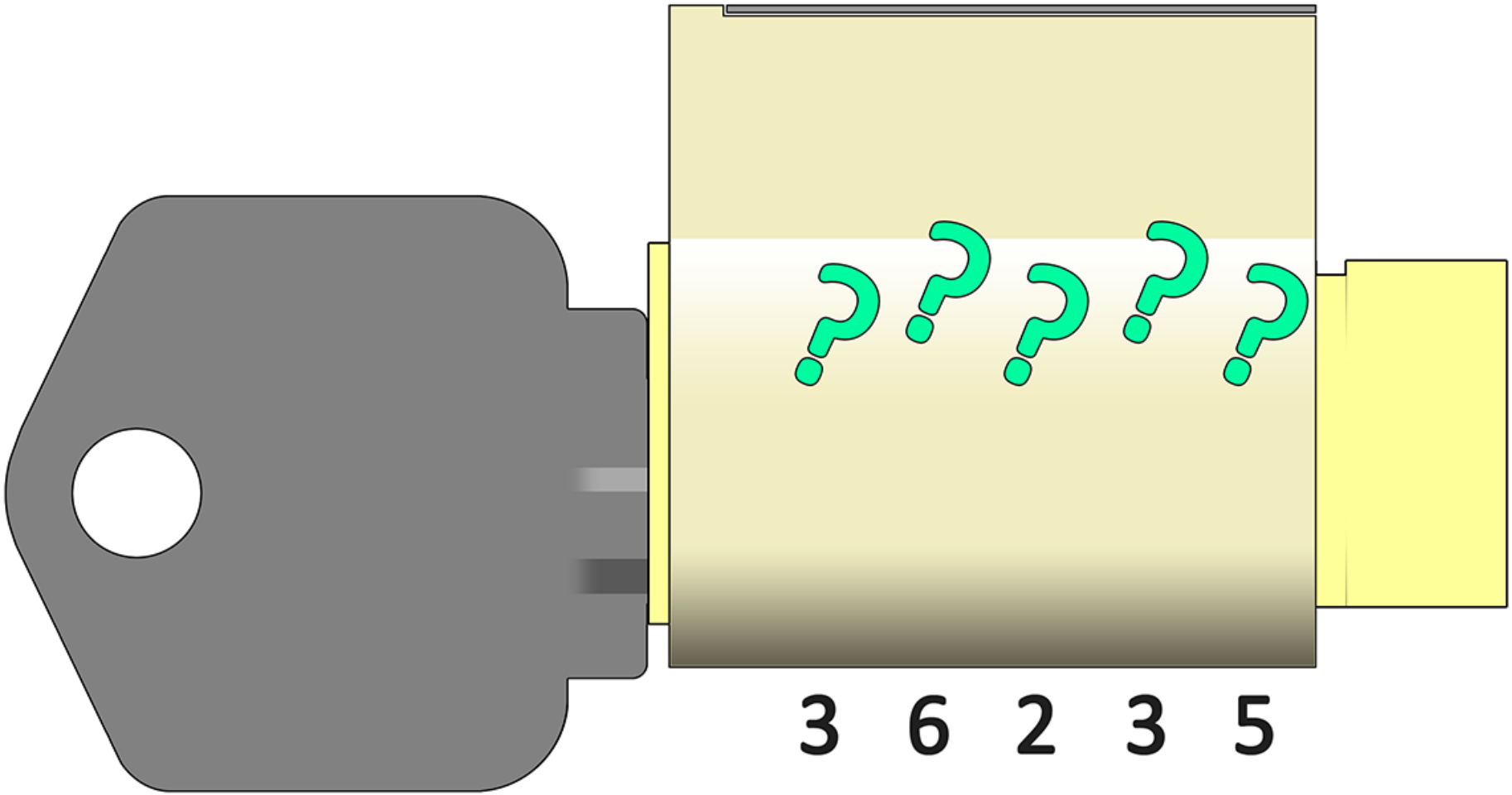
… They Could Simply be Solid Key



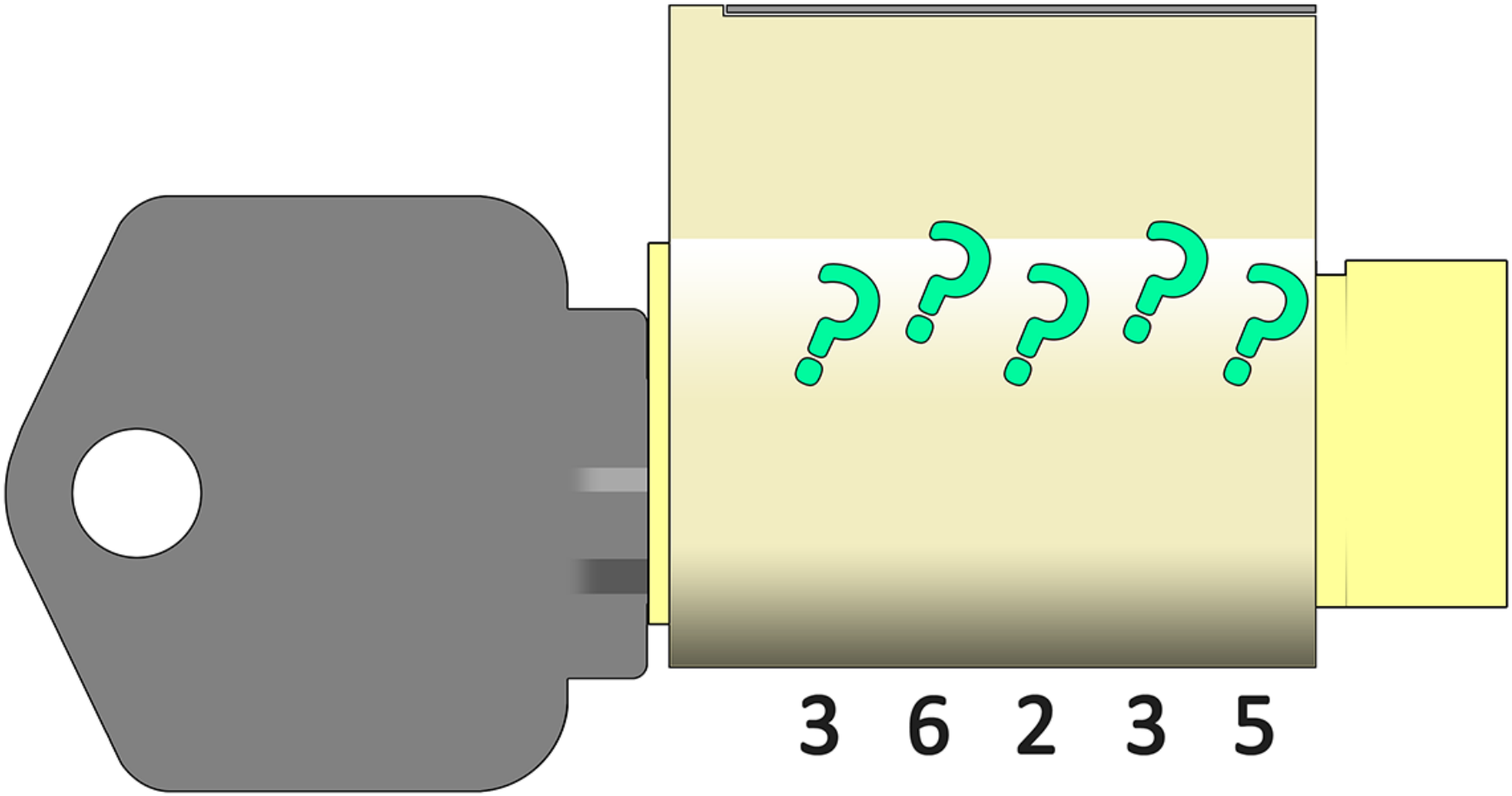
… But the Specific Details are …



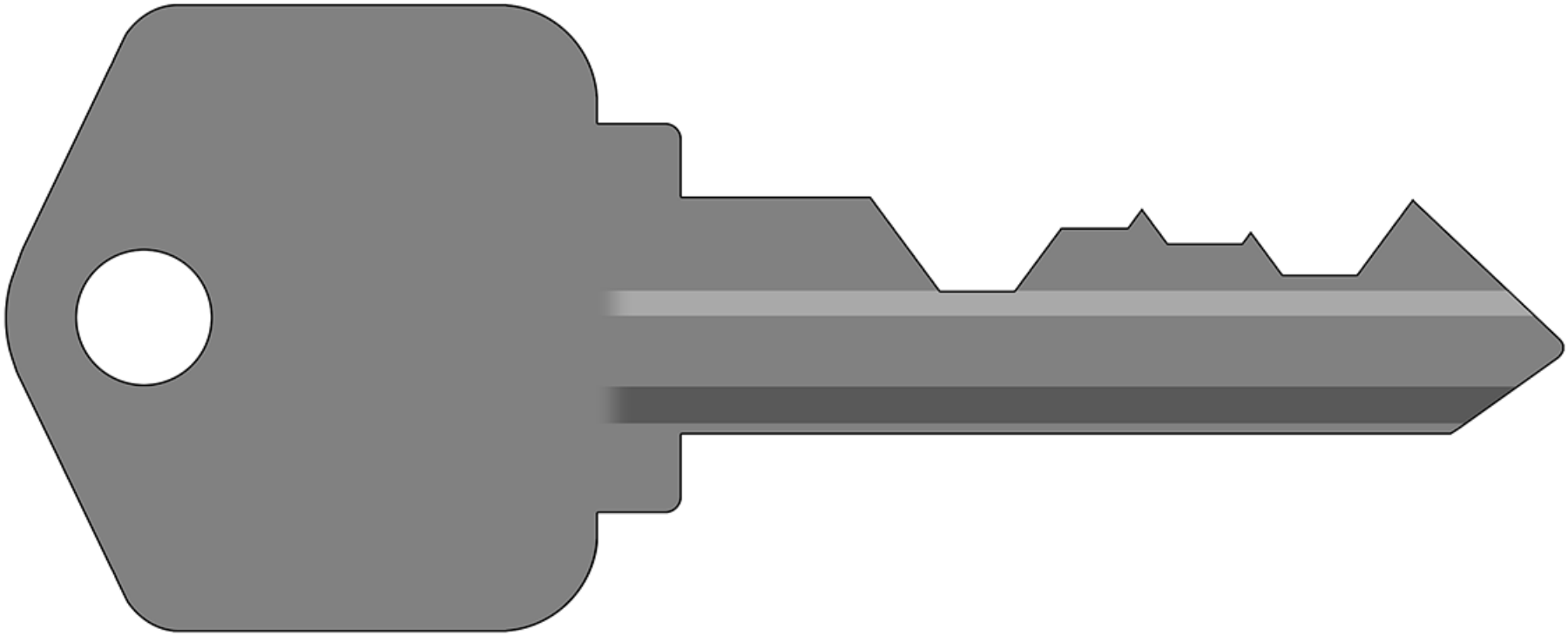
… And these Unknowns are Hidden



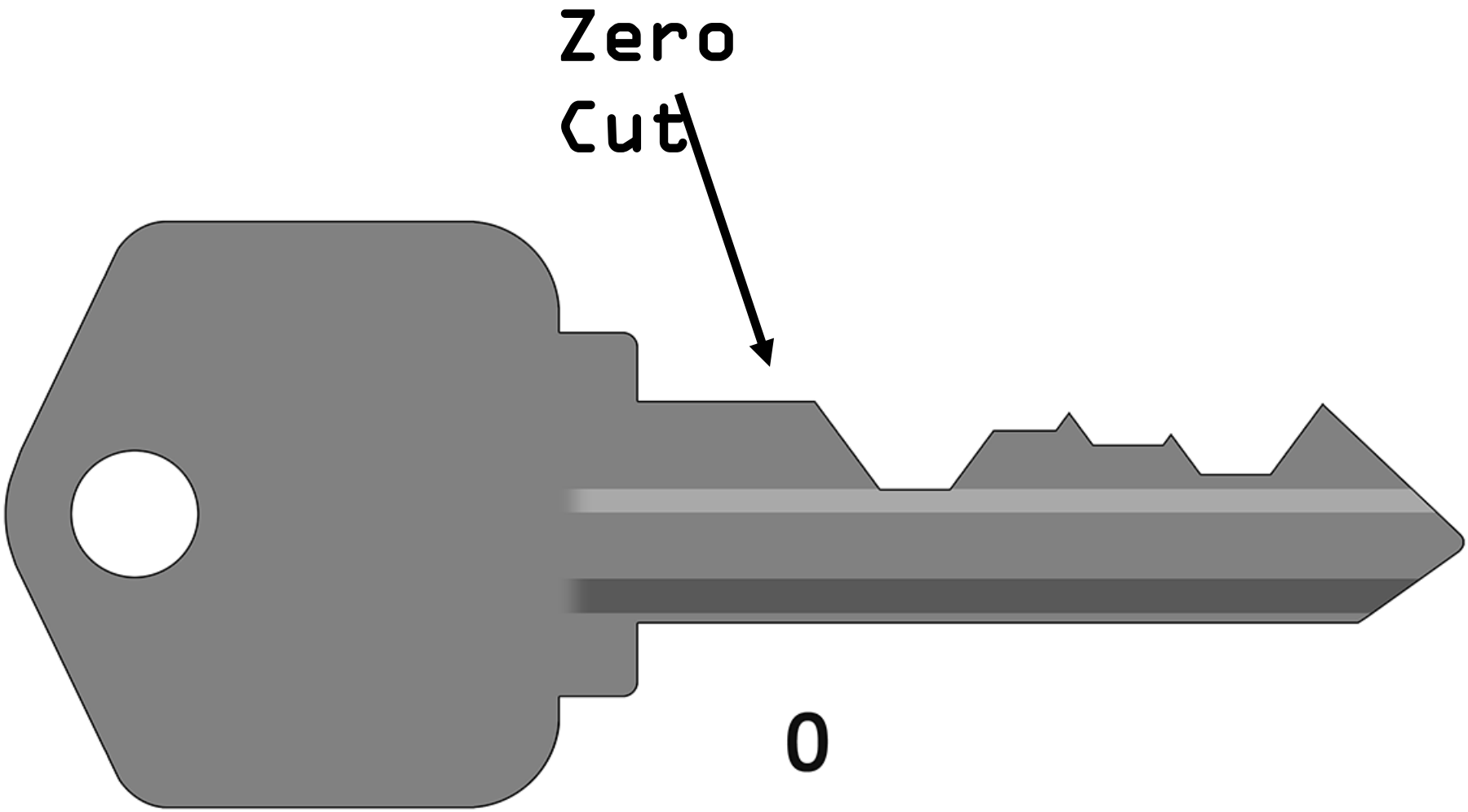
… And these Unknowns are Hidden.



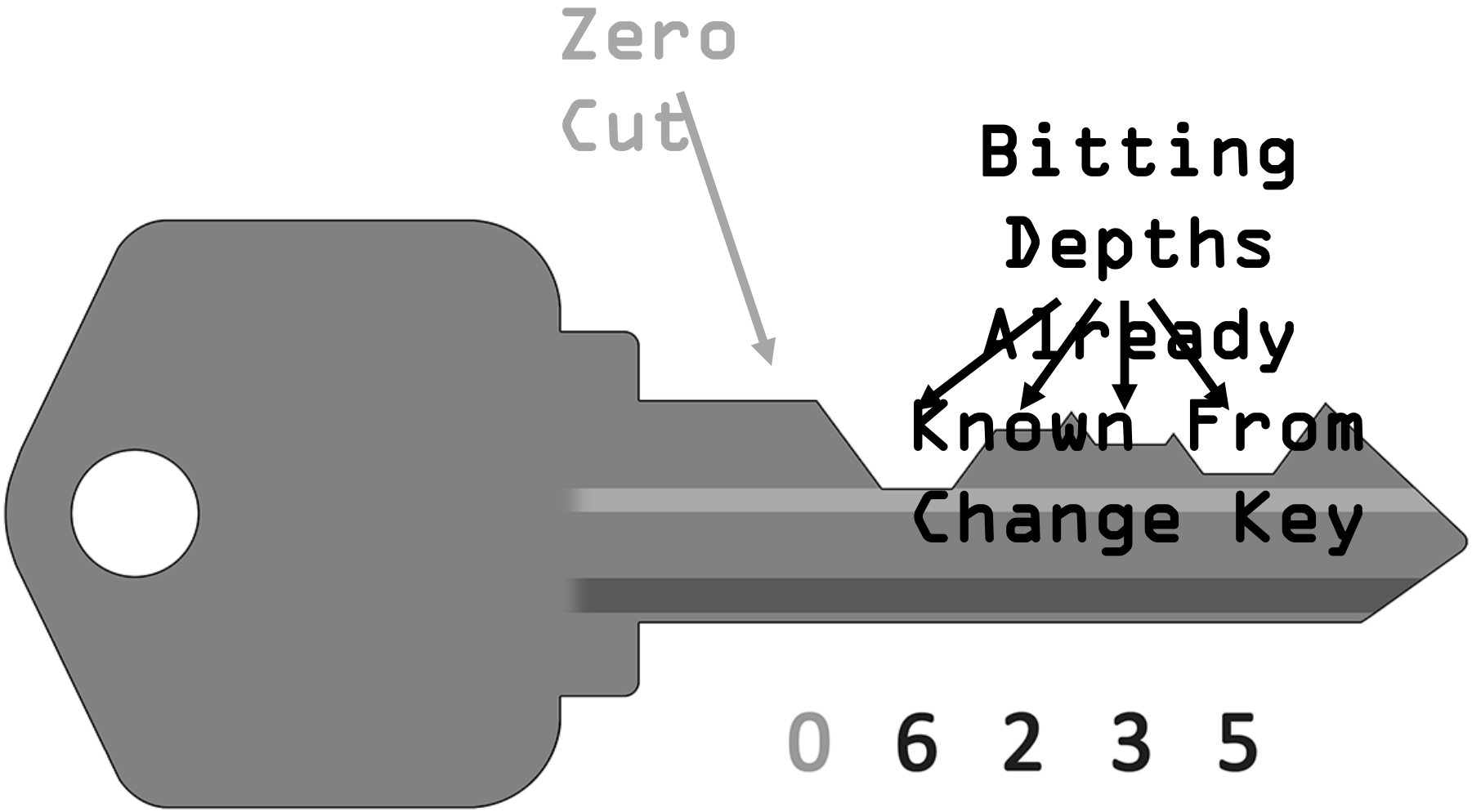
Prepare *Exploratory Key Number*



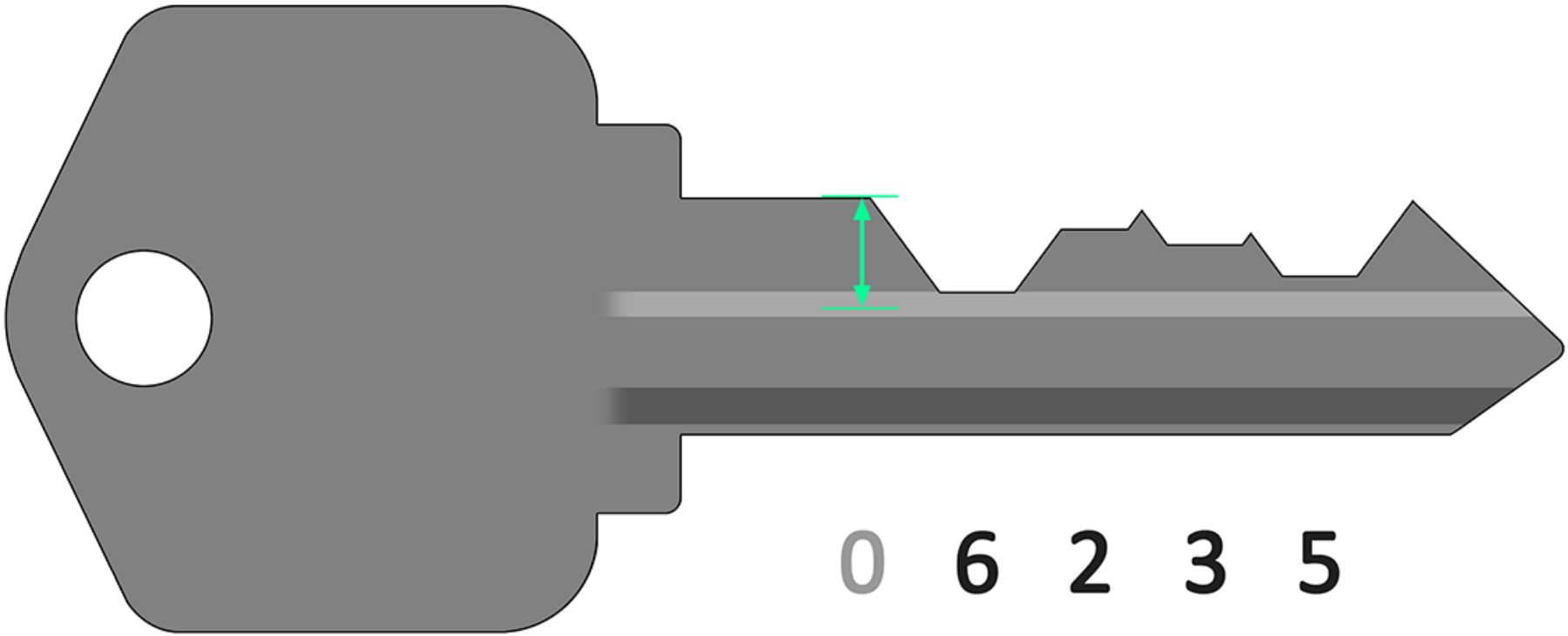
Prepare *Exploratory Key Number*



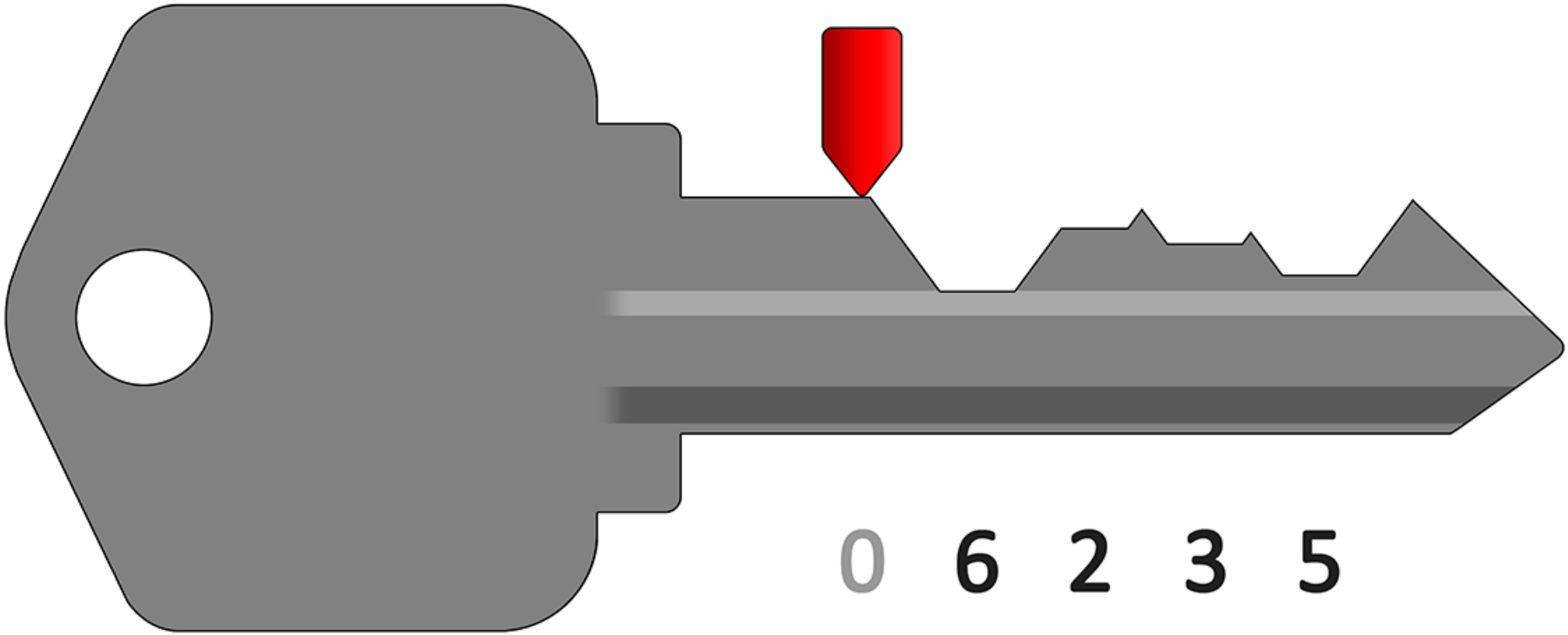
Prepare *Exploratory Key Number*



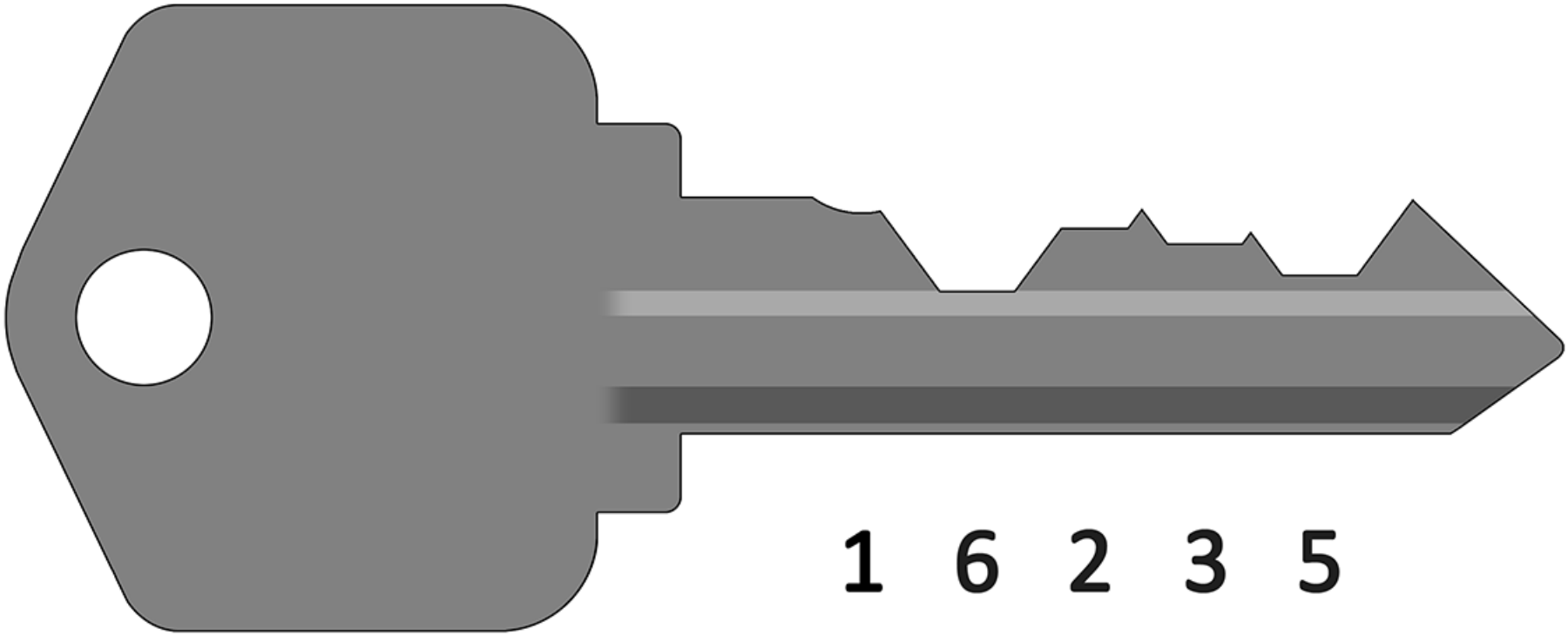
This Key Will be Used to Sweep



Beware That MACS Issues Can

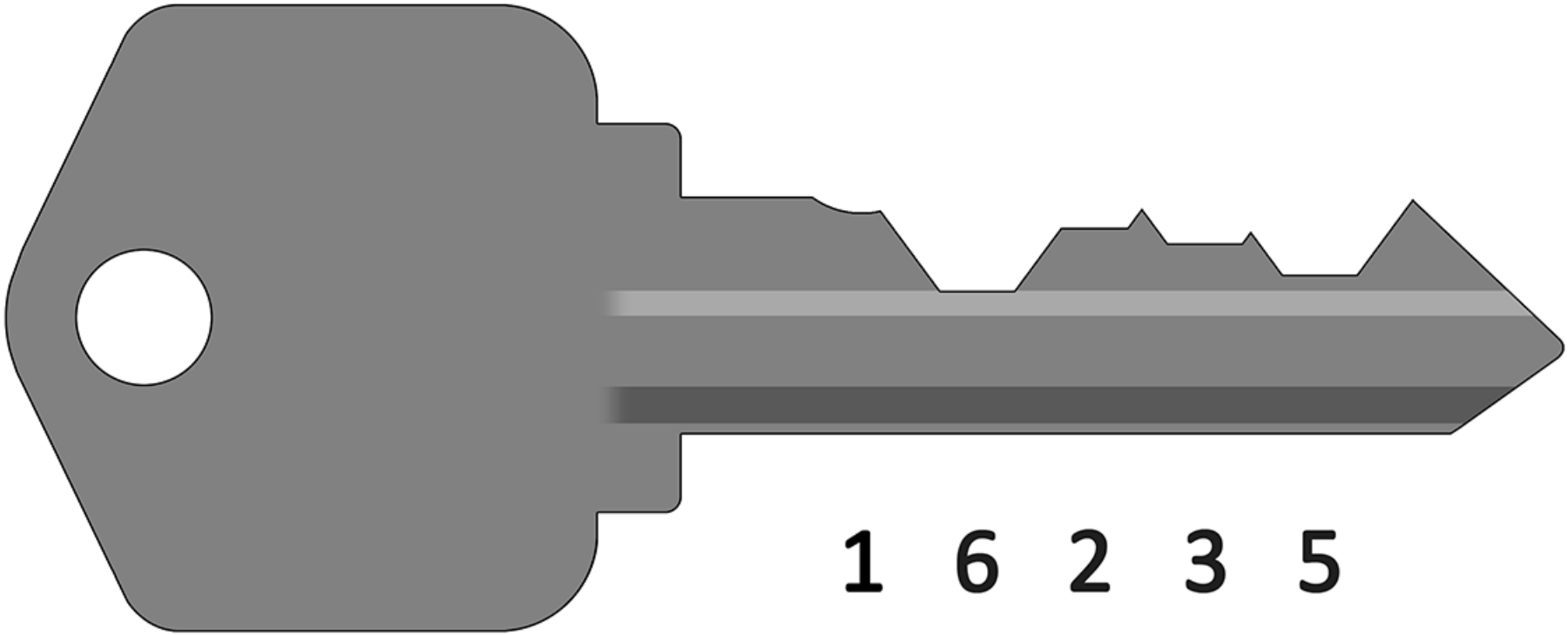


File Position One Down a Bit

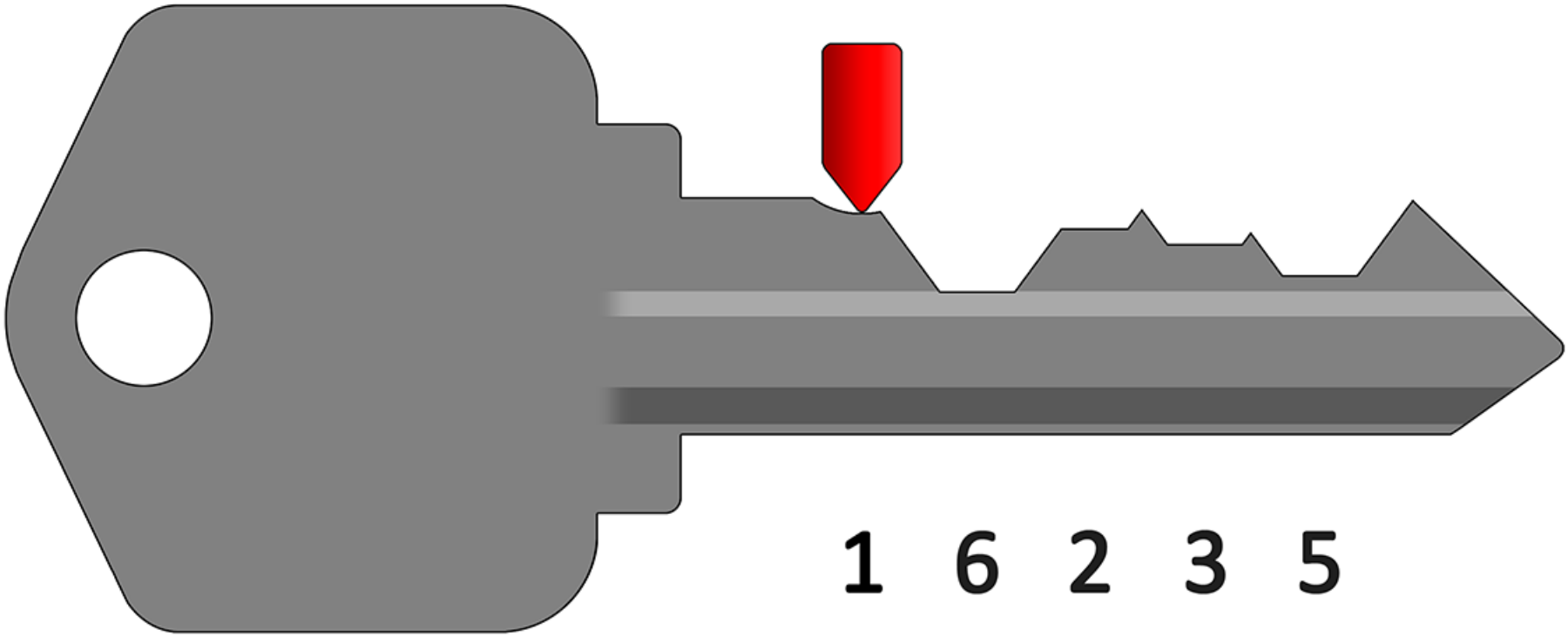


File Position One Down a Bit

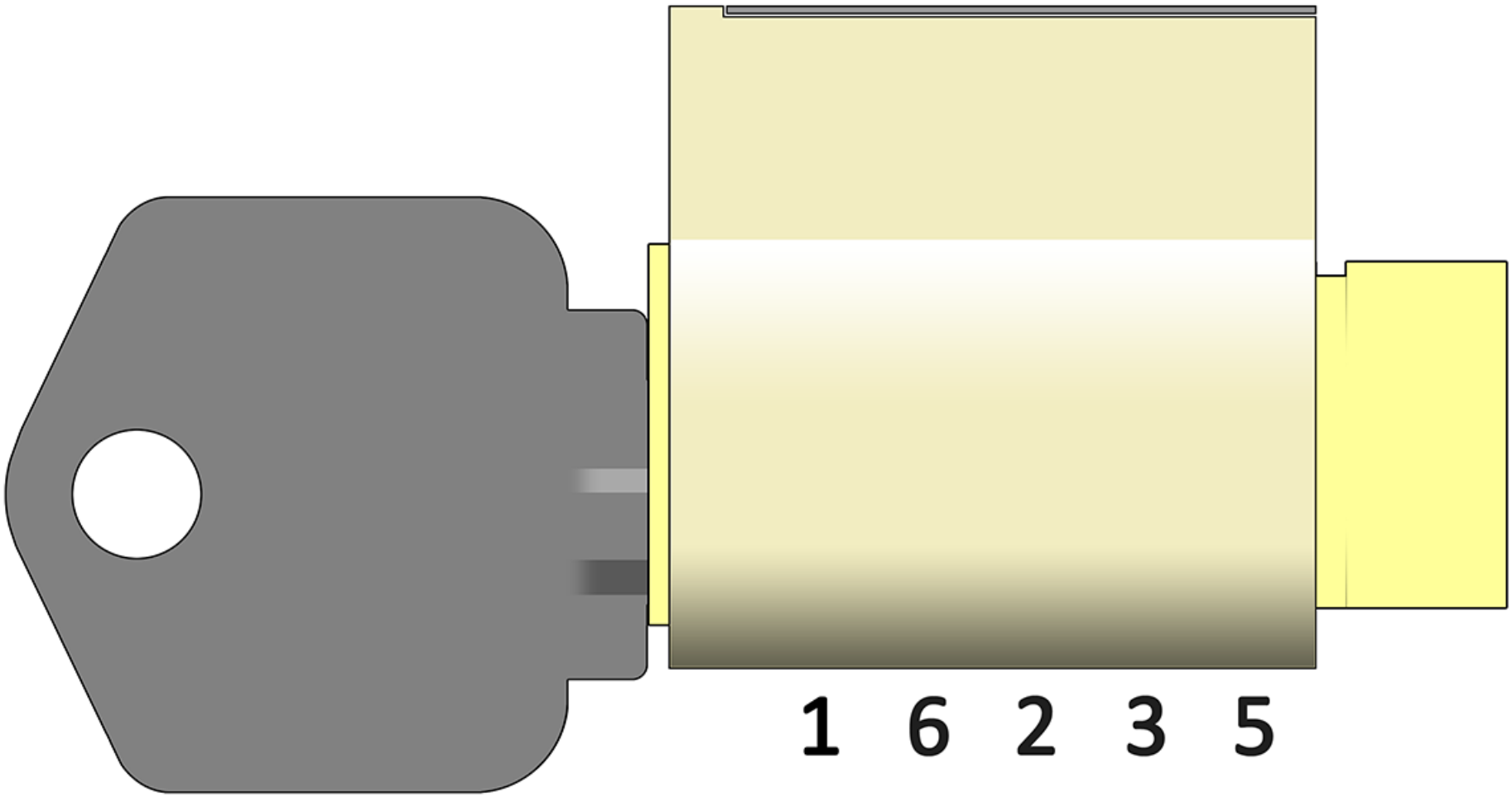
File Position One Down a Bit



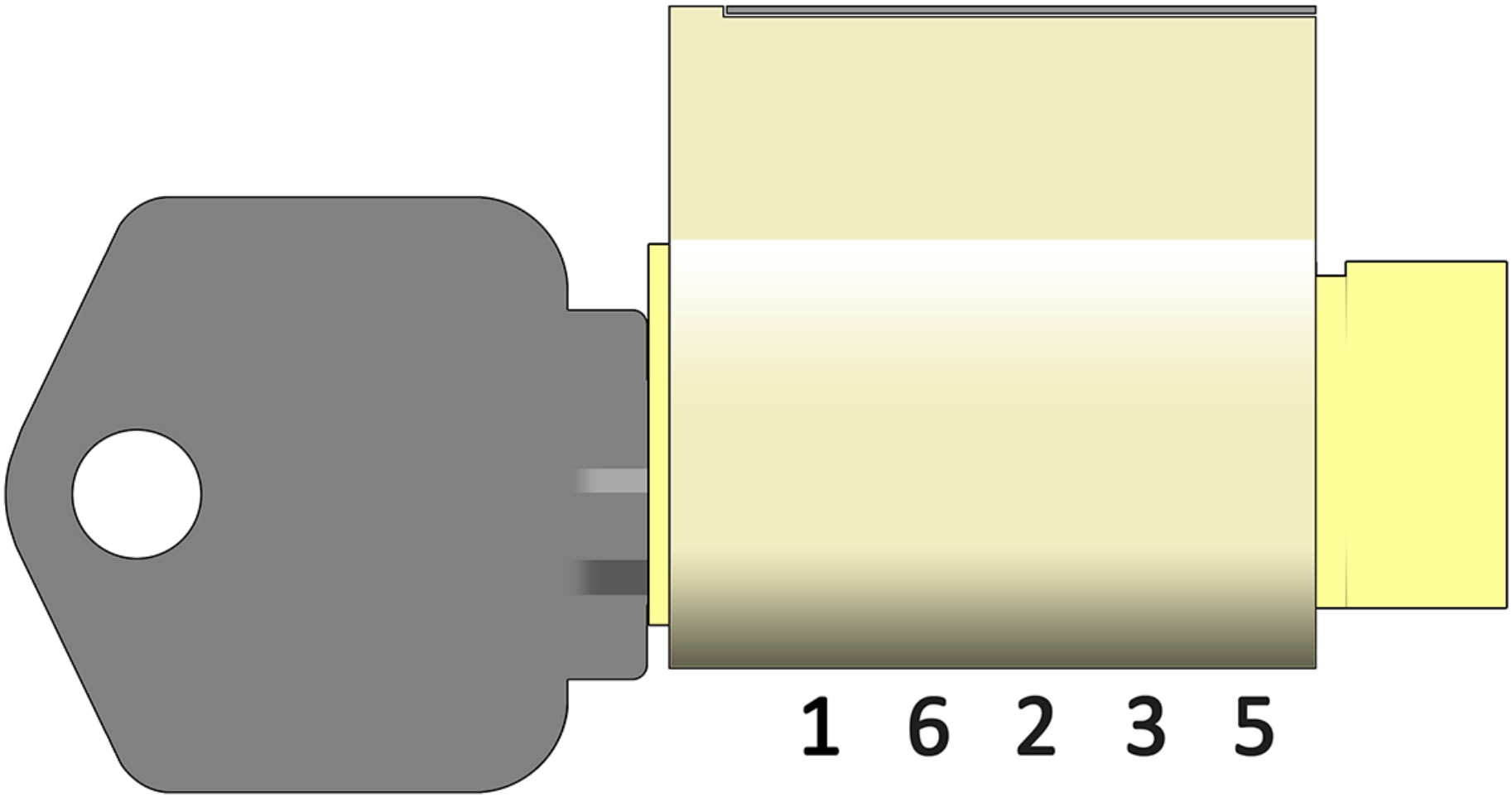
We're Still Encountering MACS



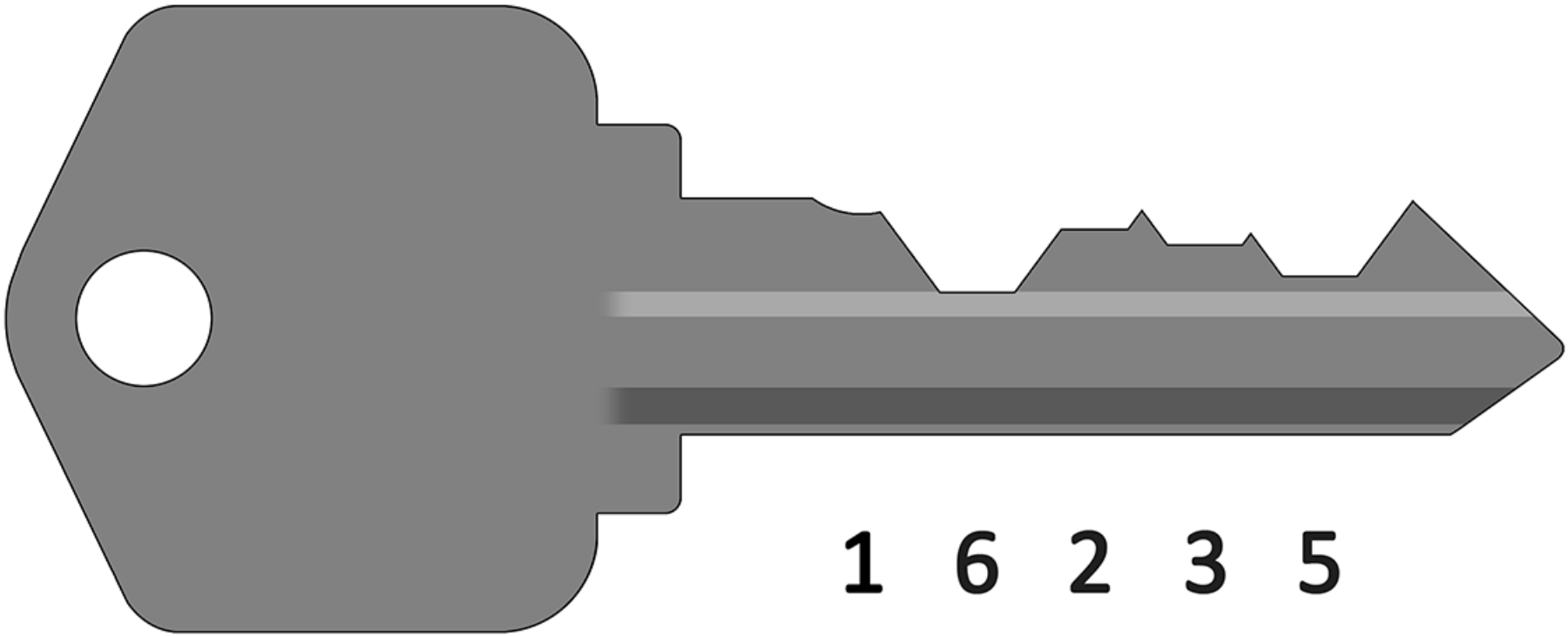
But Let's Try the Key Anyway…



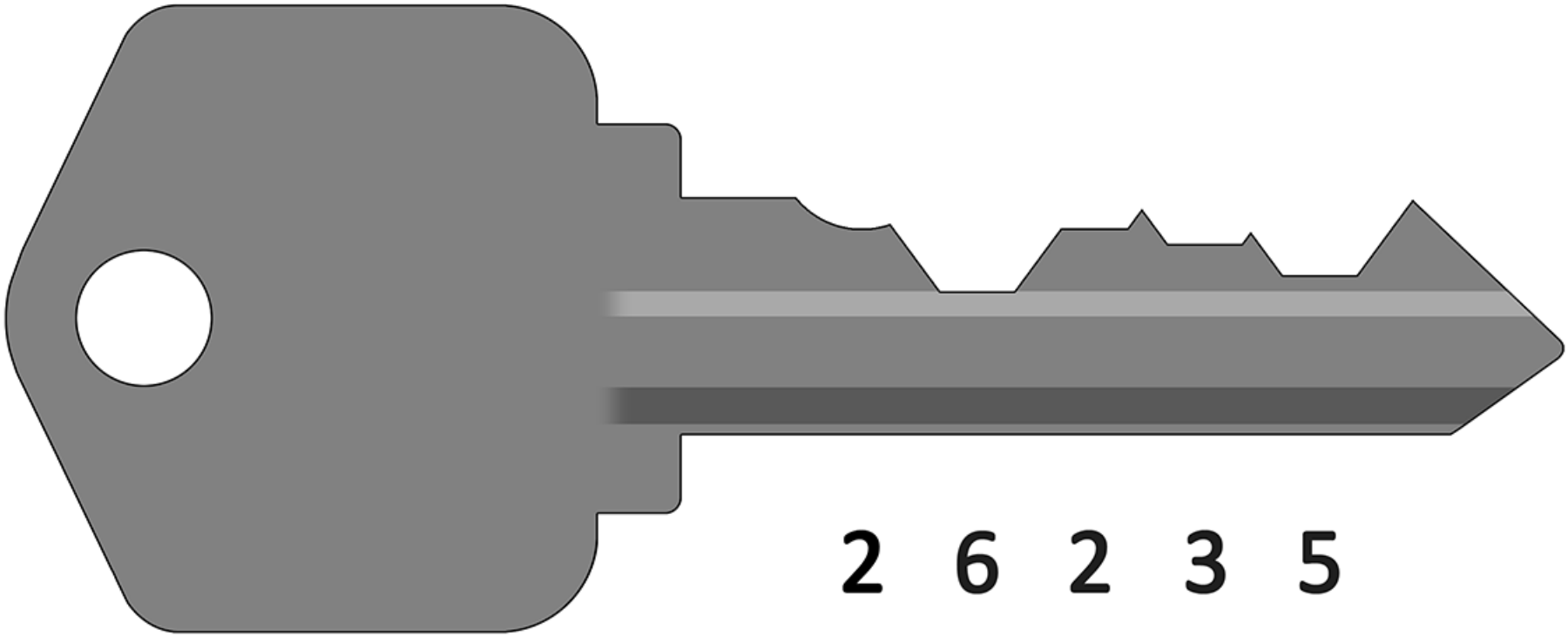
But Let's Try the Key Anyway… the



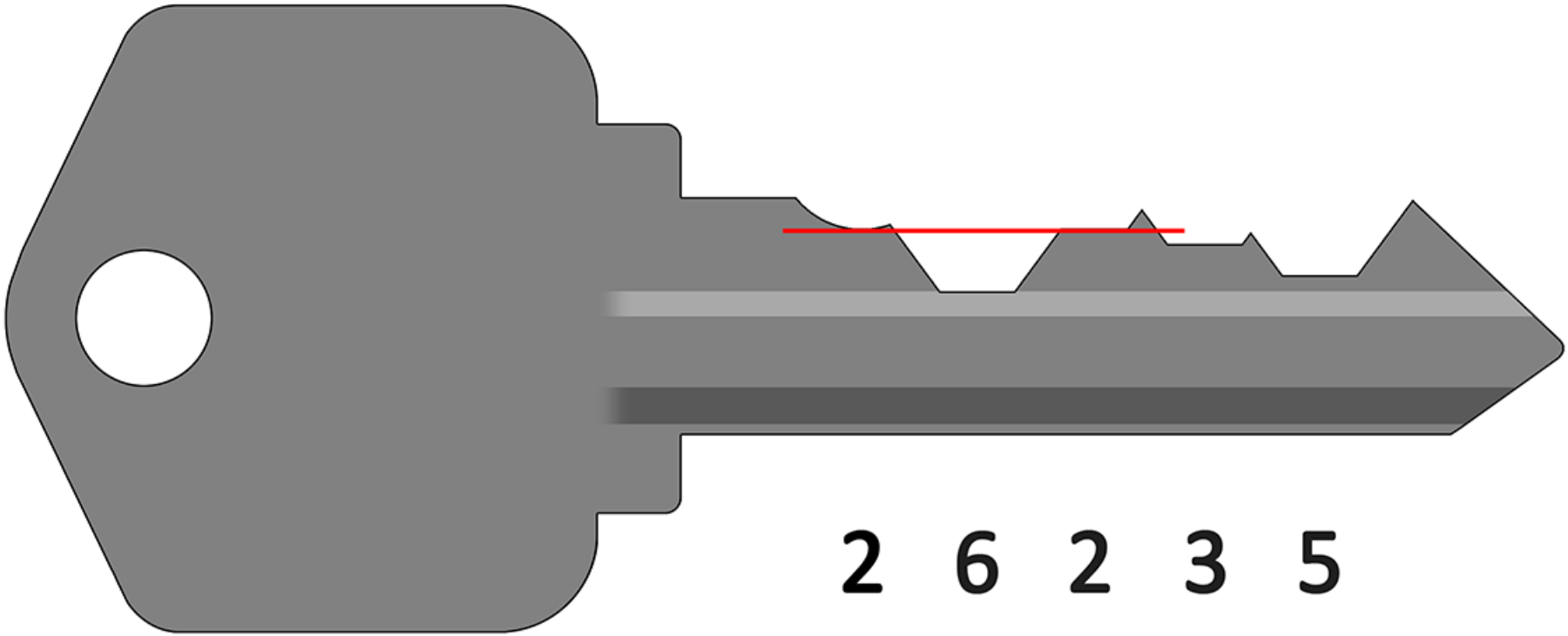
Remove the Key



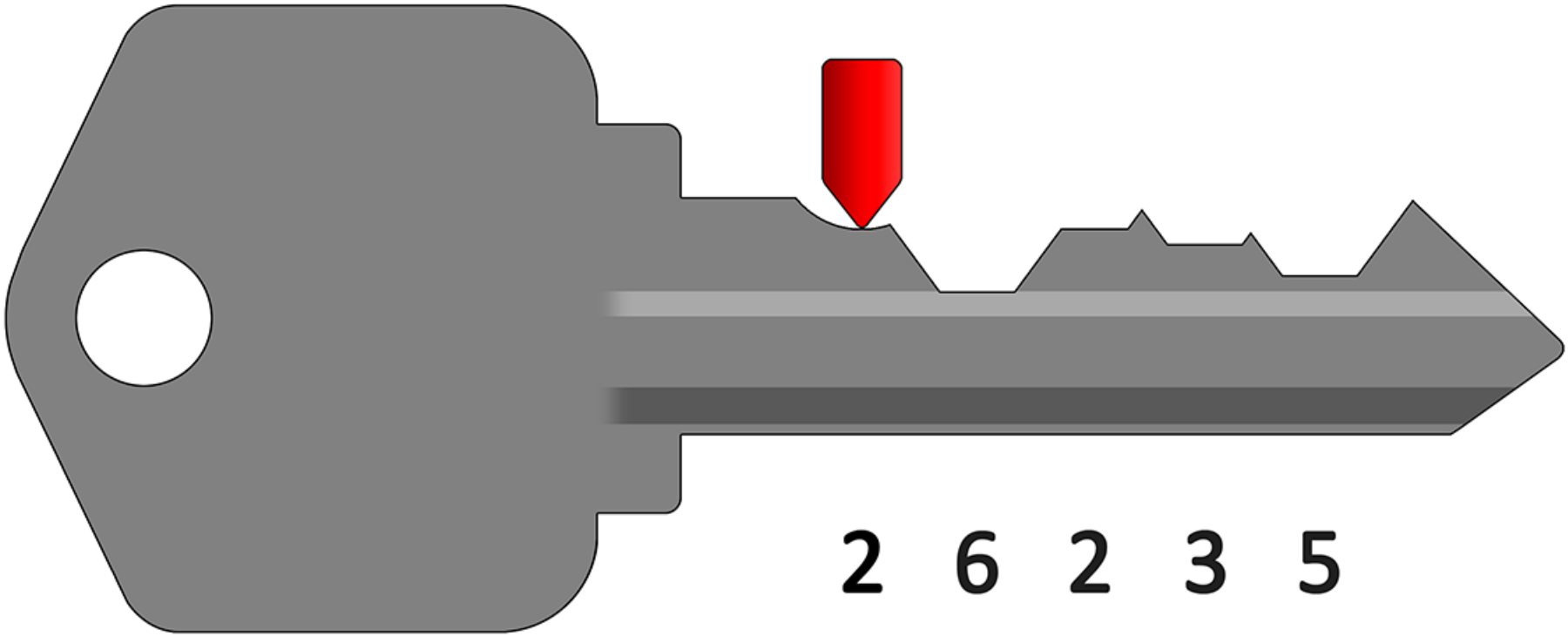
File Position One Down to the



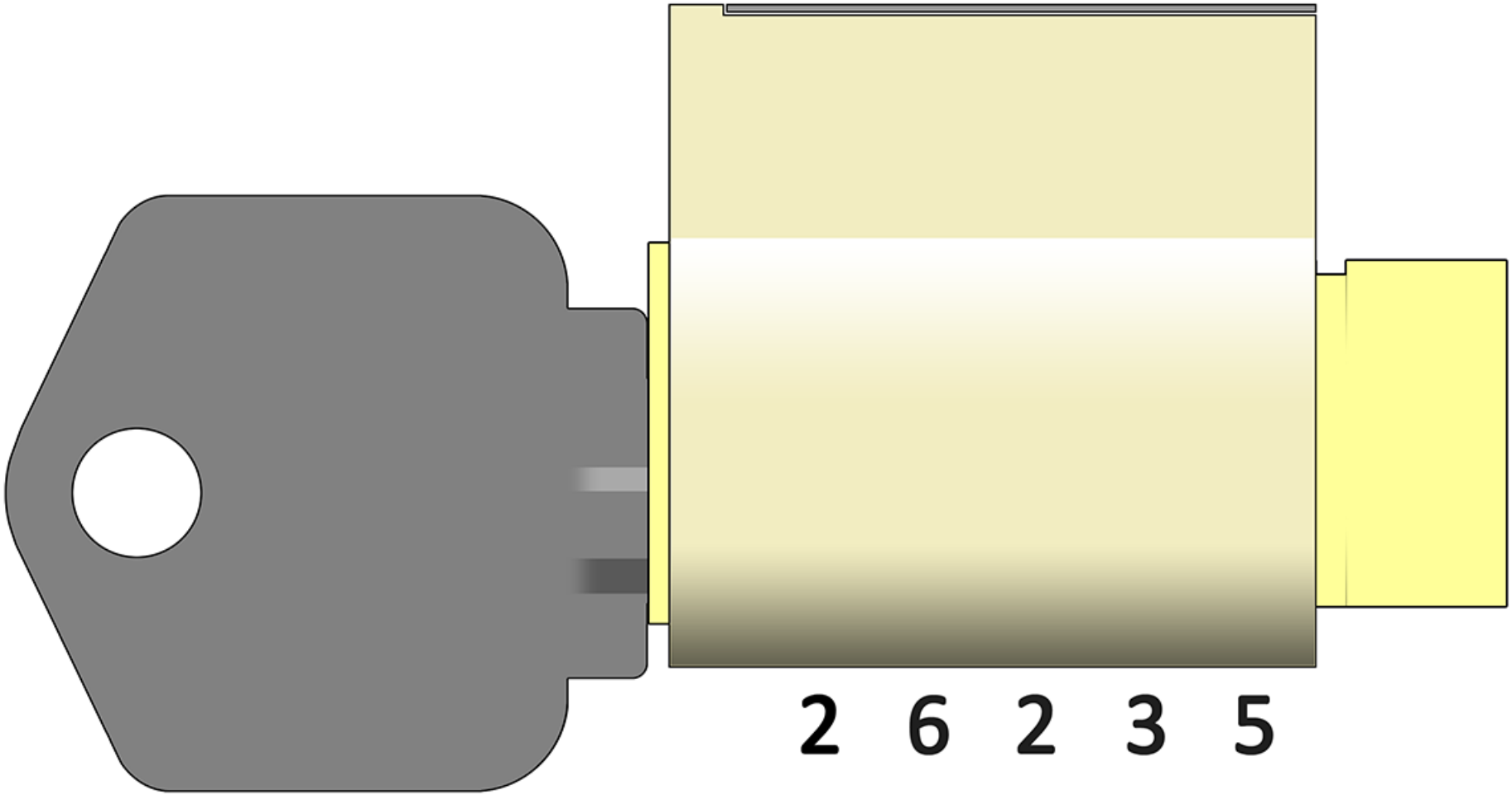
Although They Look Different,



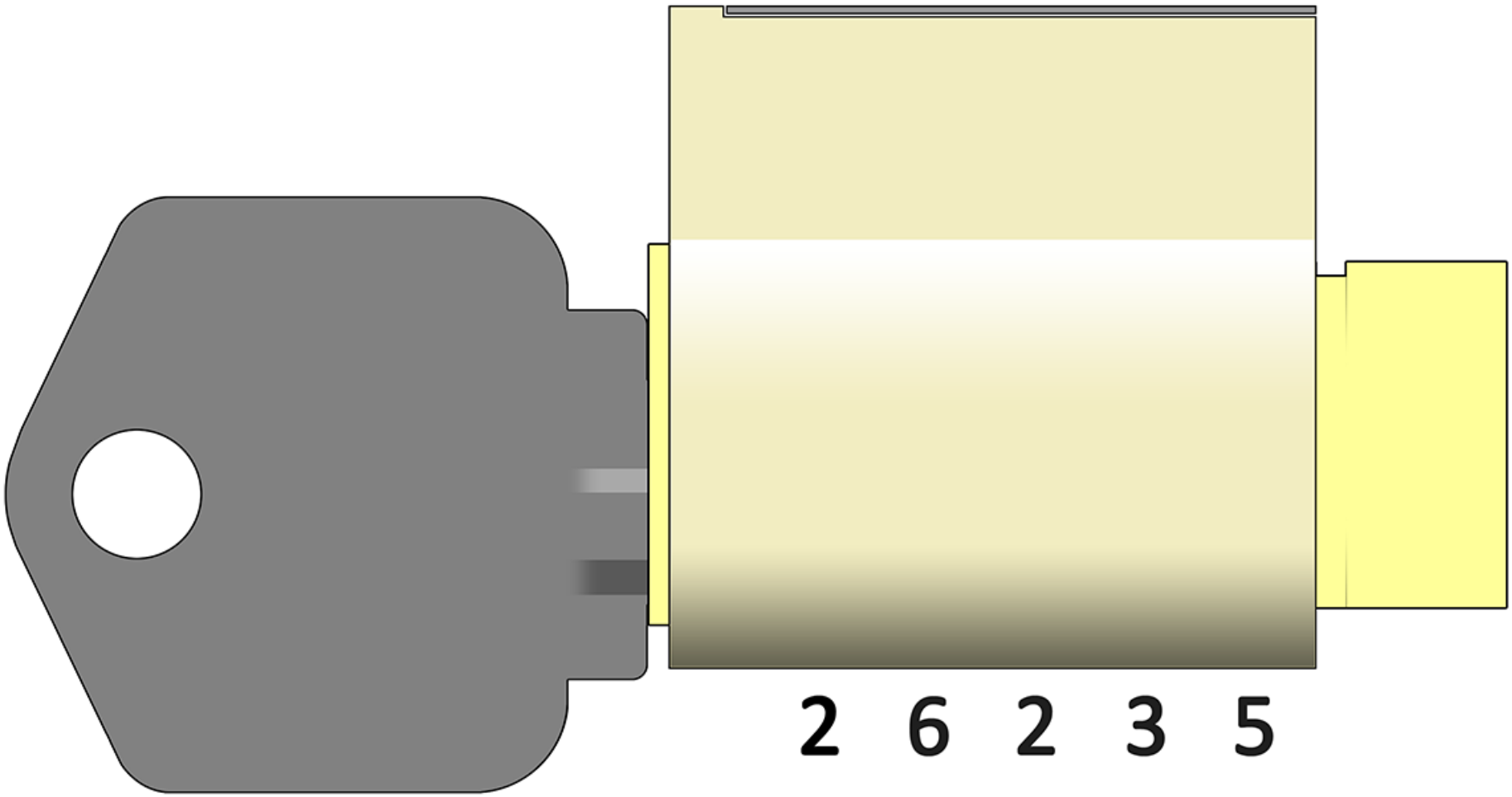
MACS is No Longer Being Violated



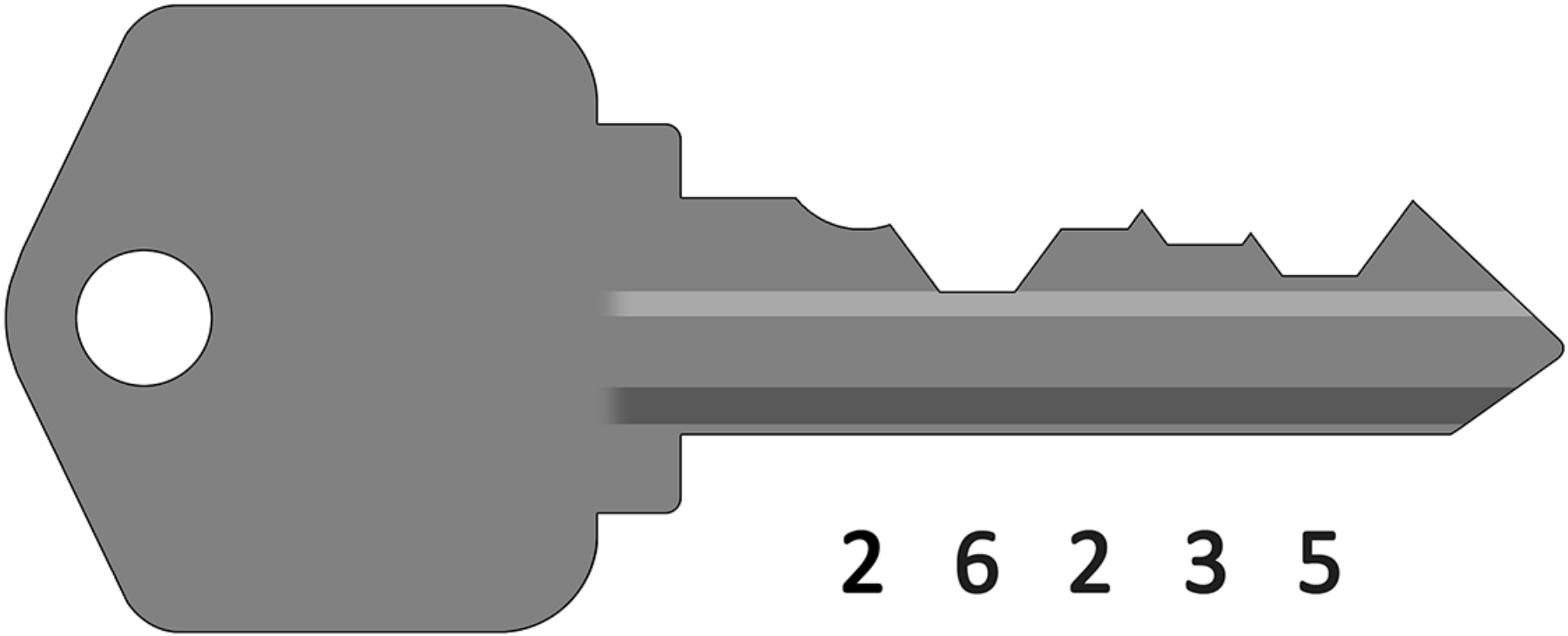
So, Let's Try the Key Again…



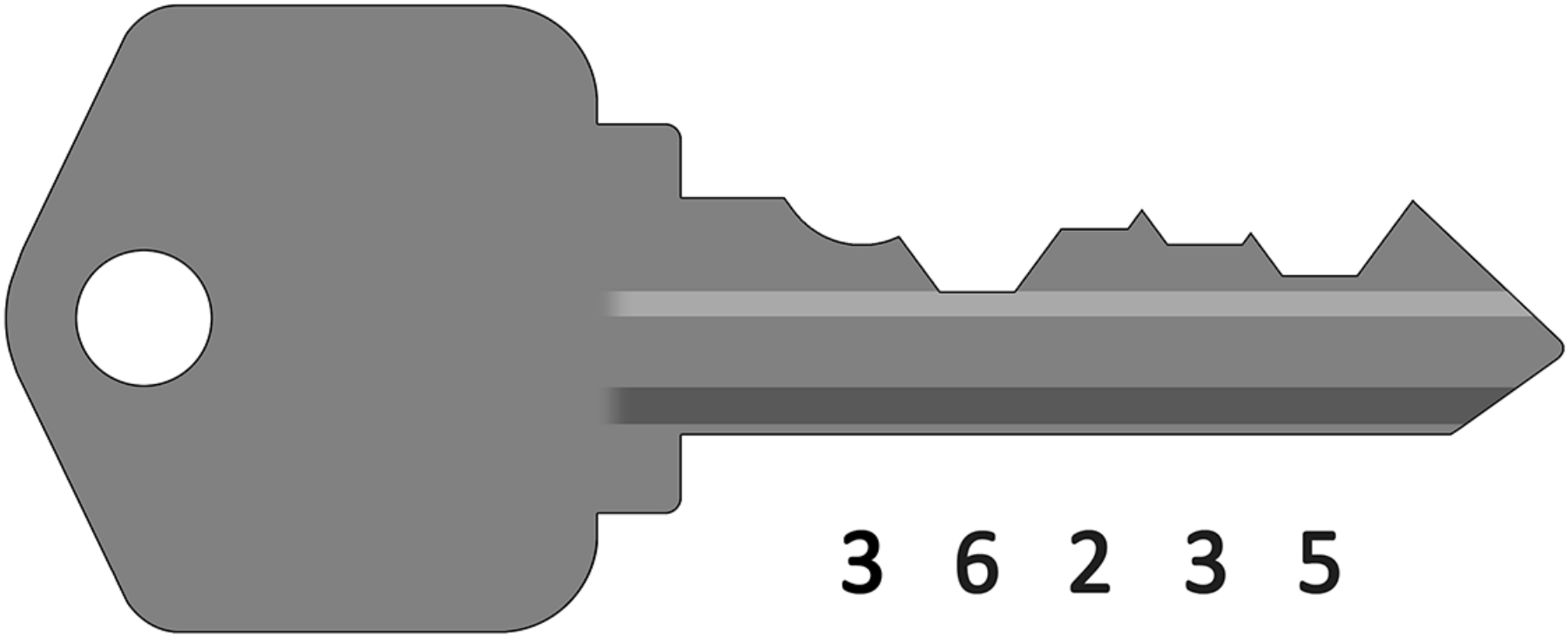
So, Let's Try the Key Again… the



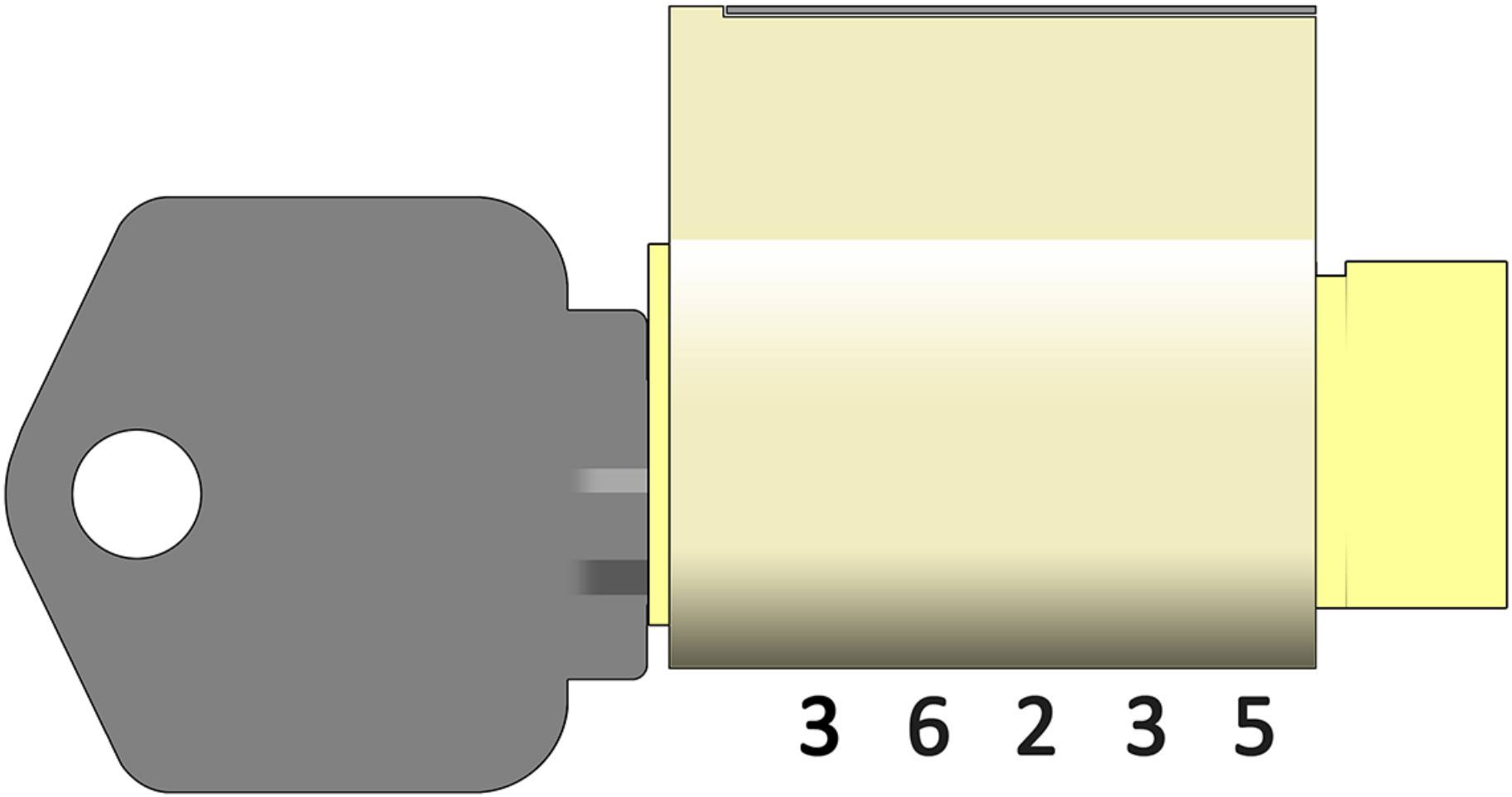
Remove the Key



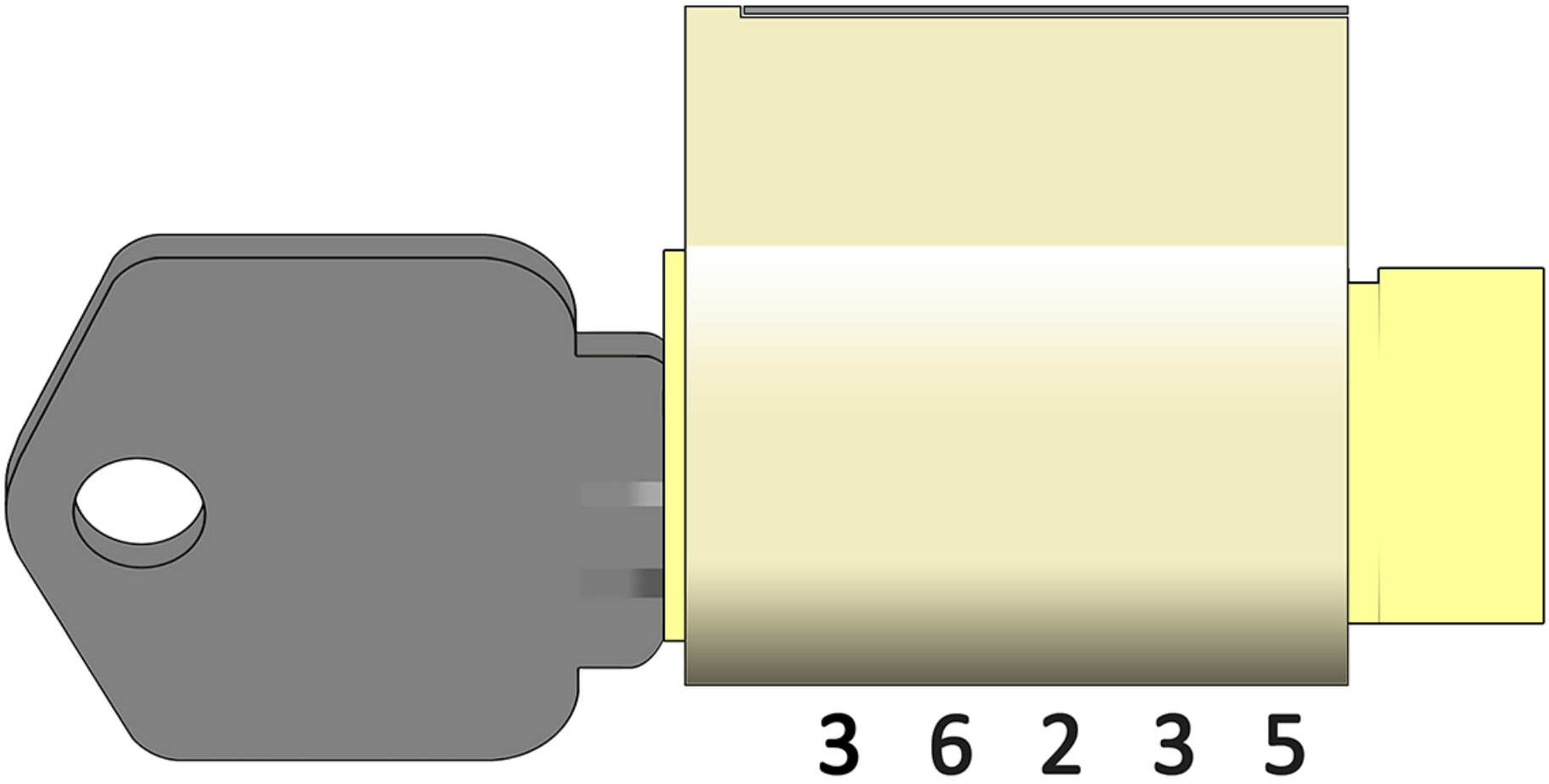
File Down Position One Again



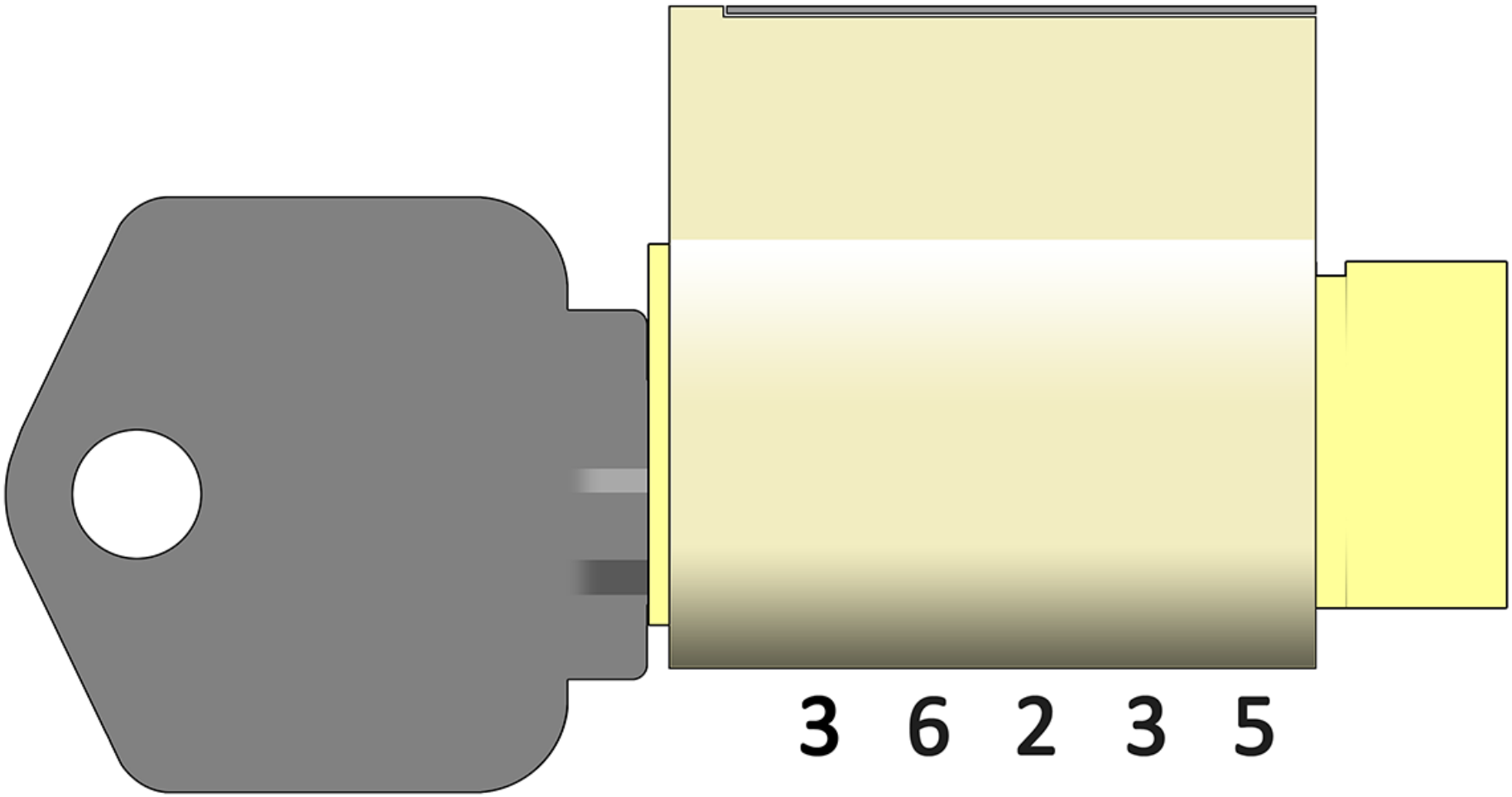
Let's Try The Key Again…



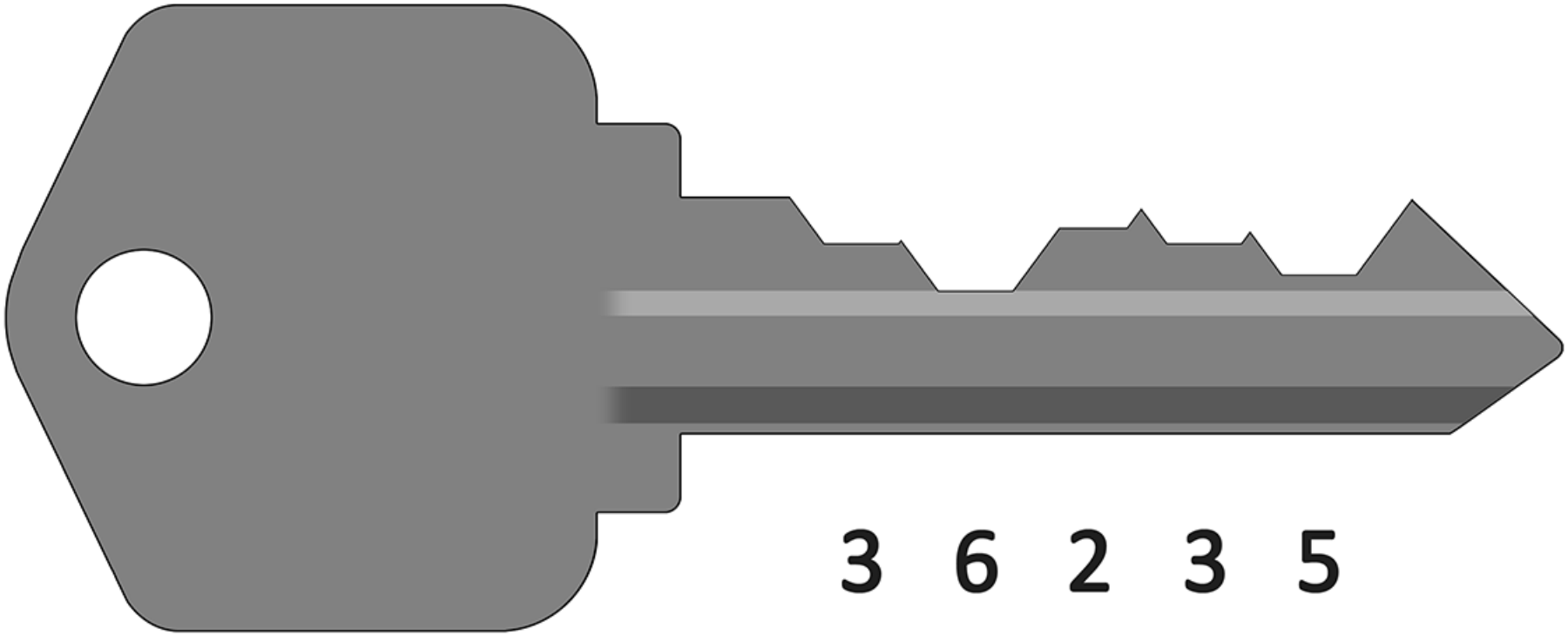
Let's Try The Key Again…OPEN!



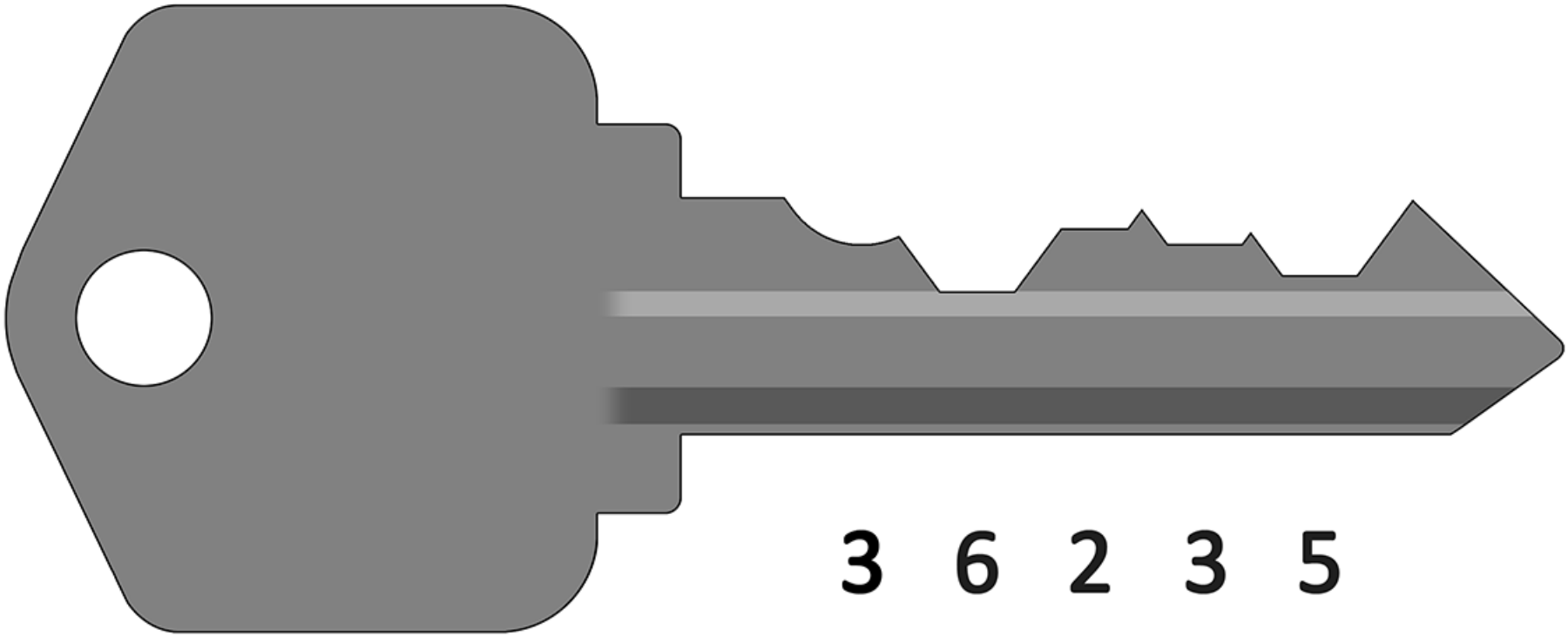
Of Course, That Was Expected



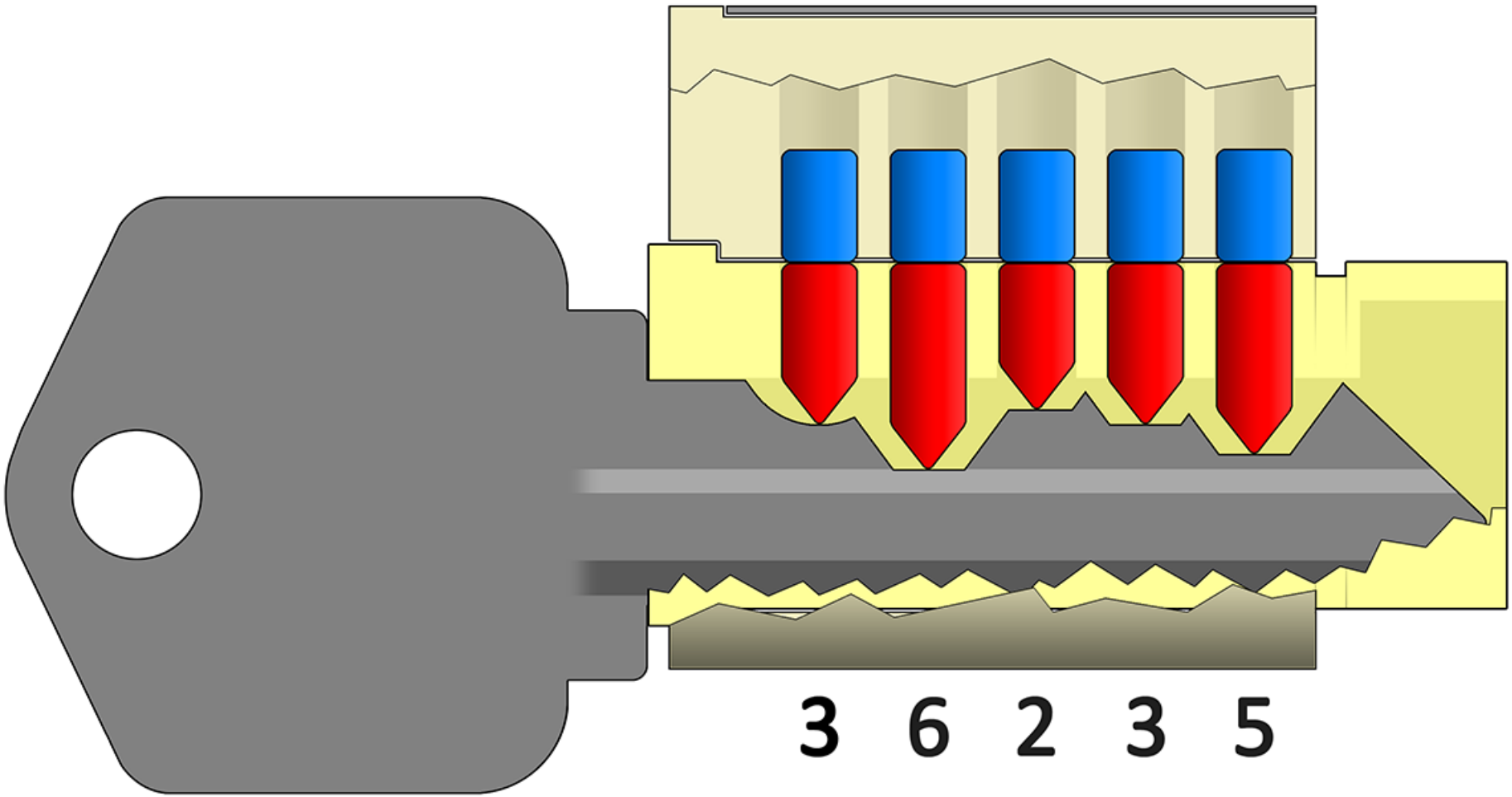
Remember the Change Key?



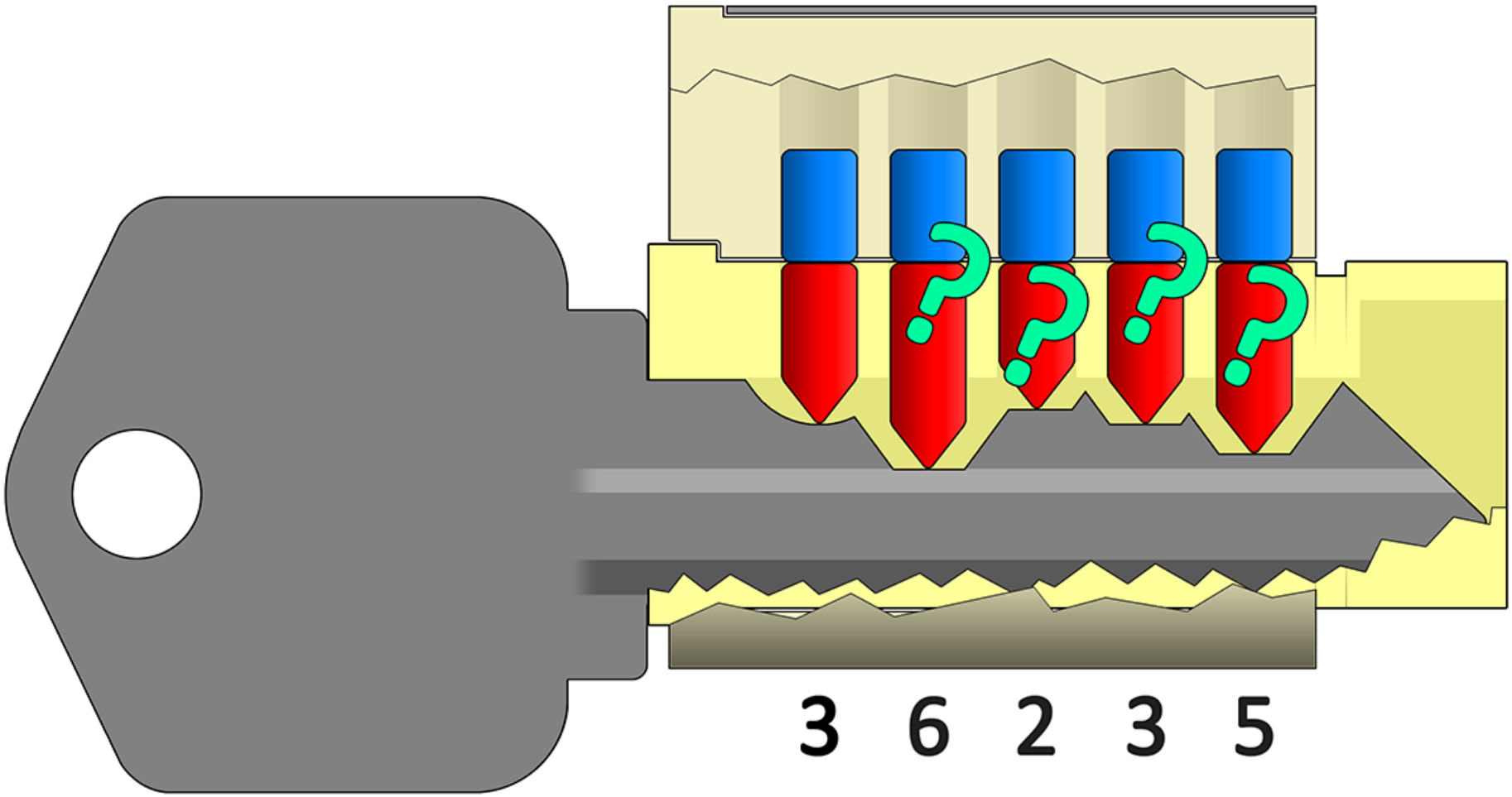
We've Duplicated That



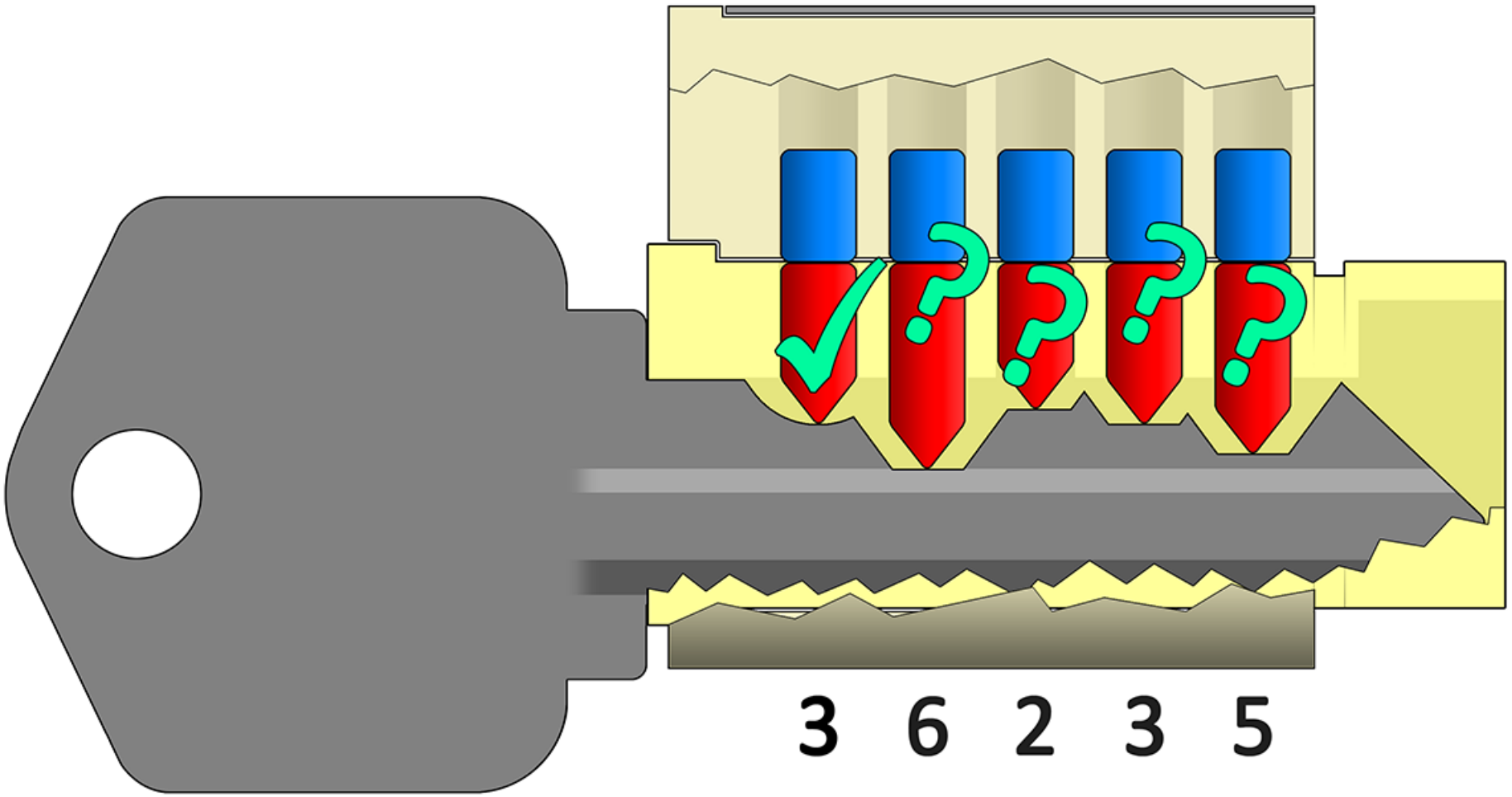
We Have Learned Something,



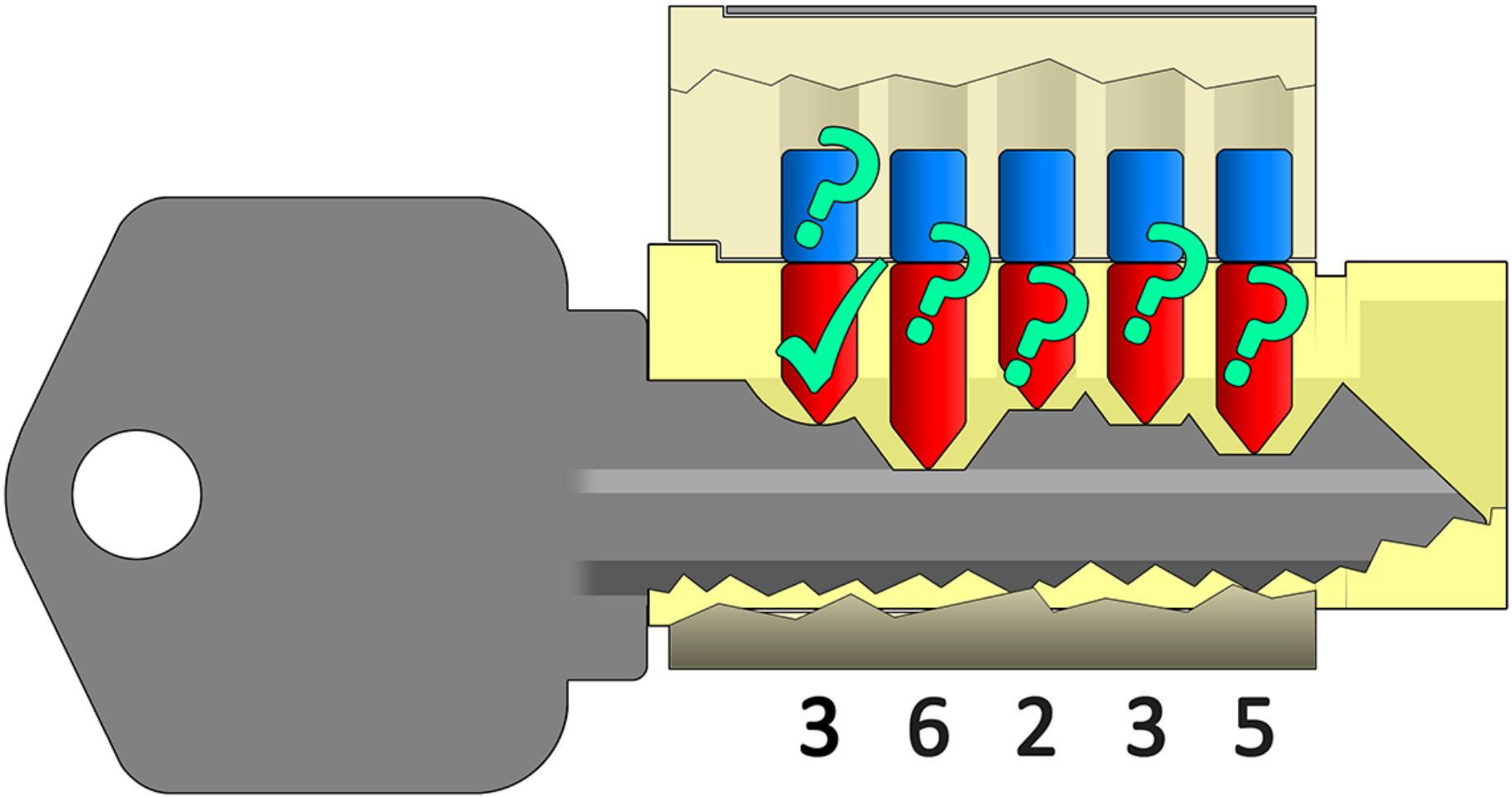
We Don't Know About These



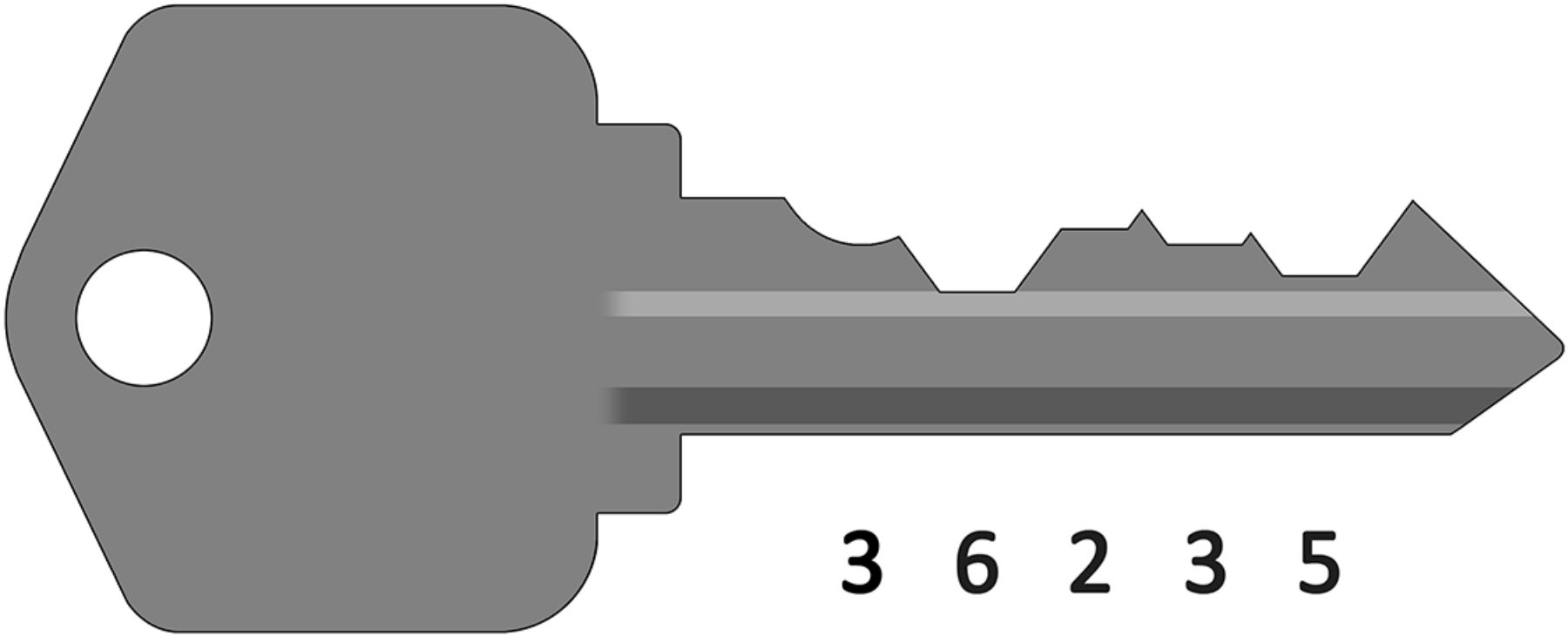
But *Now We Know* That This Key



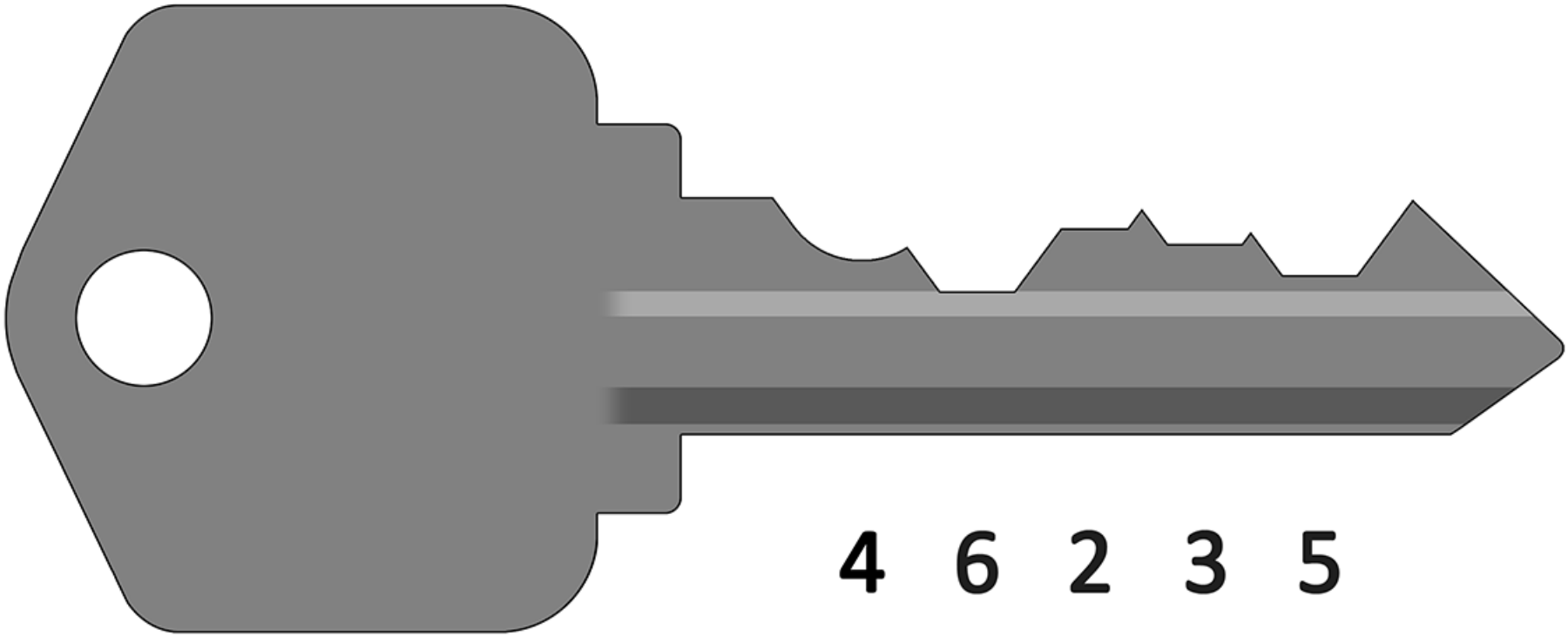
Of Course, There Could Still Be



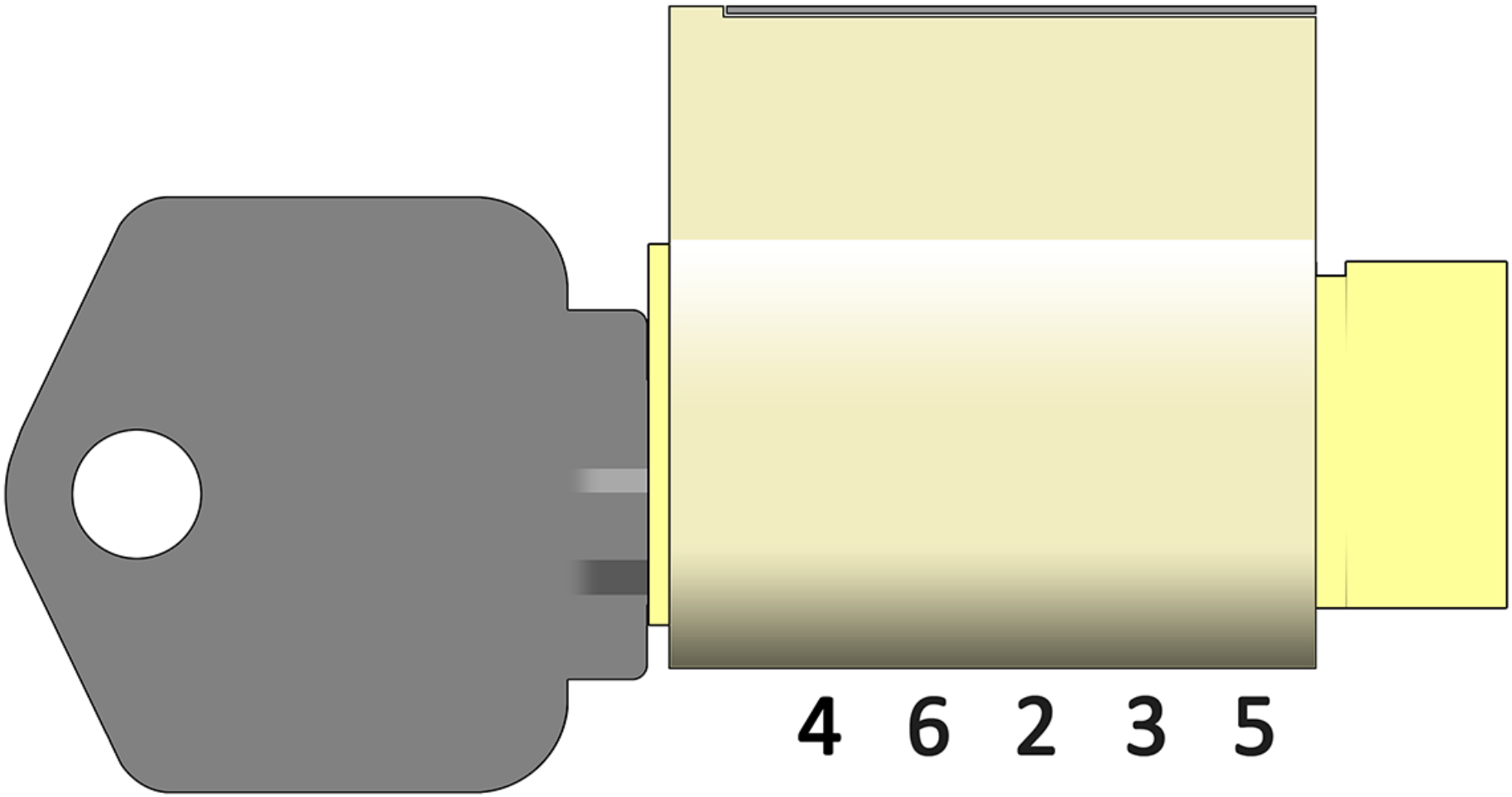
So, There is More Exploring to be



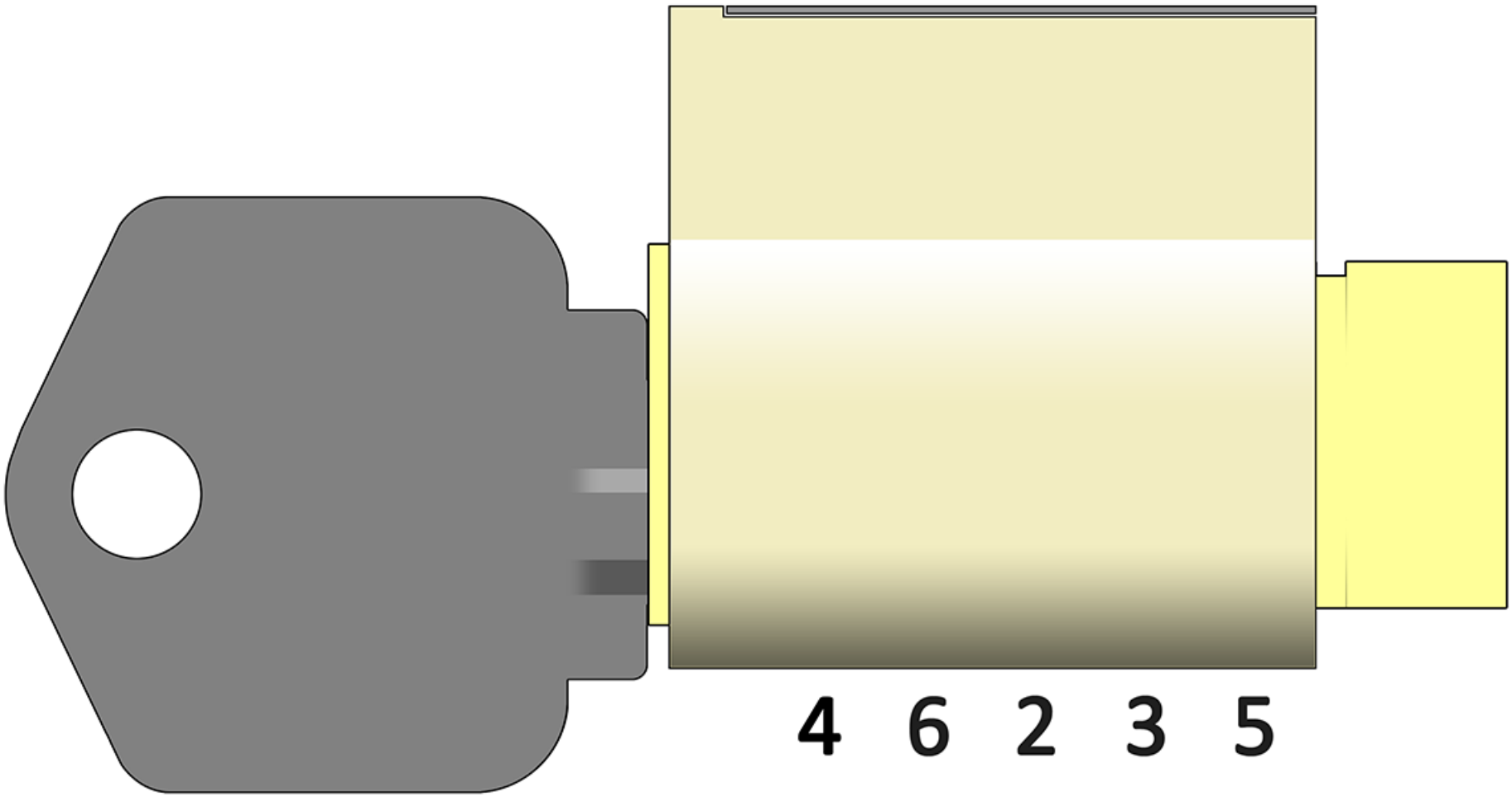
File Position One Down Further



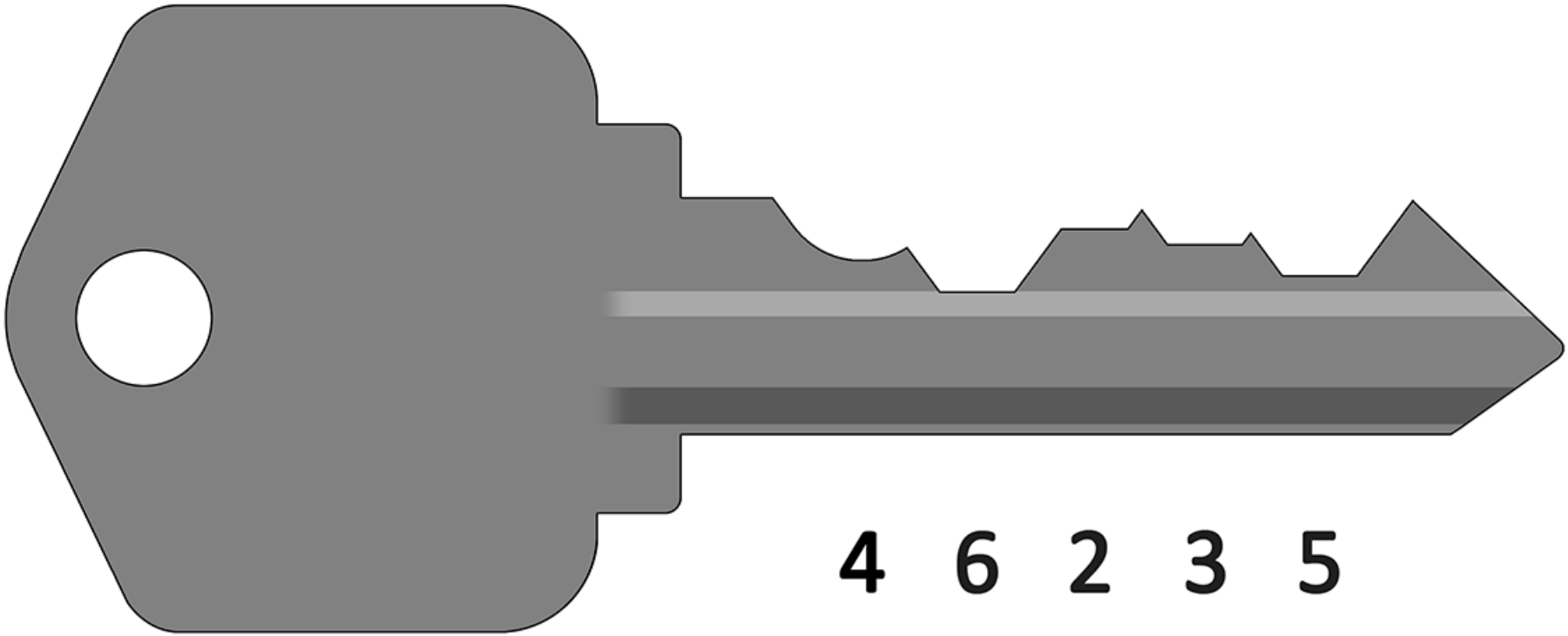
Try They Key…



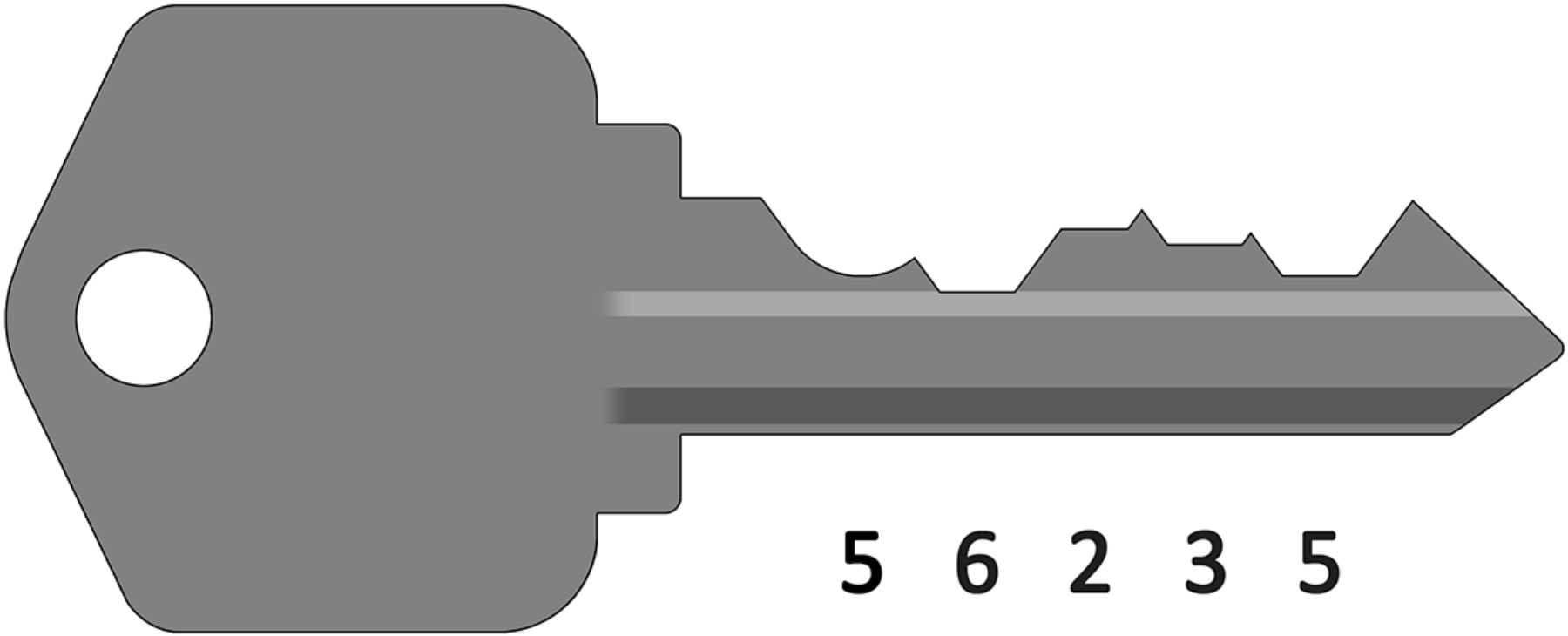
Try They Key… And Find It Does



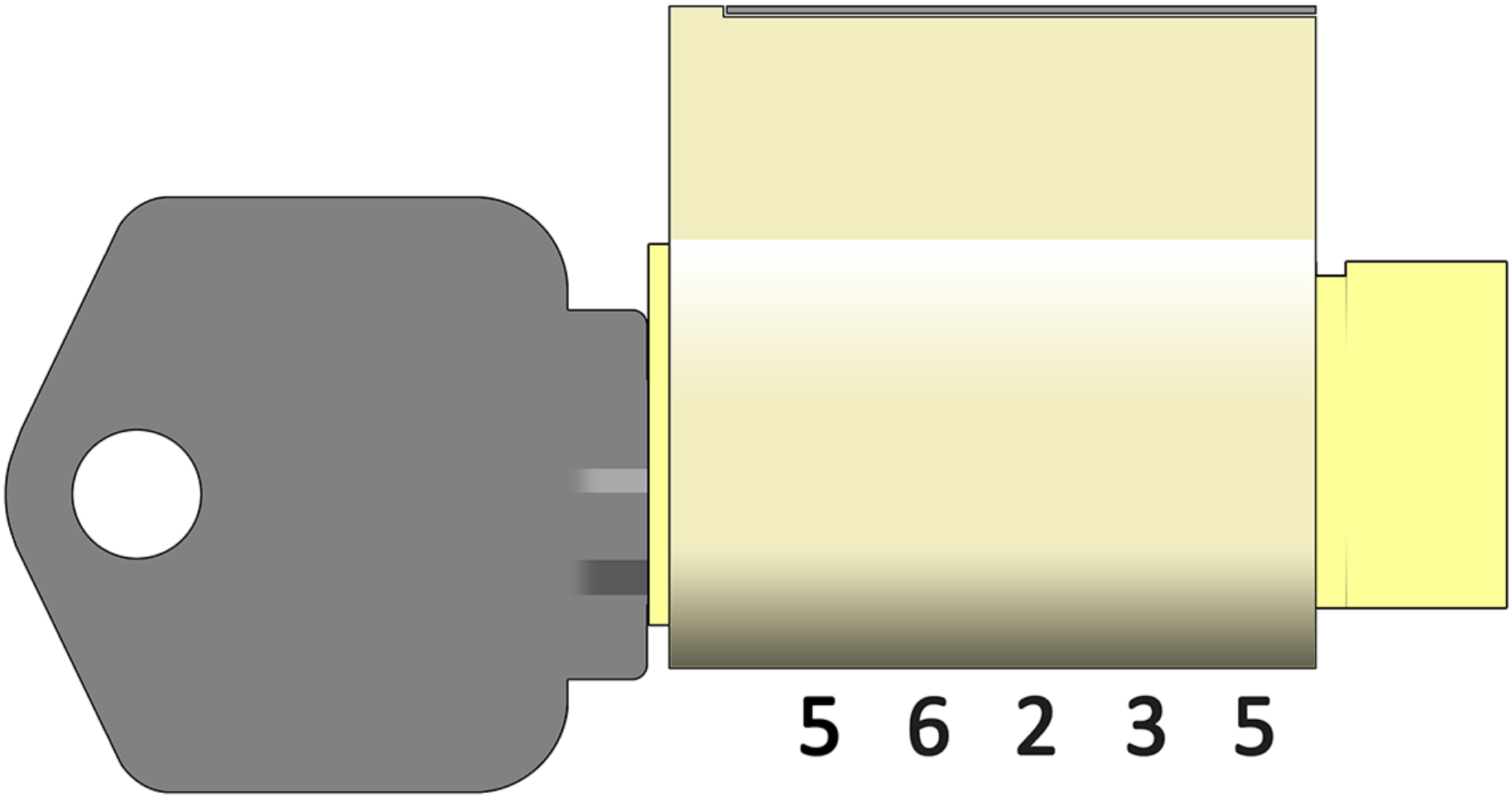
Remove the Key



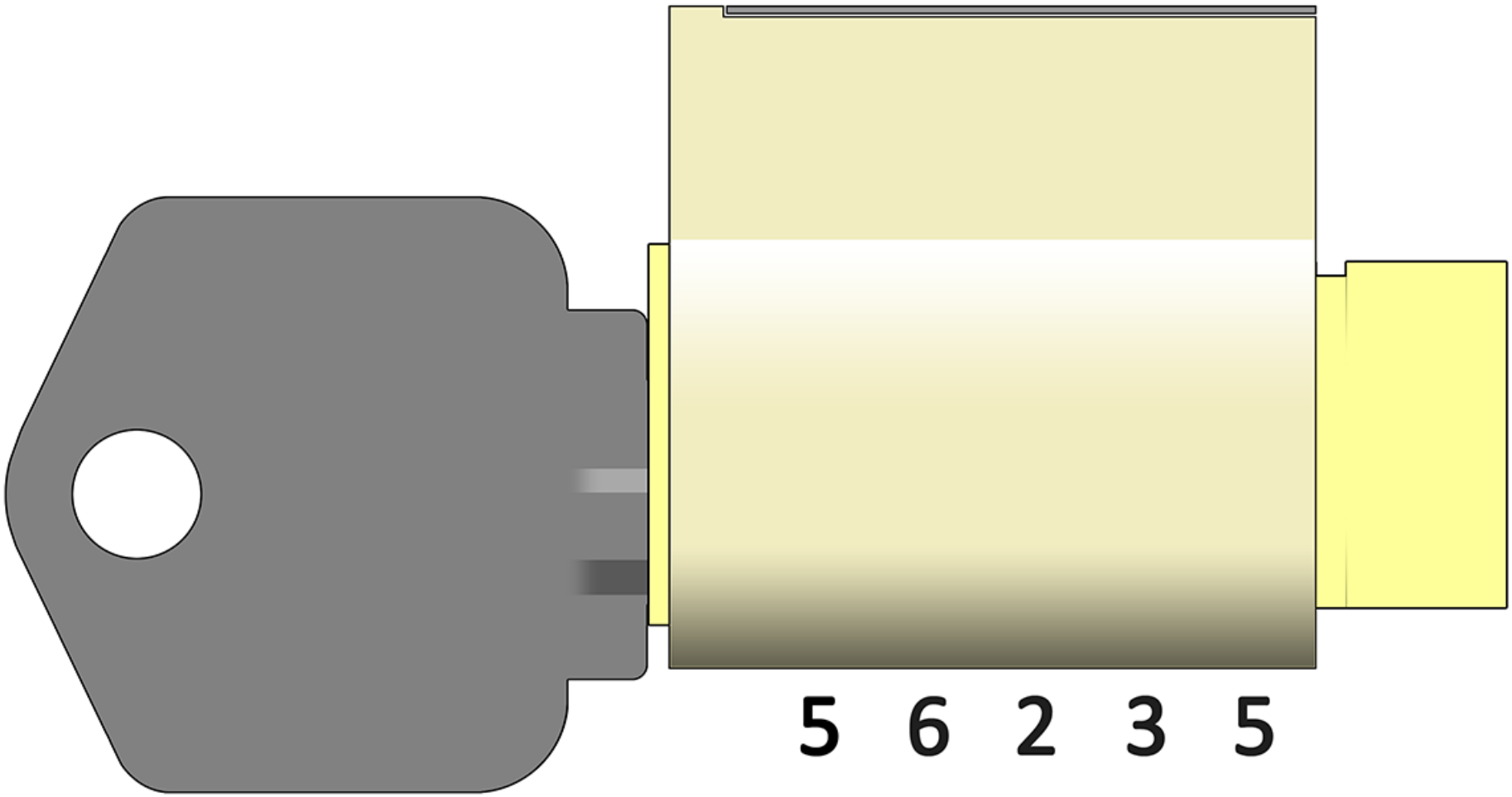
File Down Position One to the



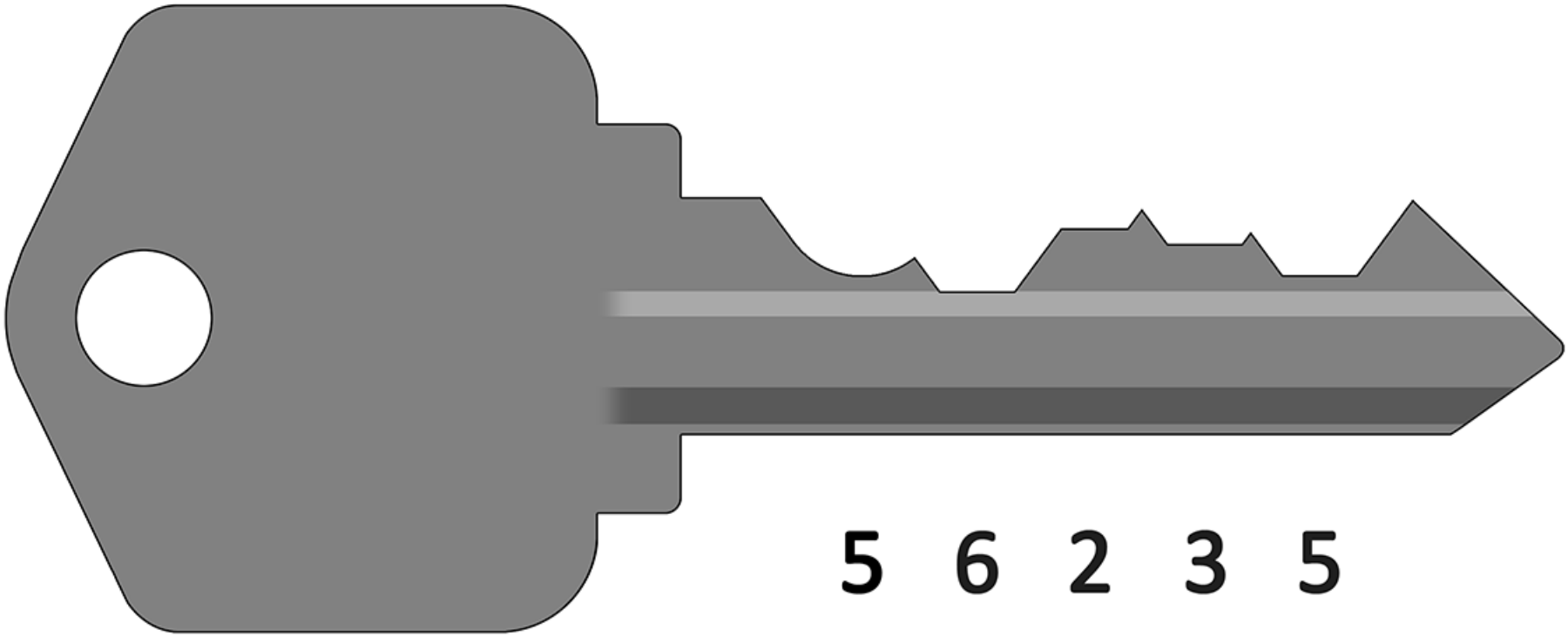
Try the Key…



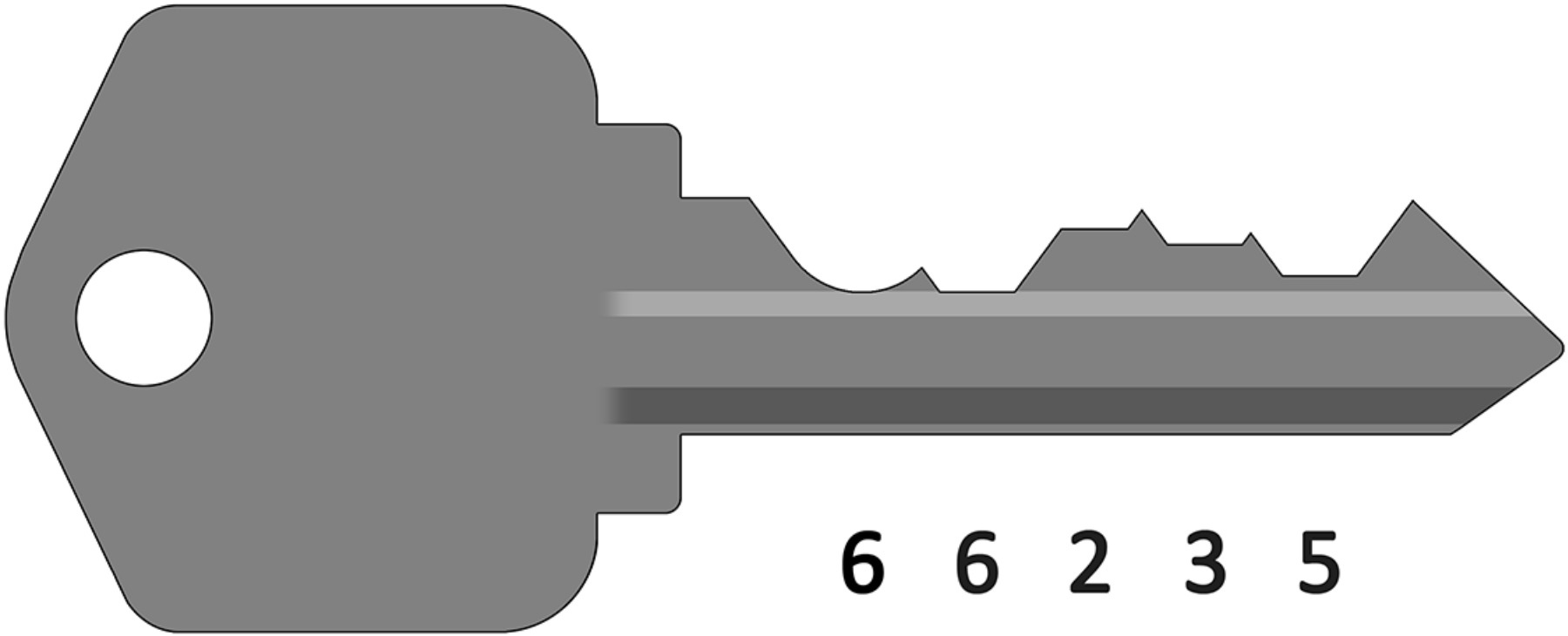
Try the Key… and Find it Does



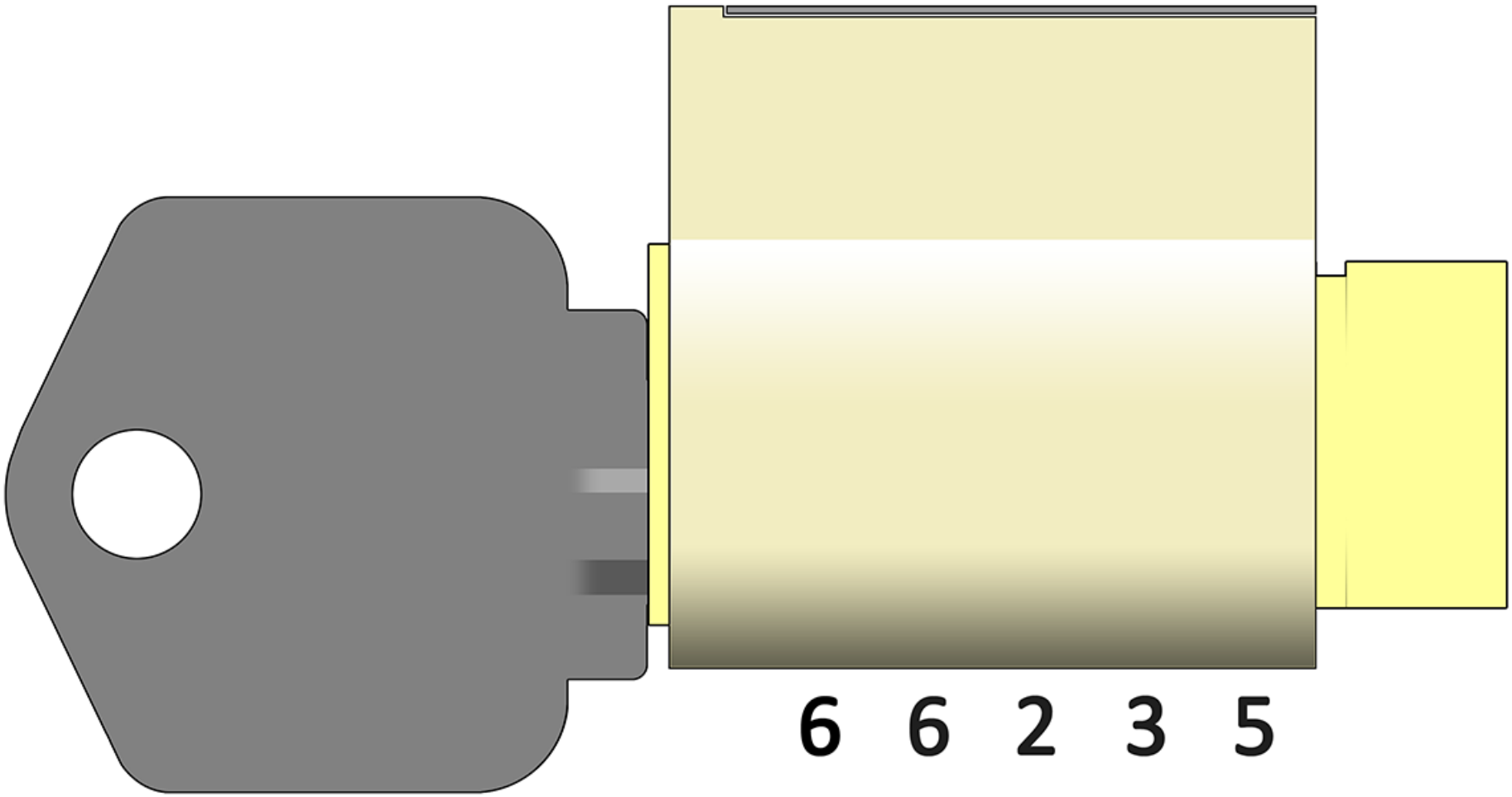
Remove the Key



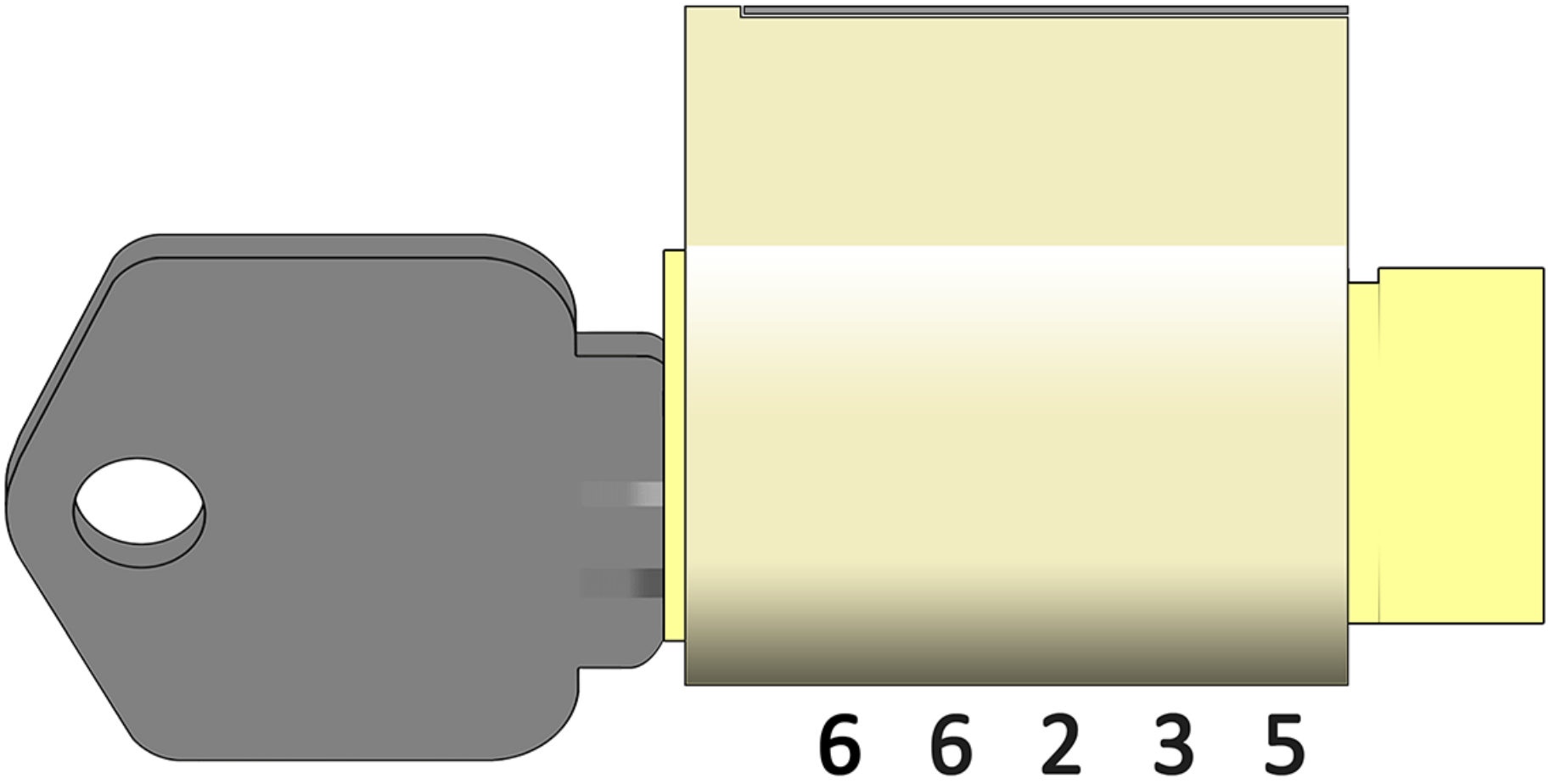
File Position One Down another



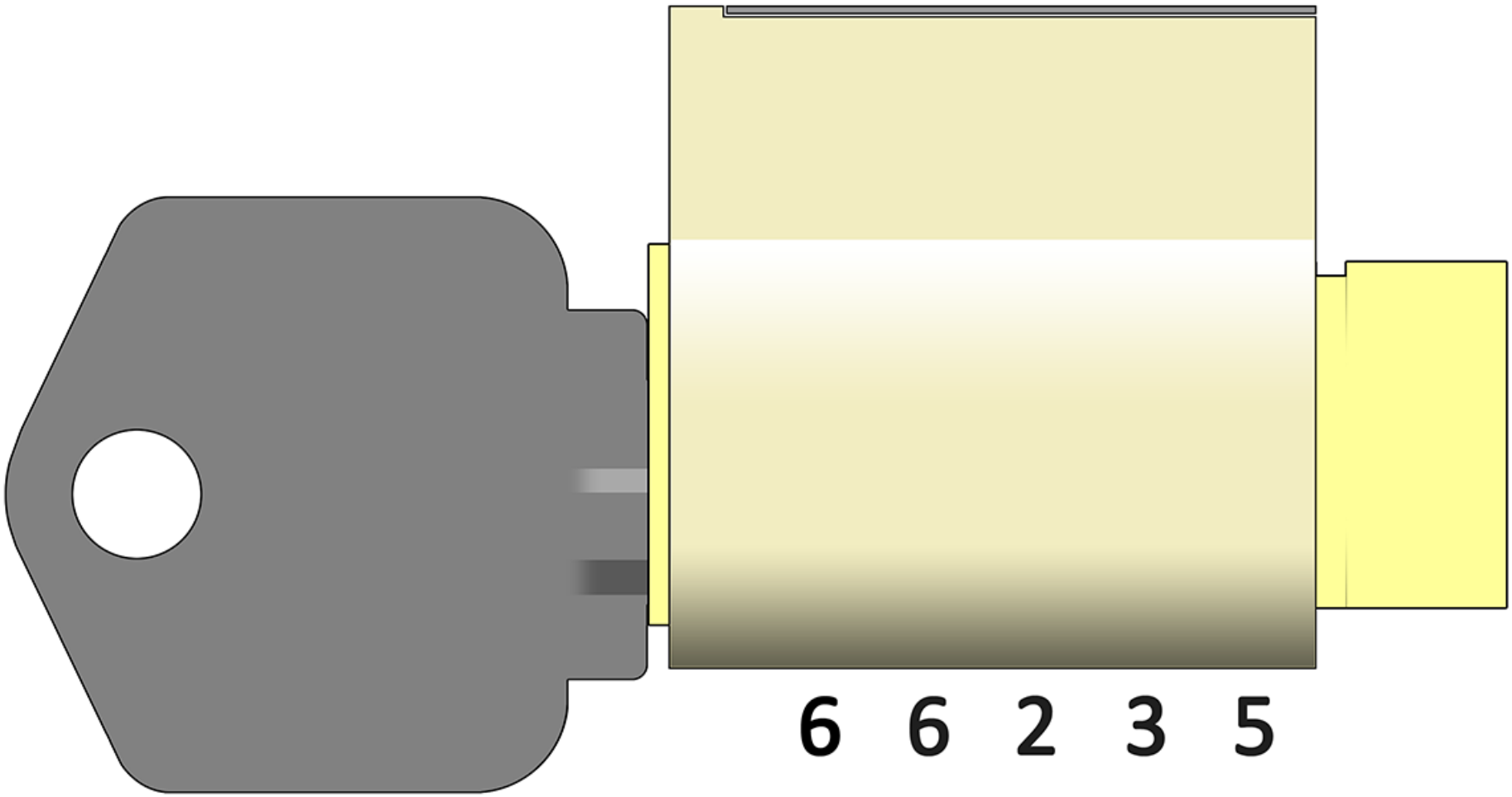
Try the Key in the Lock…



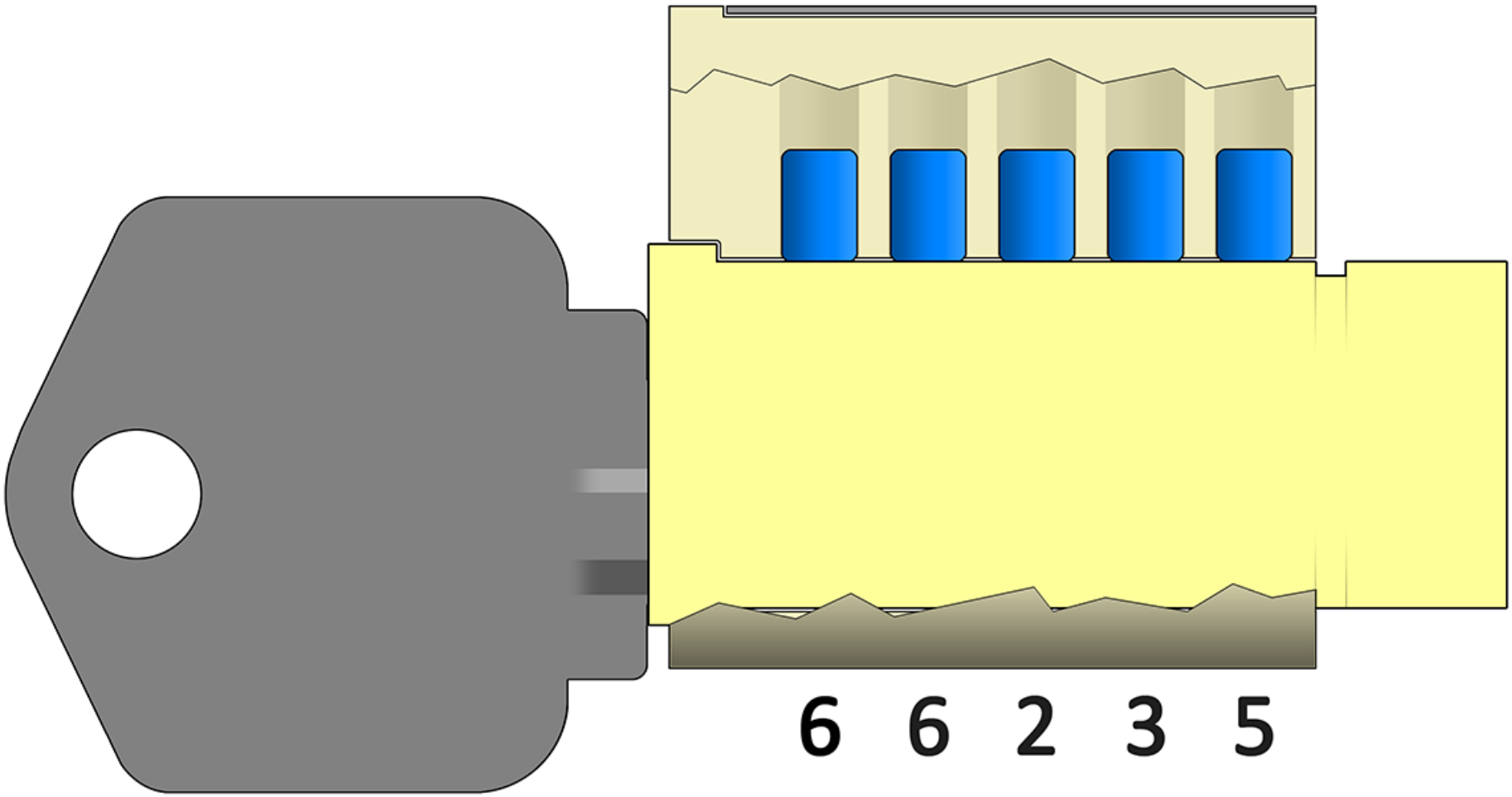
Try the Key in the Lock… 0PEN!



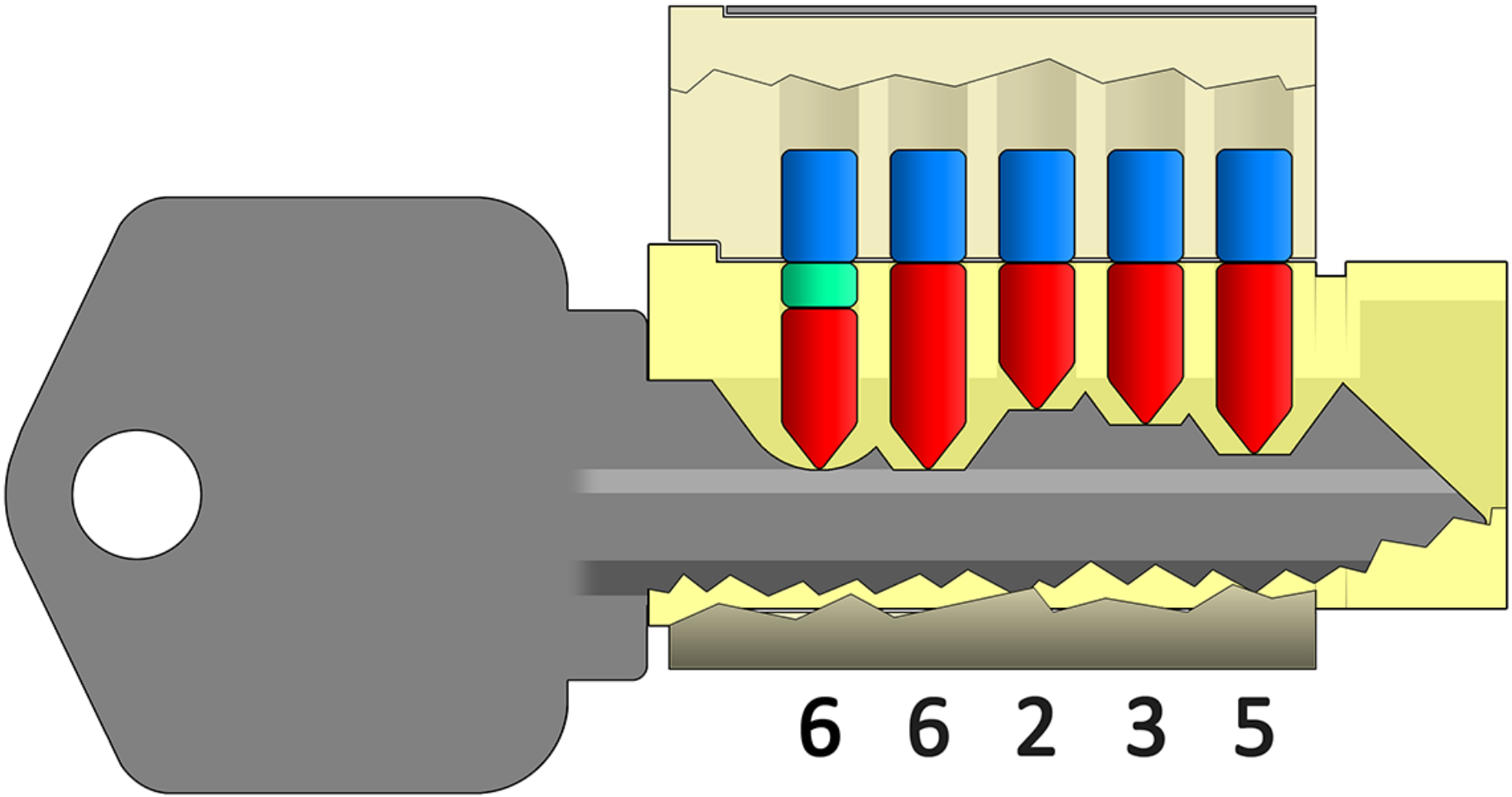
So What Has Been Learned Now?



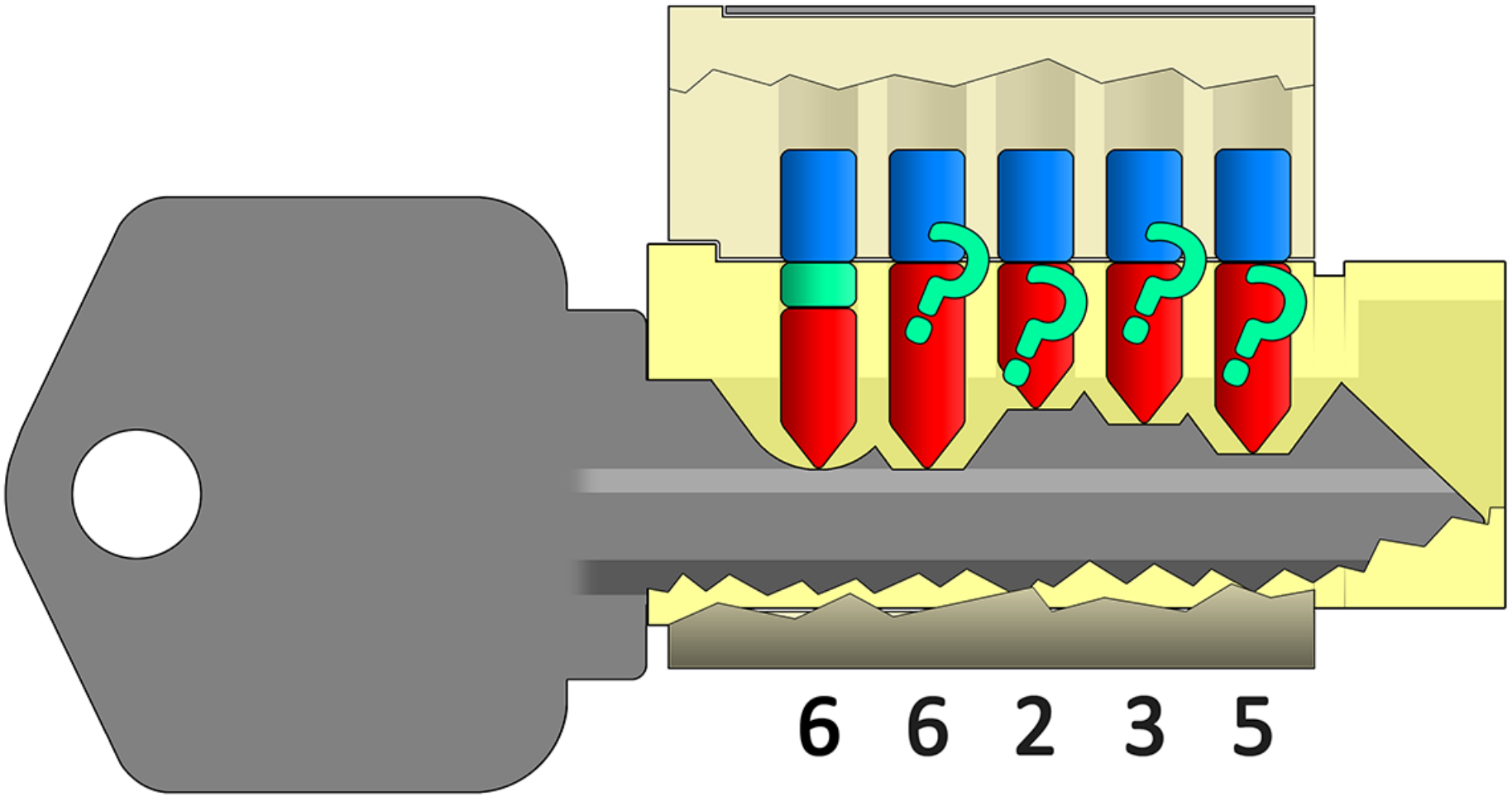
All Drivers Must Be Raised



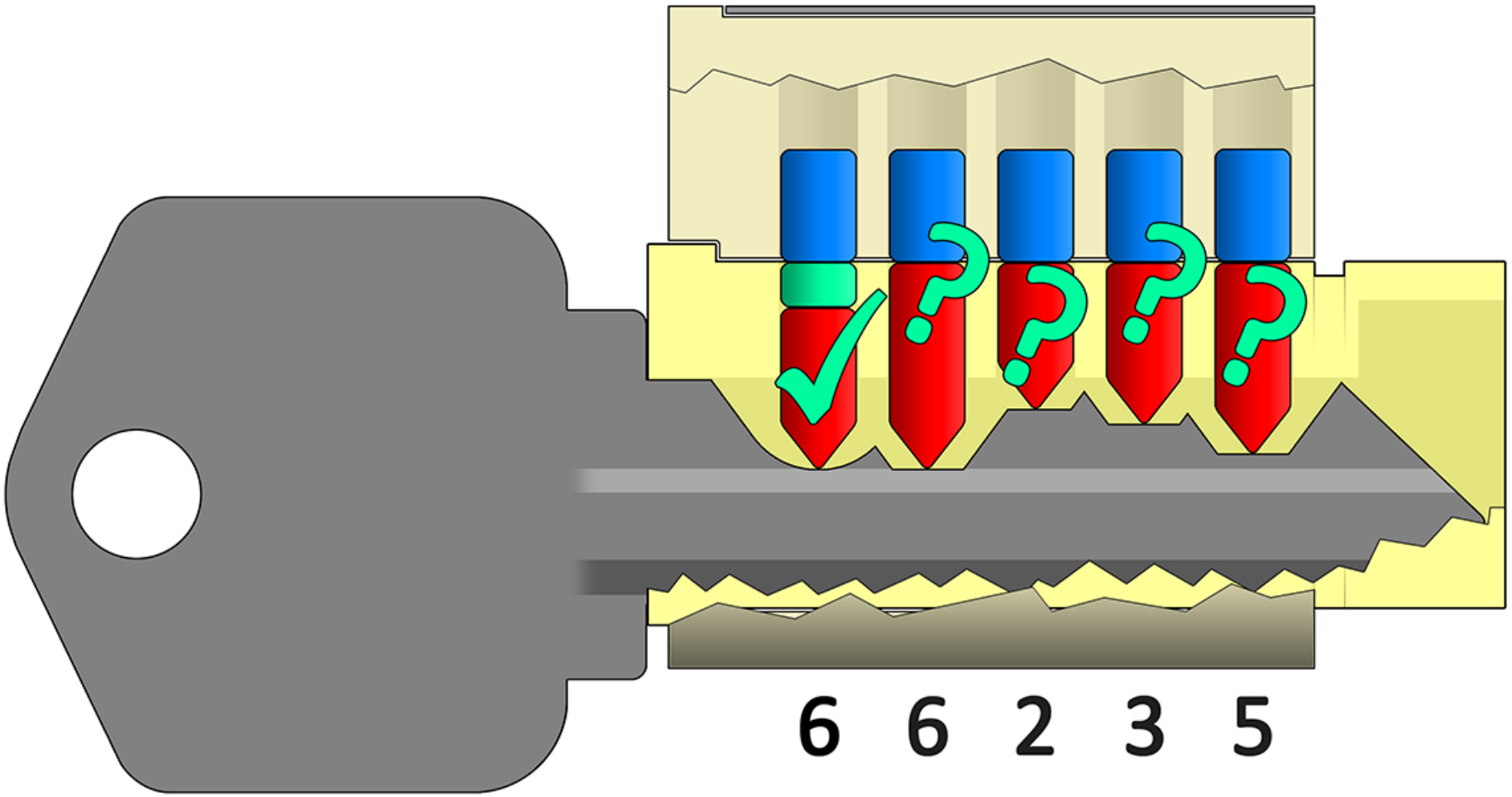
Given What We Know From Before,



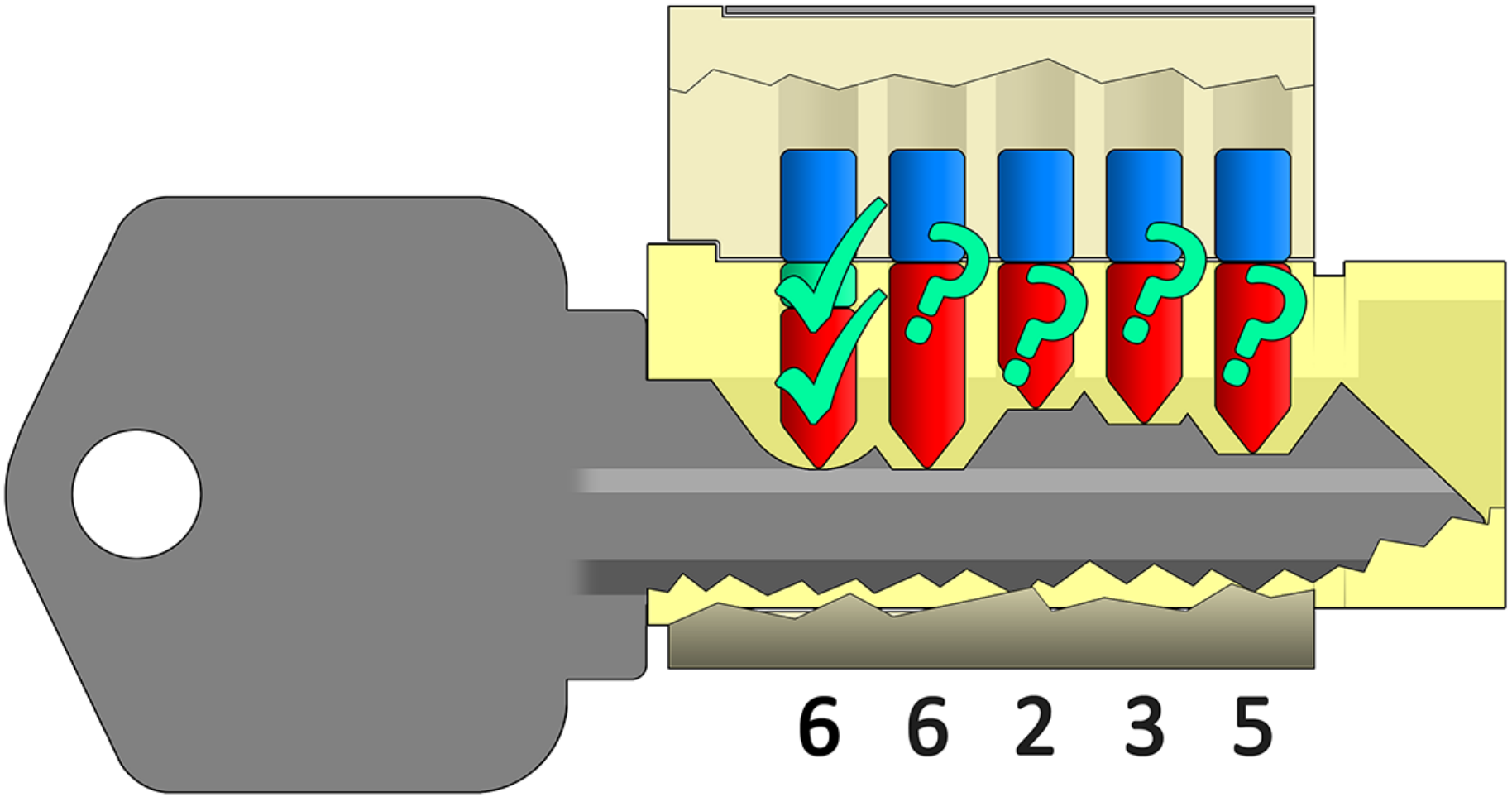
We Still Haven't Explored These



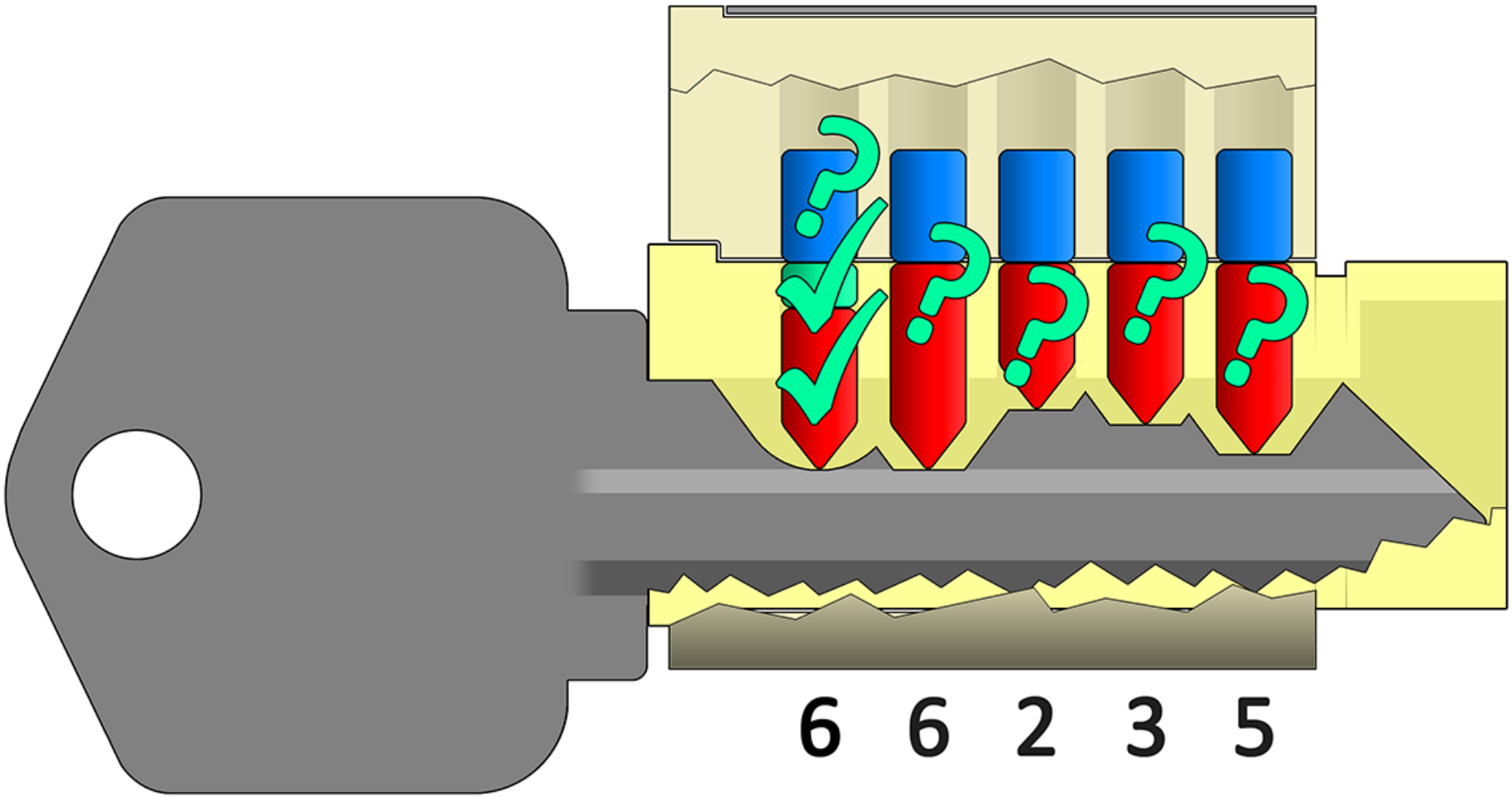
We Know This Key Pin



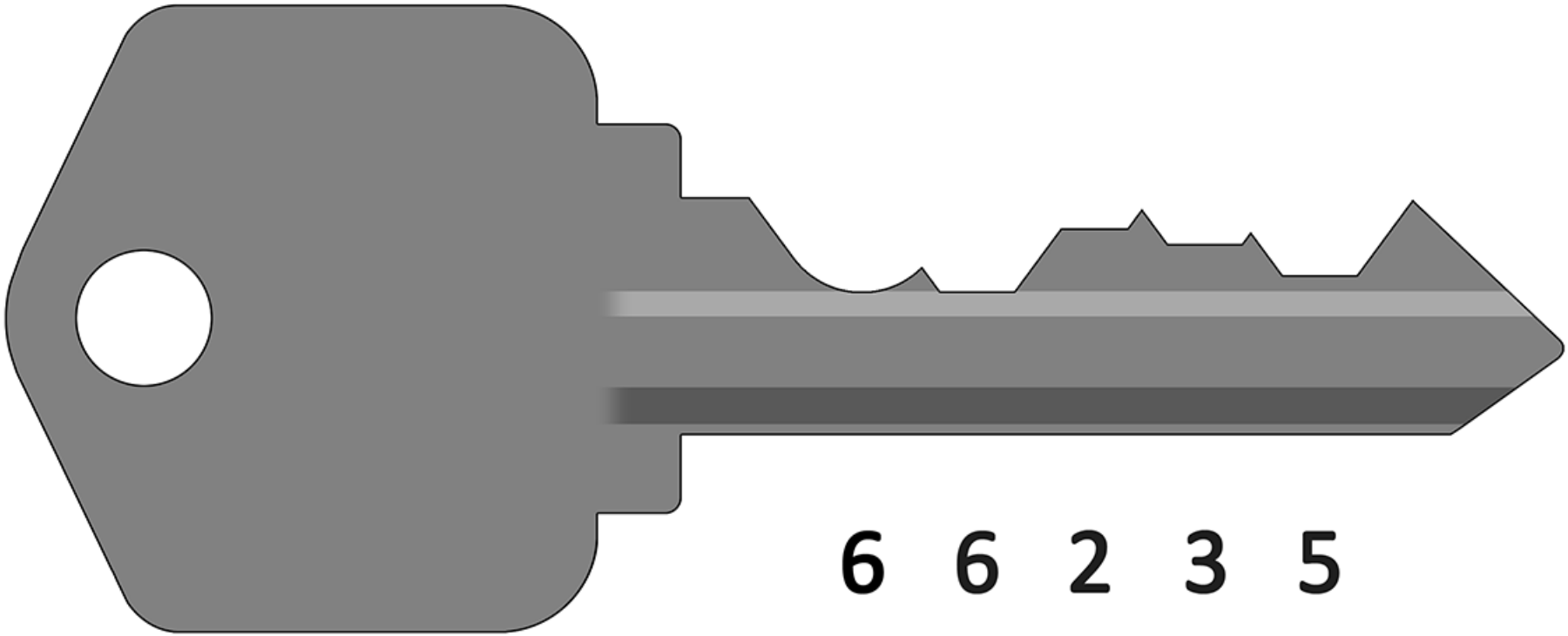
We Know This Mastering Pin



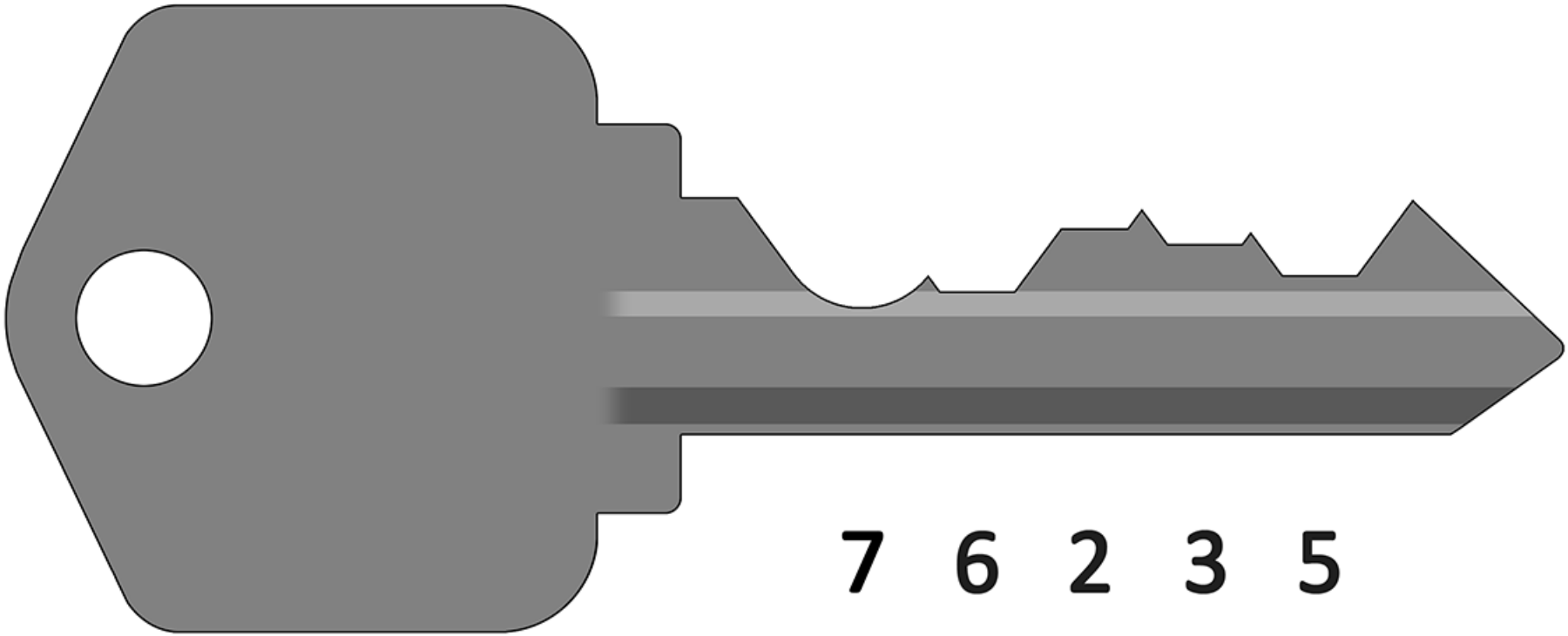
There's a Chance of More Shear



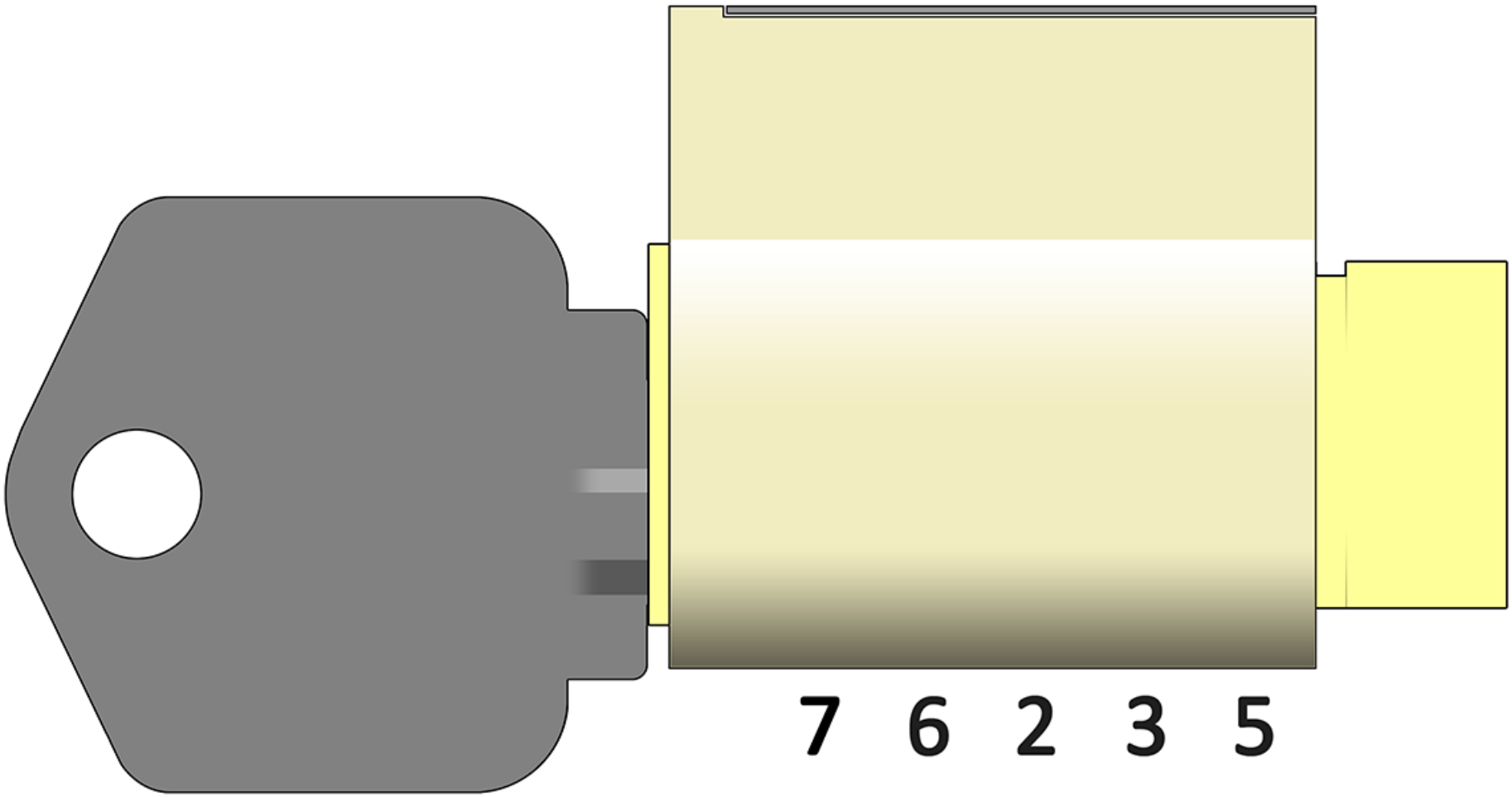
Remove the Key



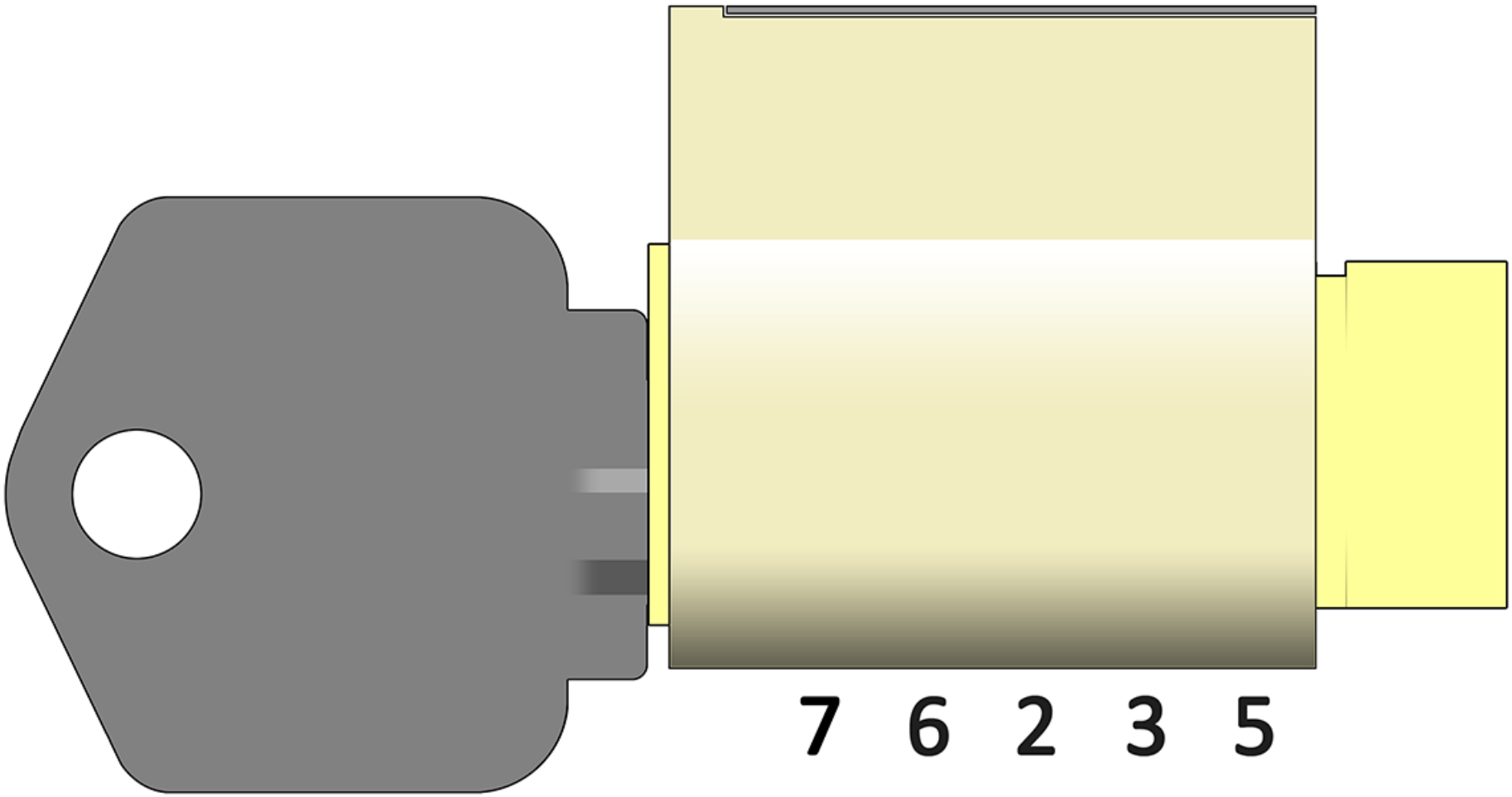
File Position One Down a bit



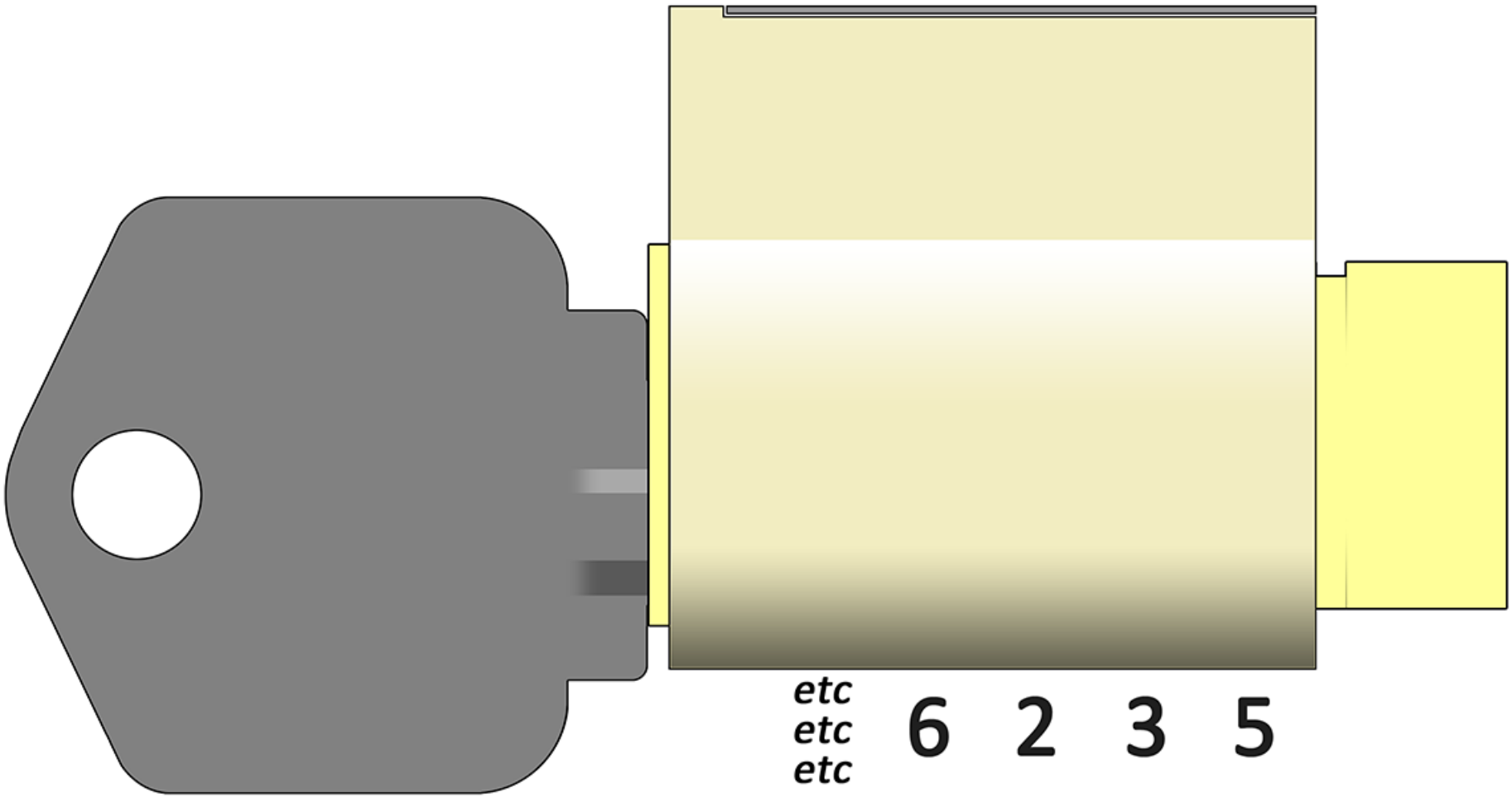
Try the Key…



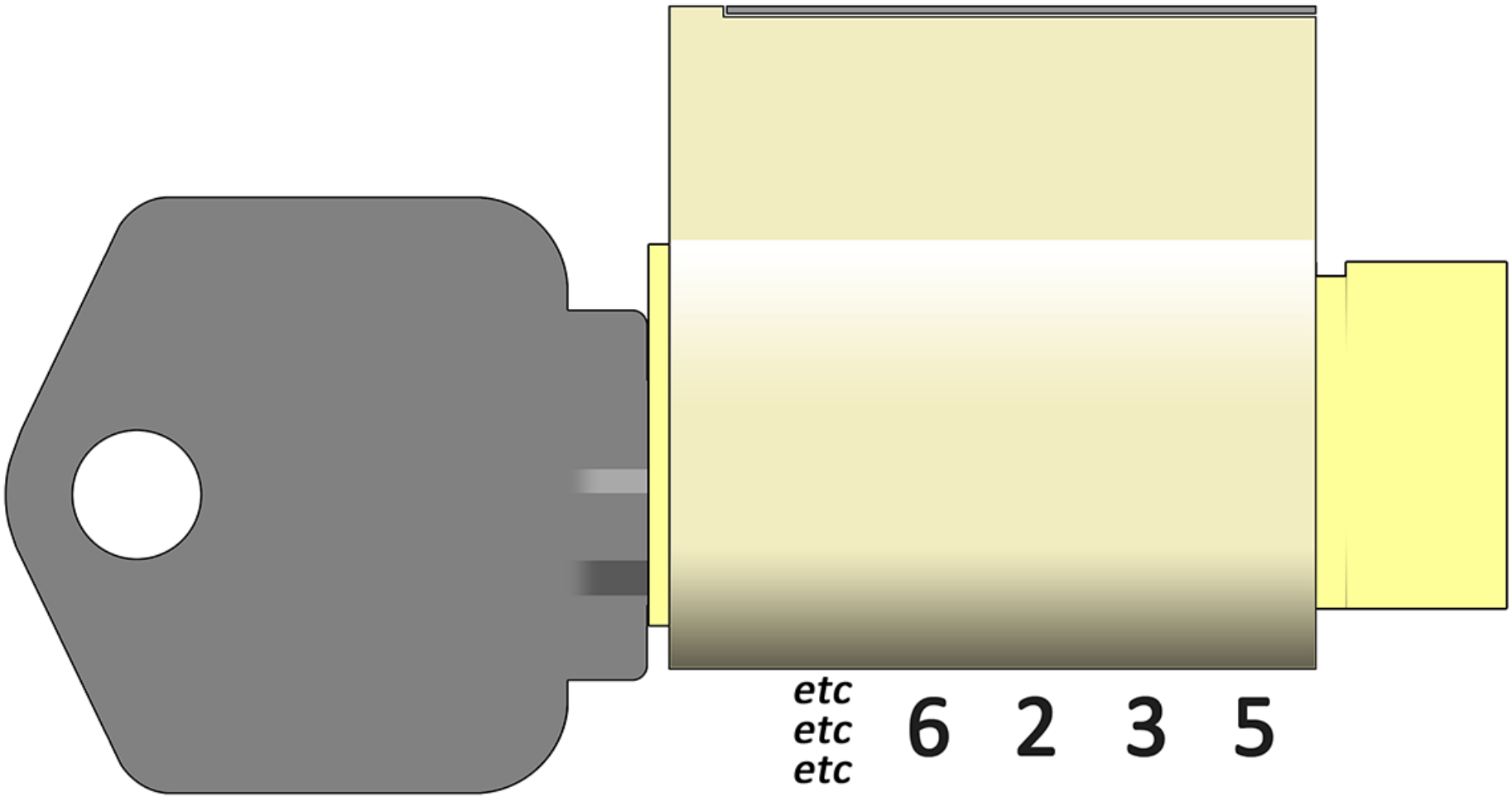
Try the Key… and Find it Does



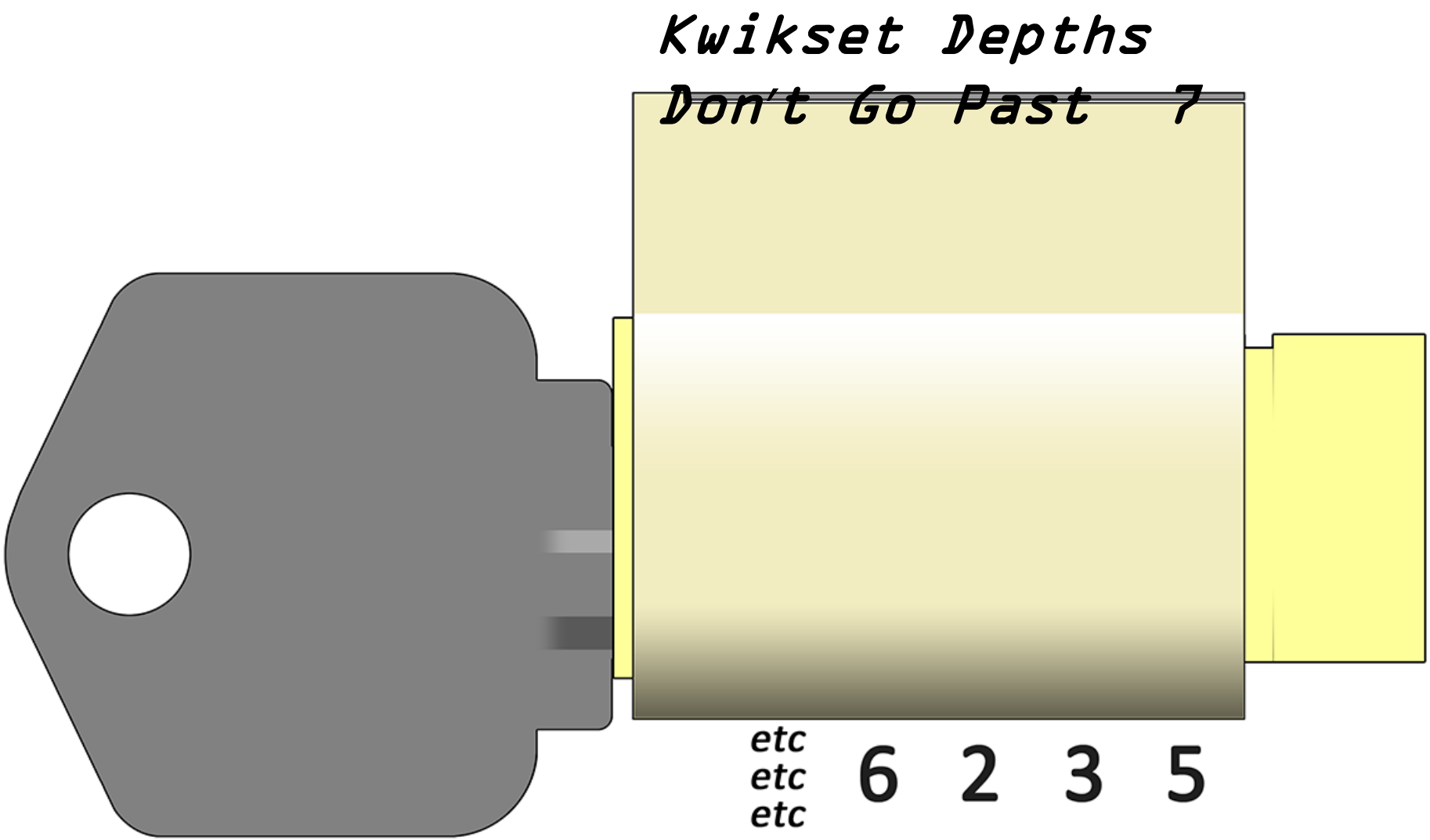
You Can Continue For The Rest of



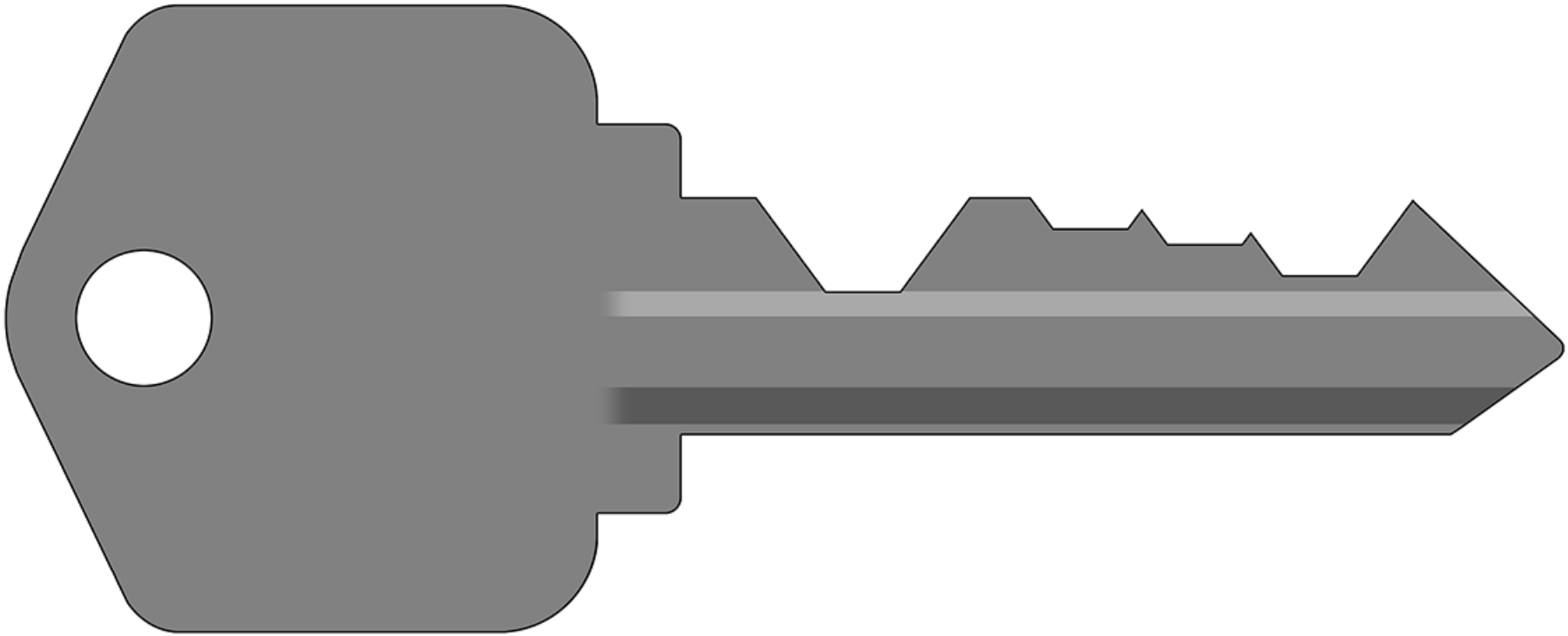
(If There is More to the Bitting



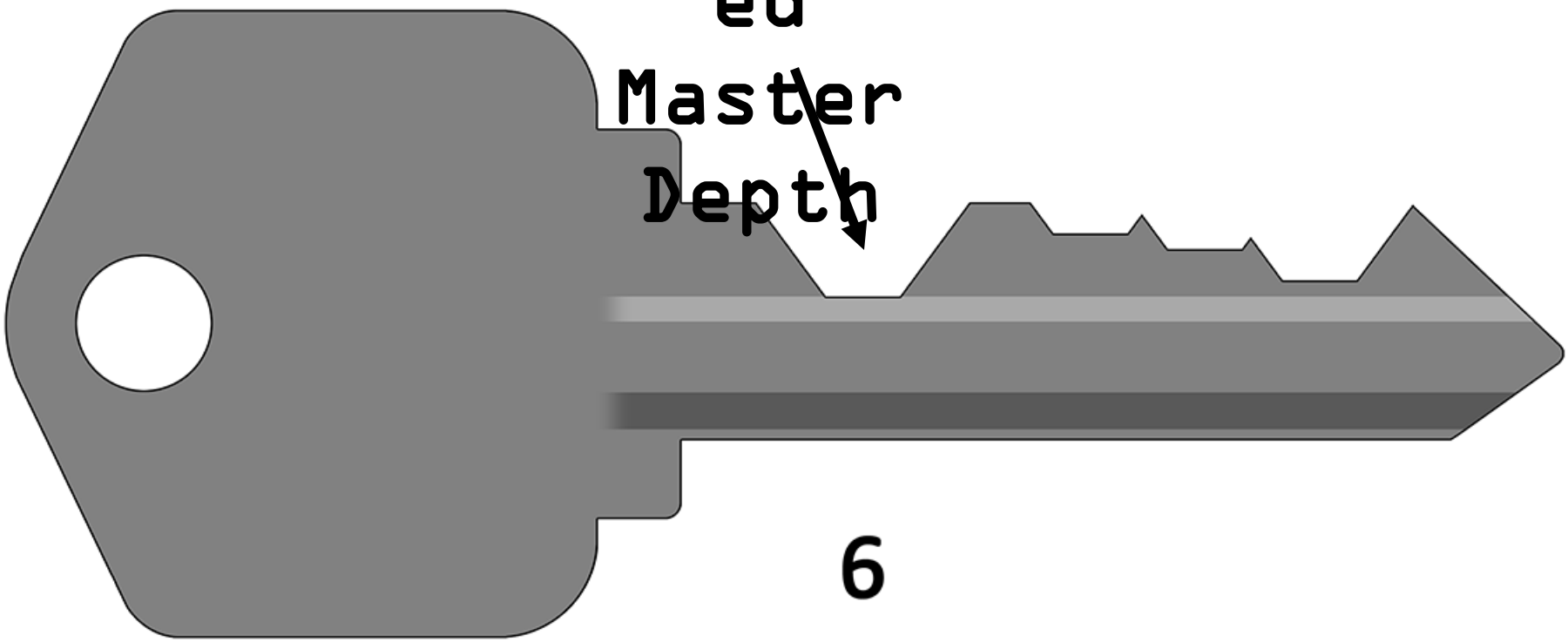
(If There is More to the Bitting



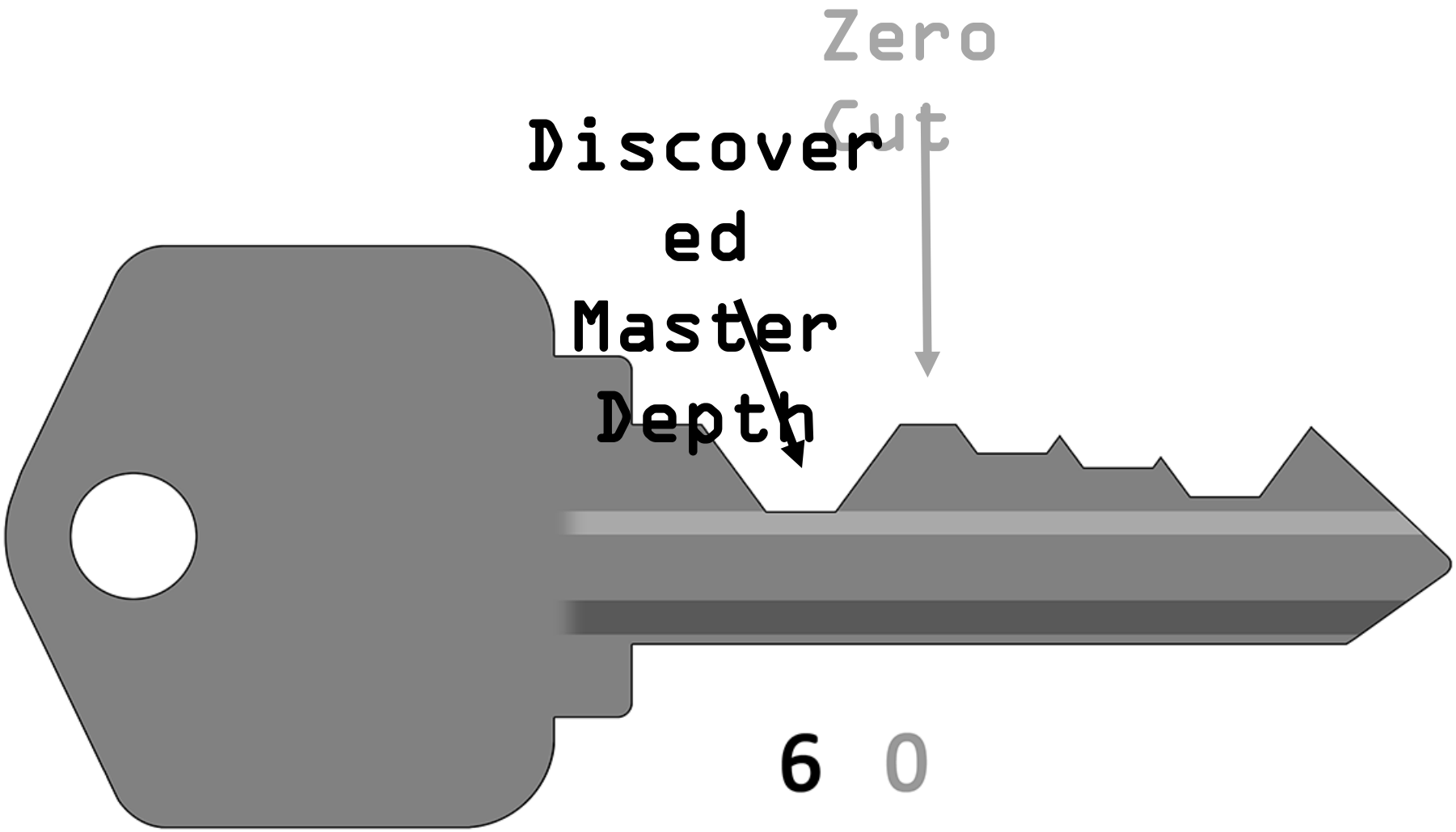
Prepare Another Key, for



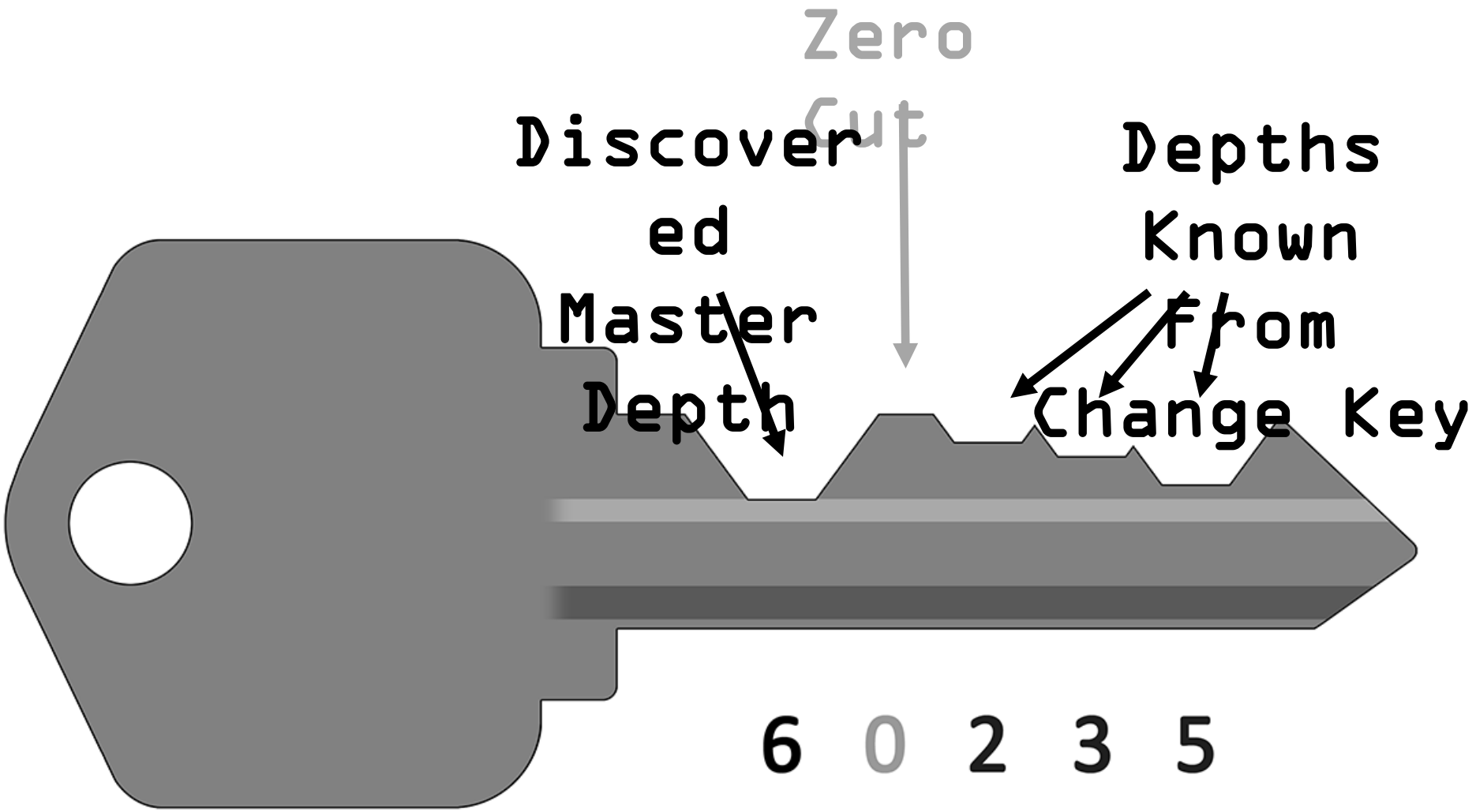
Prepare Another Key, for



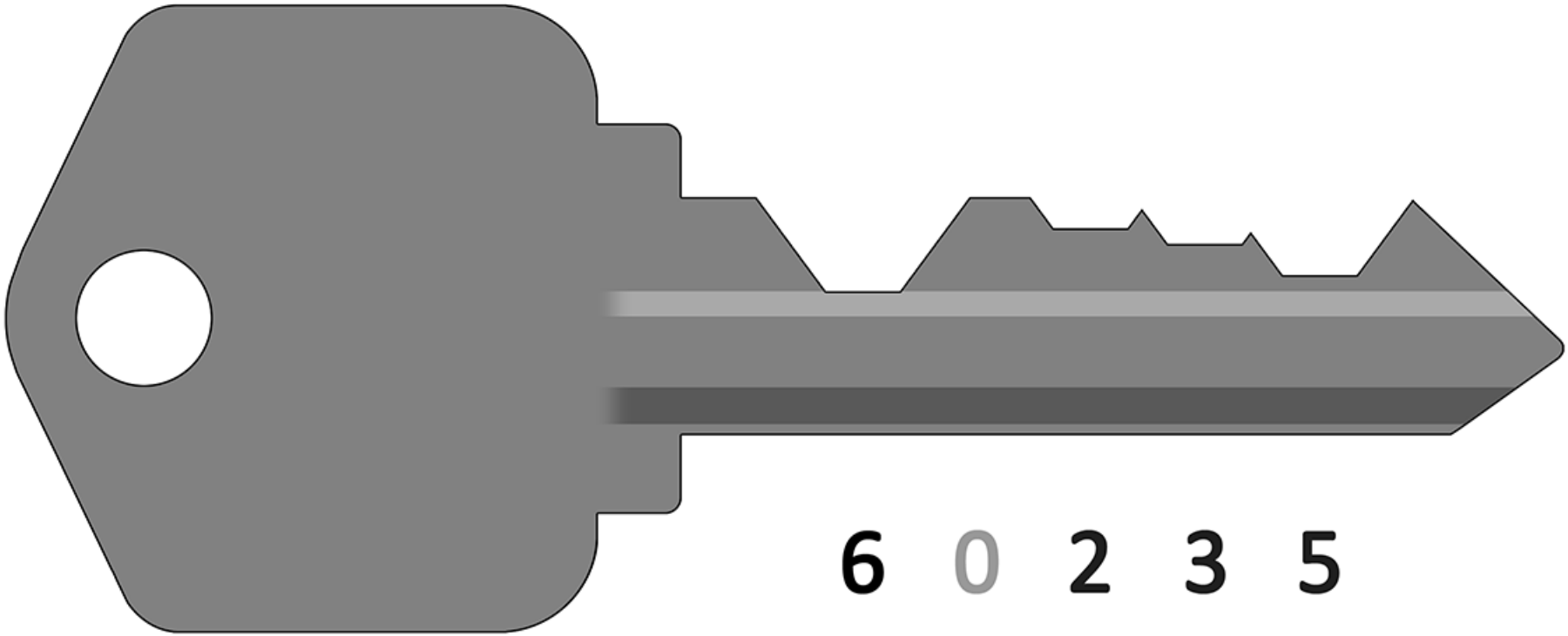
Prepare Another Key, for



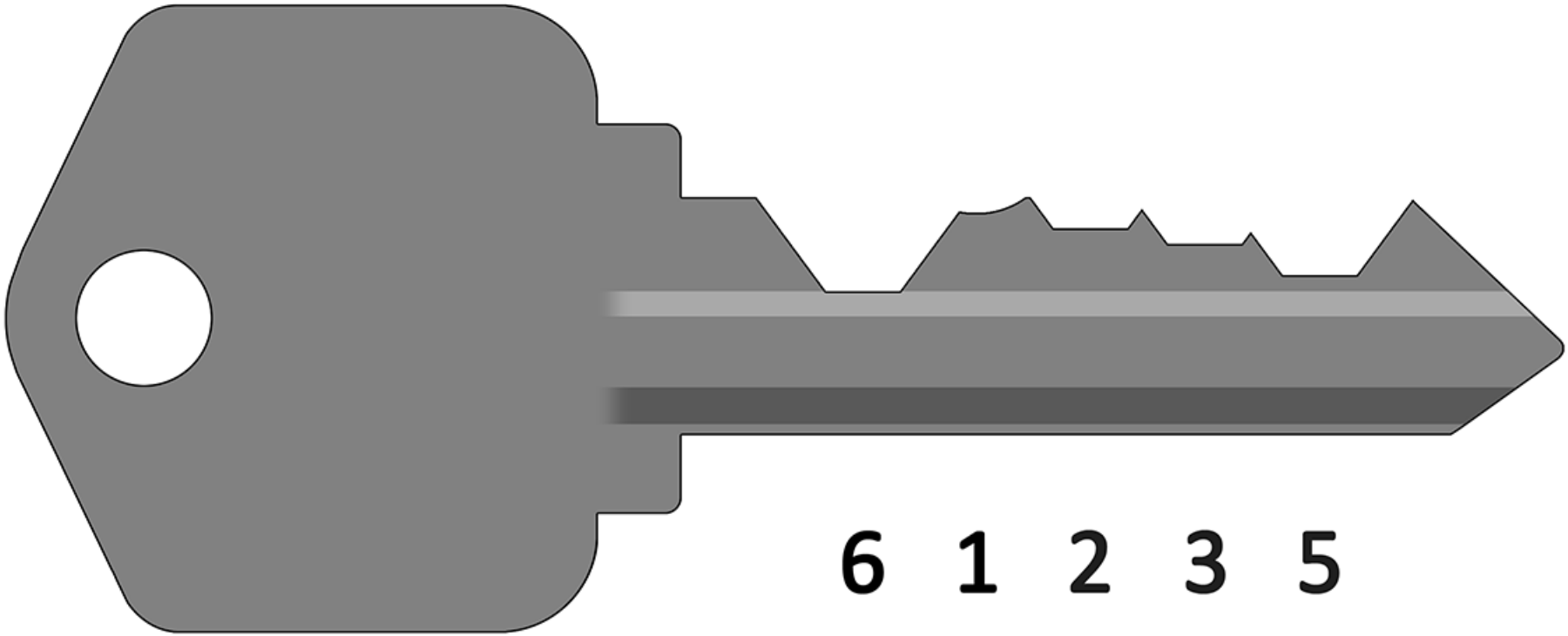
Prepare Another Key, for



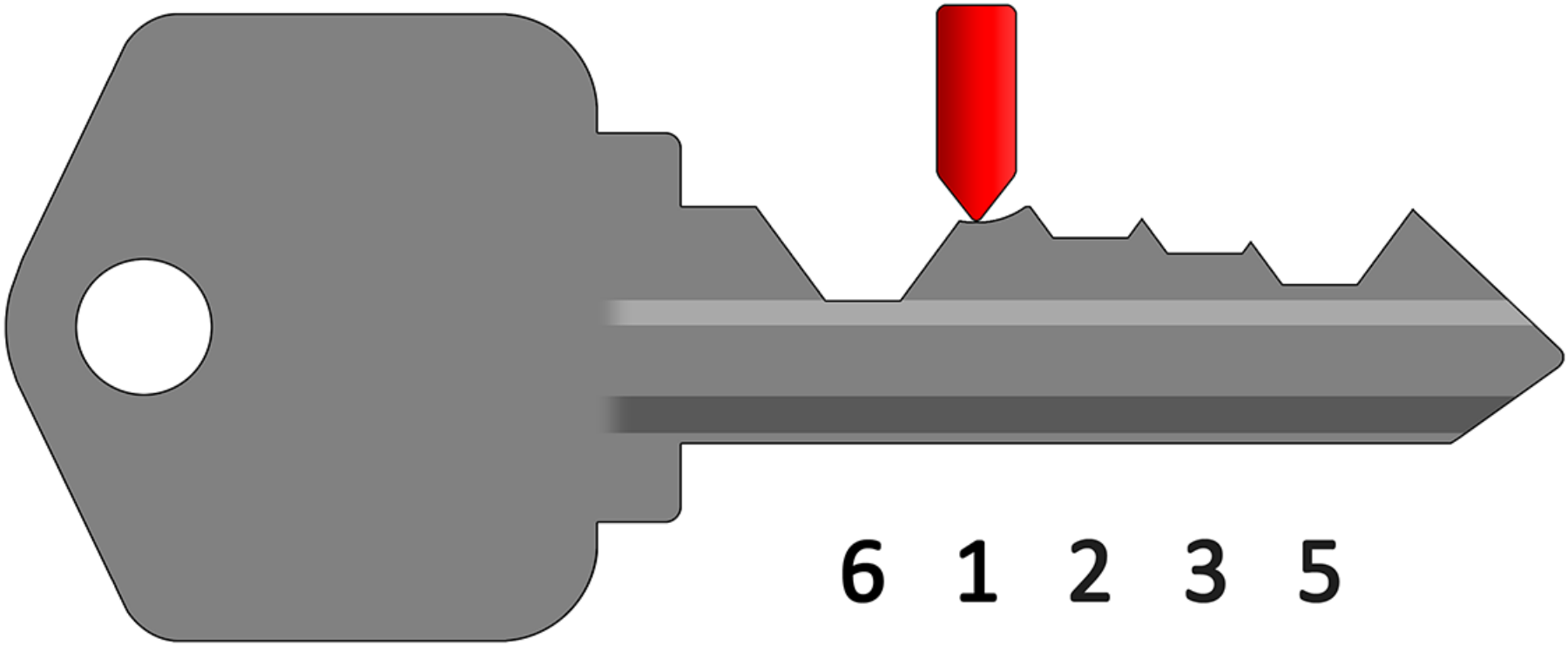
NOTE - The Zero Depth is Almost



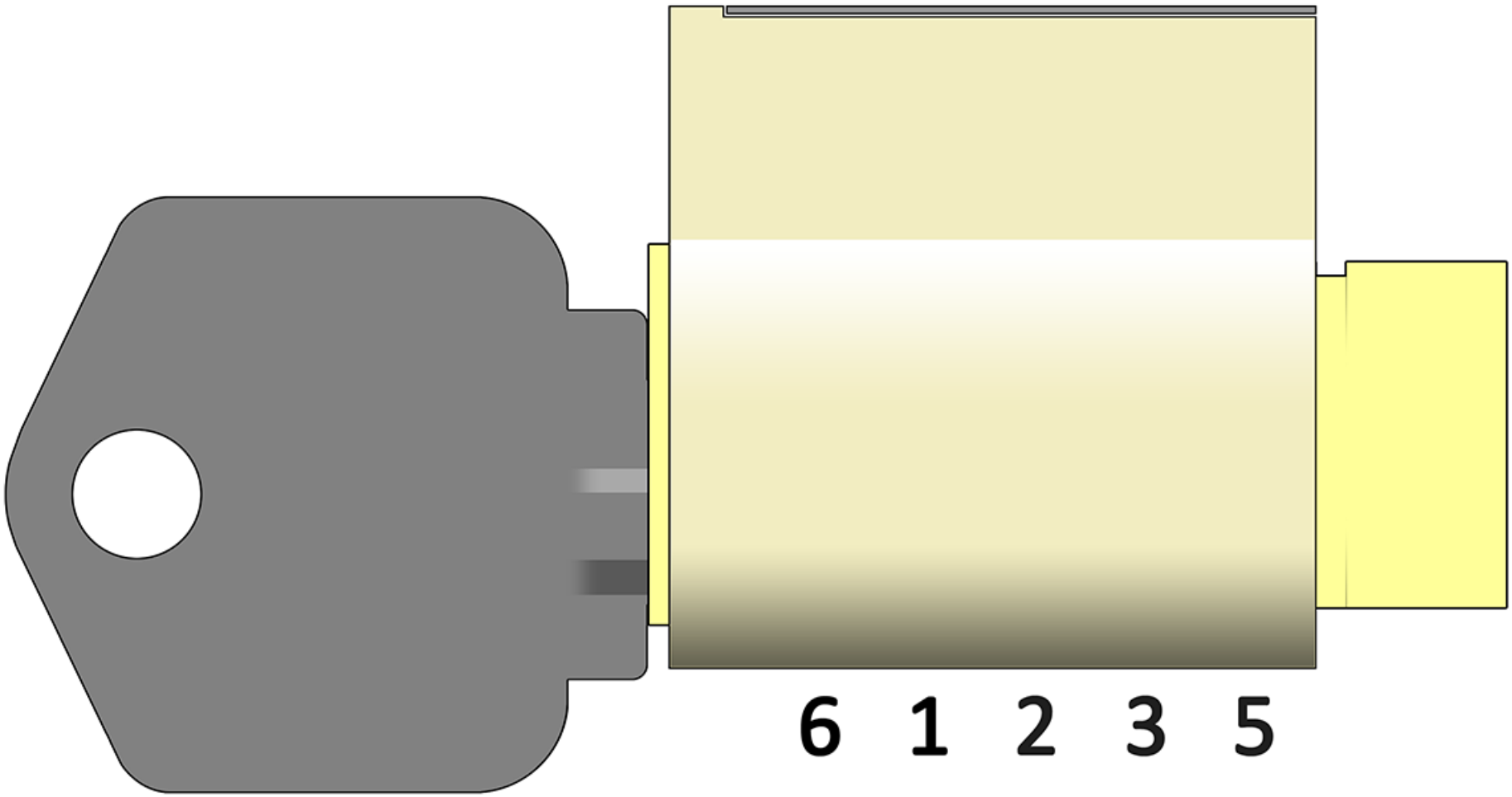
So, Save Time by Starting



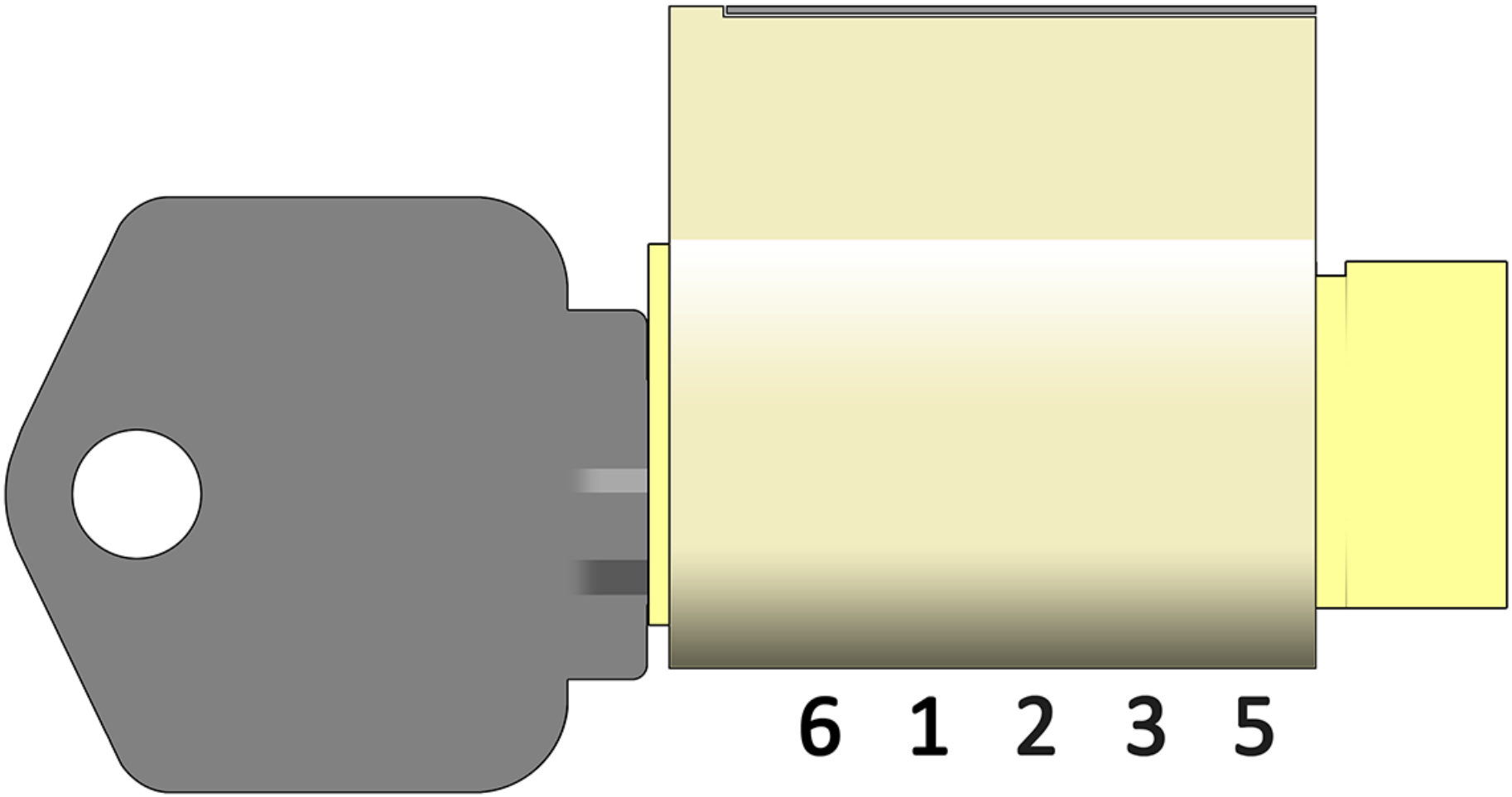
MACS is Being Violated Here



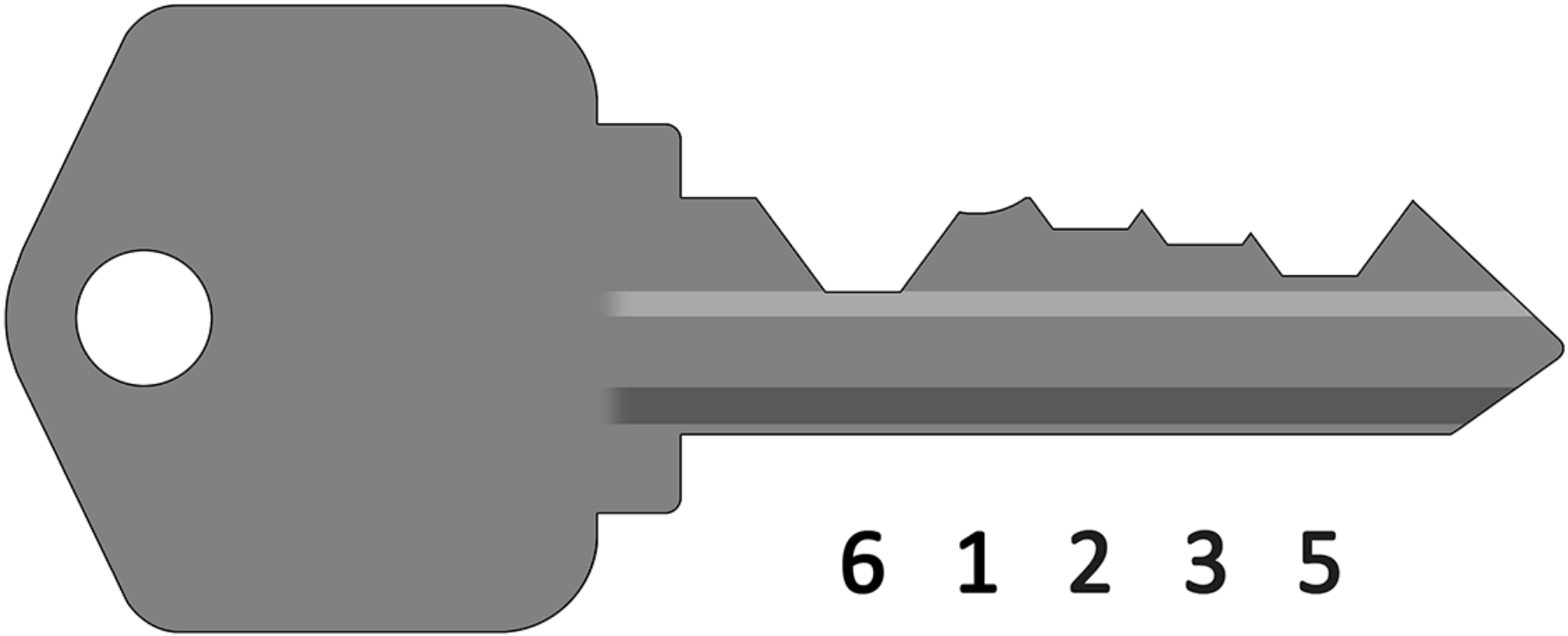
But Let's Try the Key Anyway…



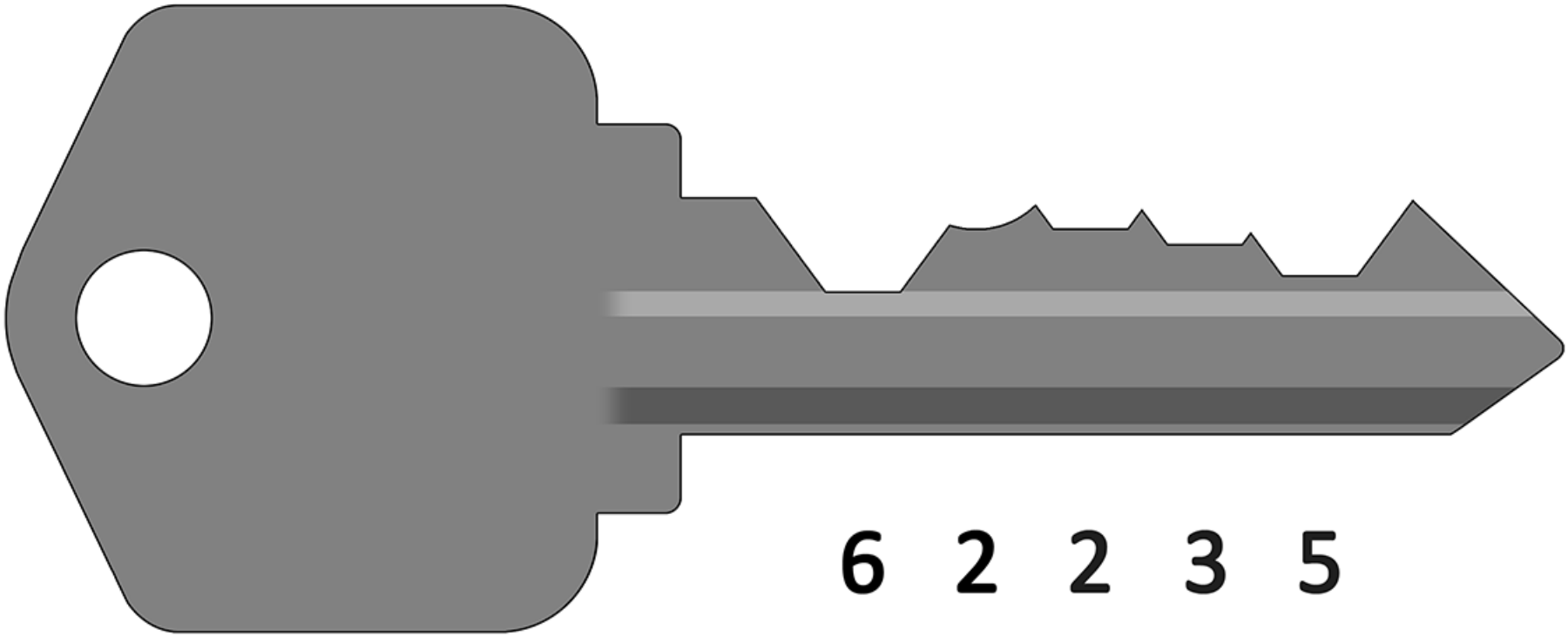
But Let's Try the Key Anyway… The



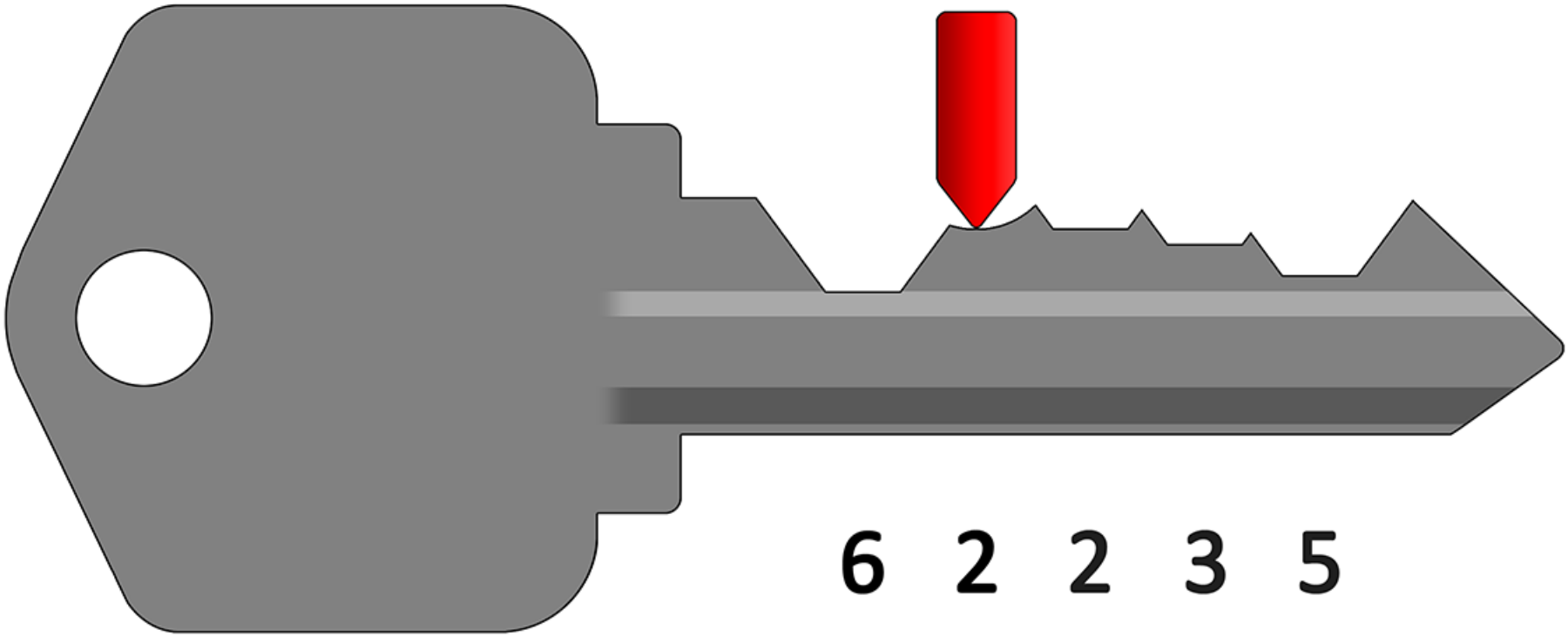
Remove the Key



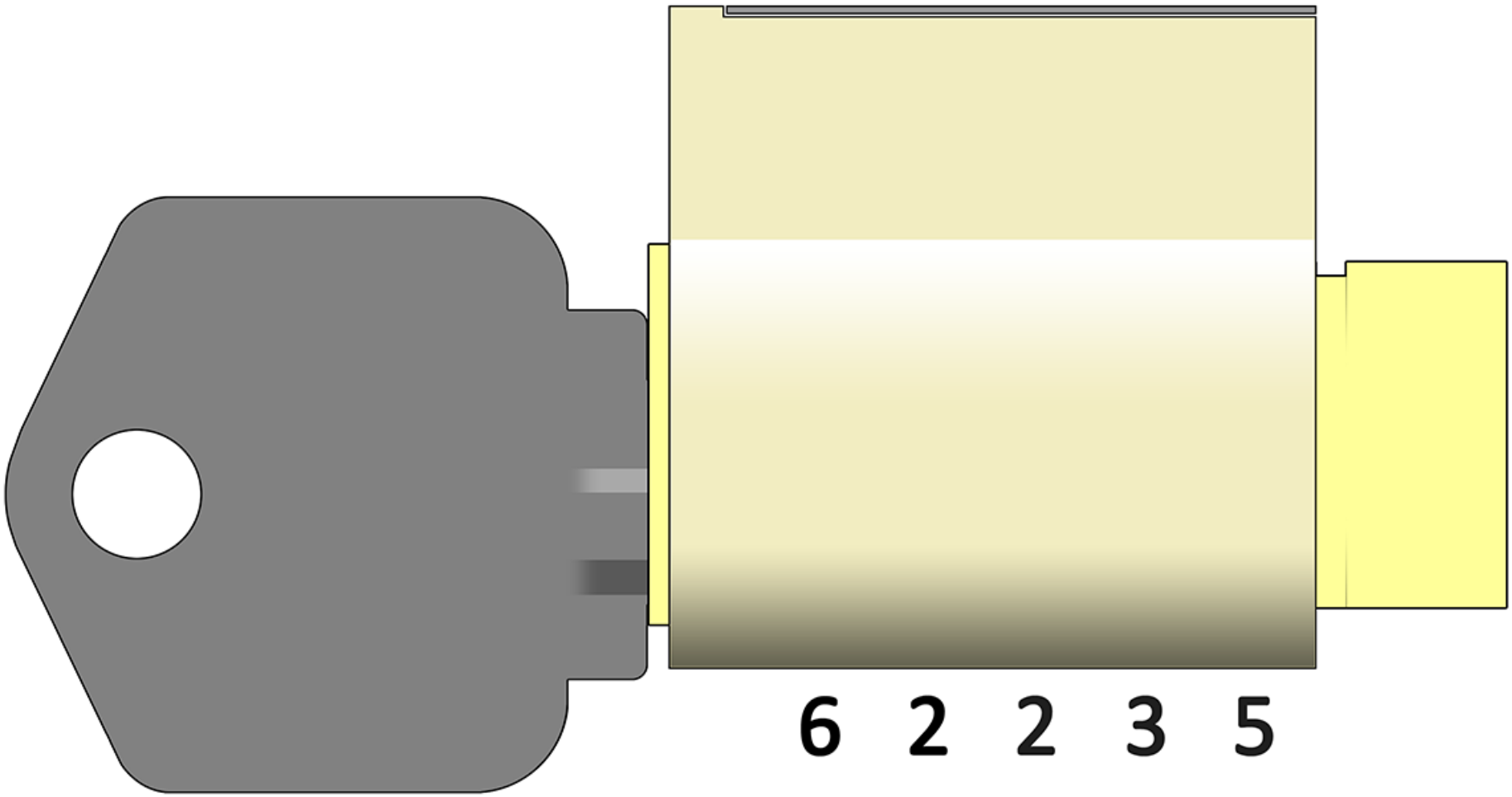
File Down Position Two by a



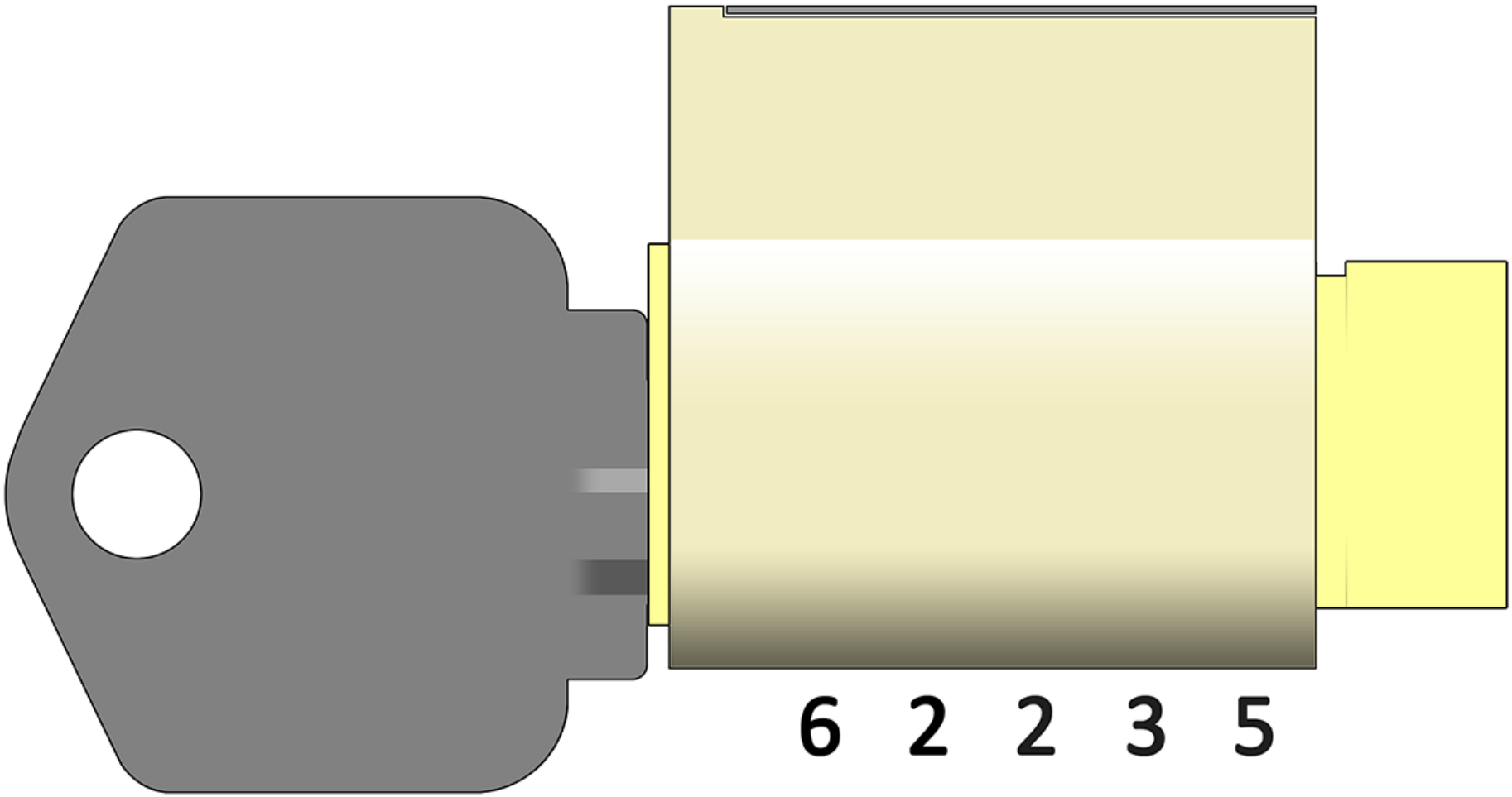
MACS is OK now, BTW



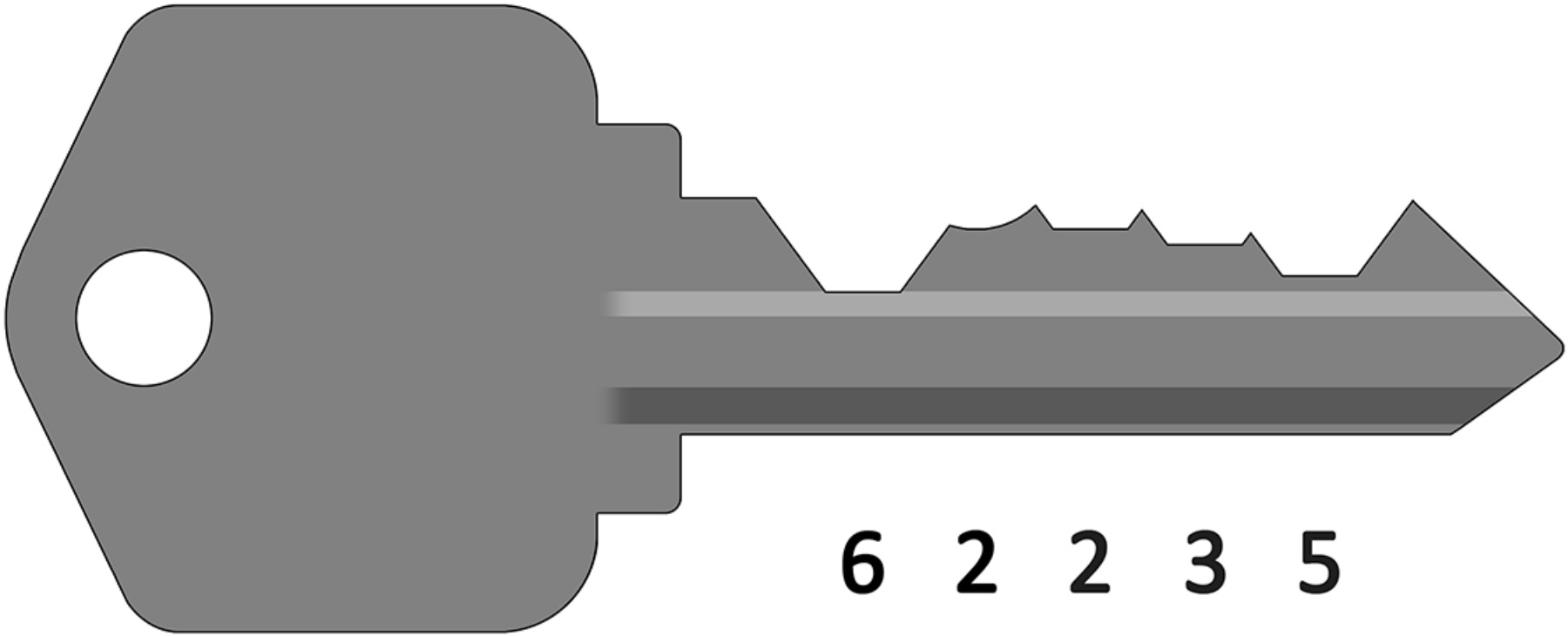
Try the Key in the Lock…



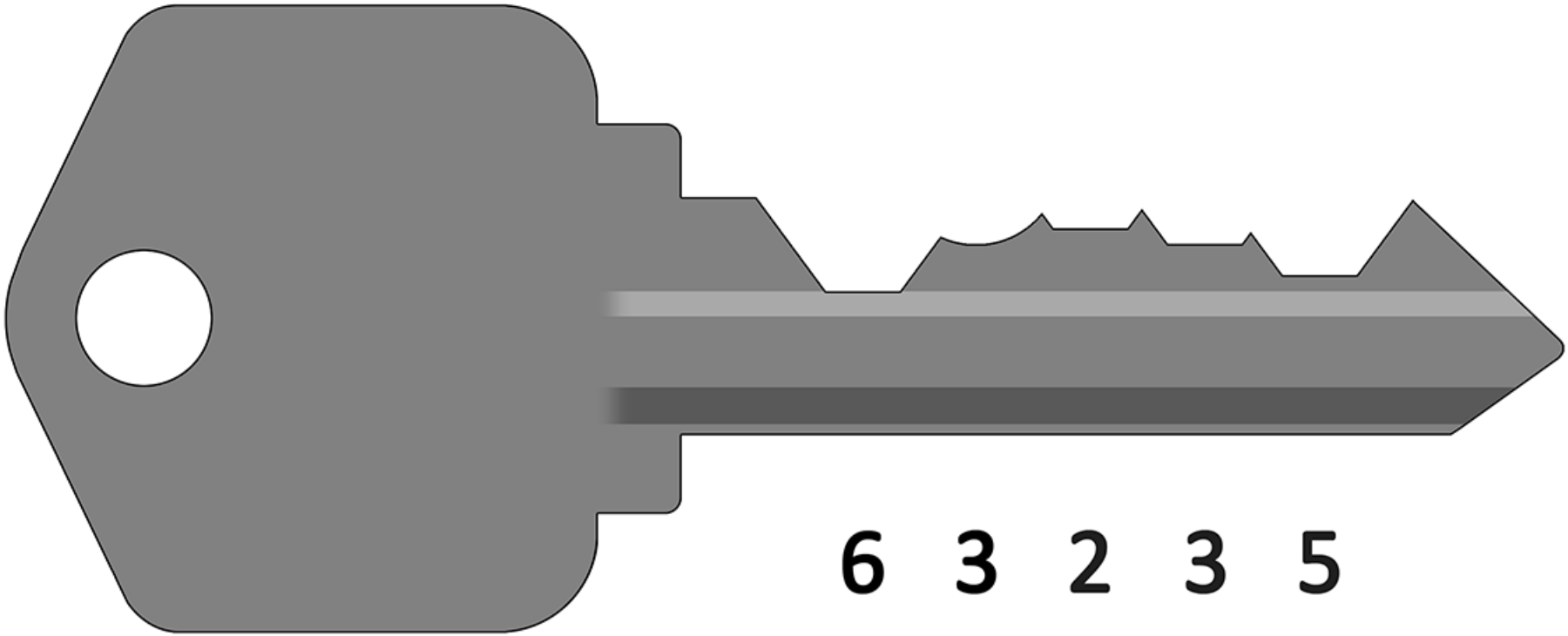
Try the Key in the Lock… The



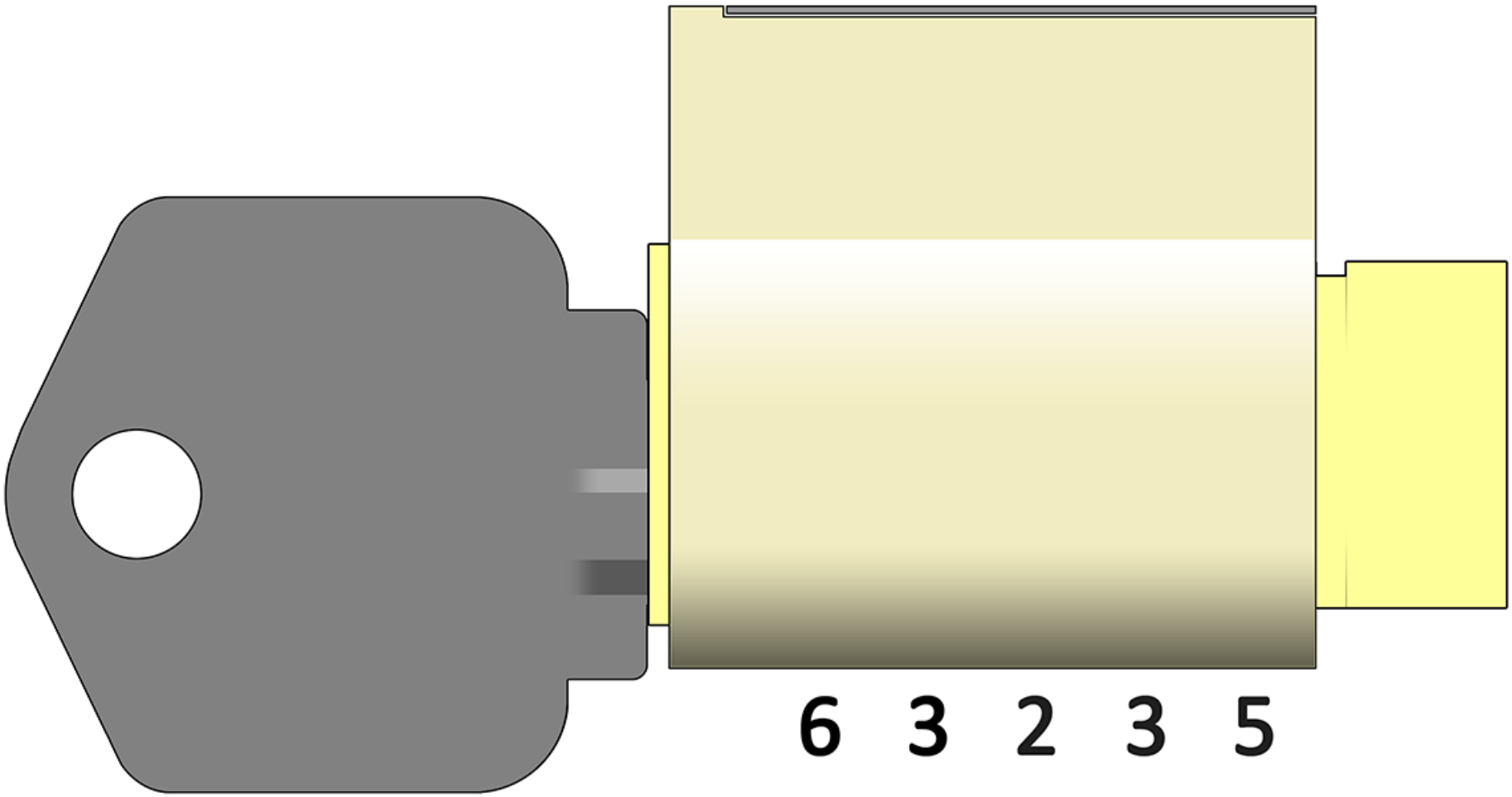
Remove the Key



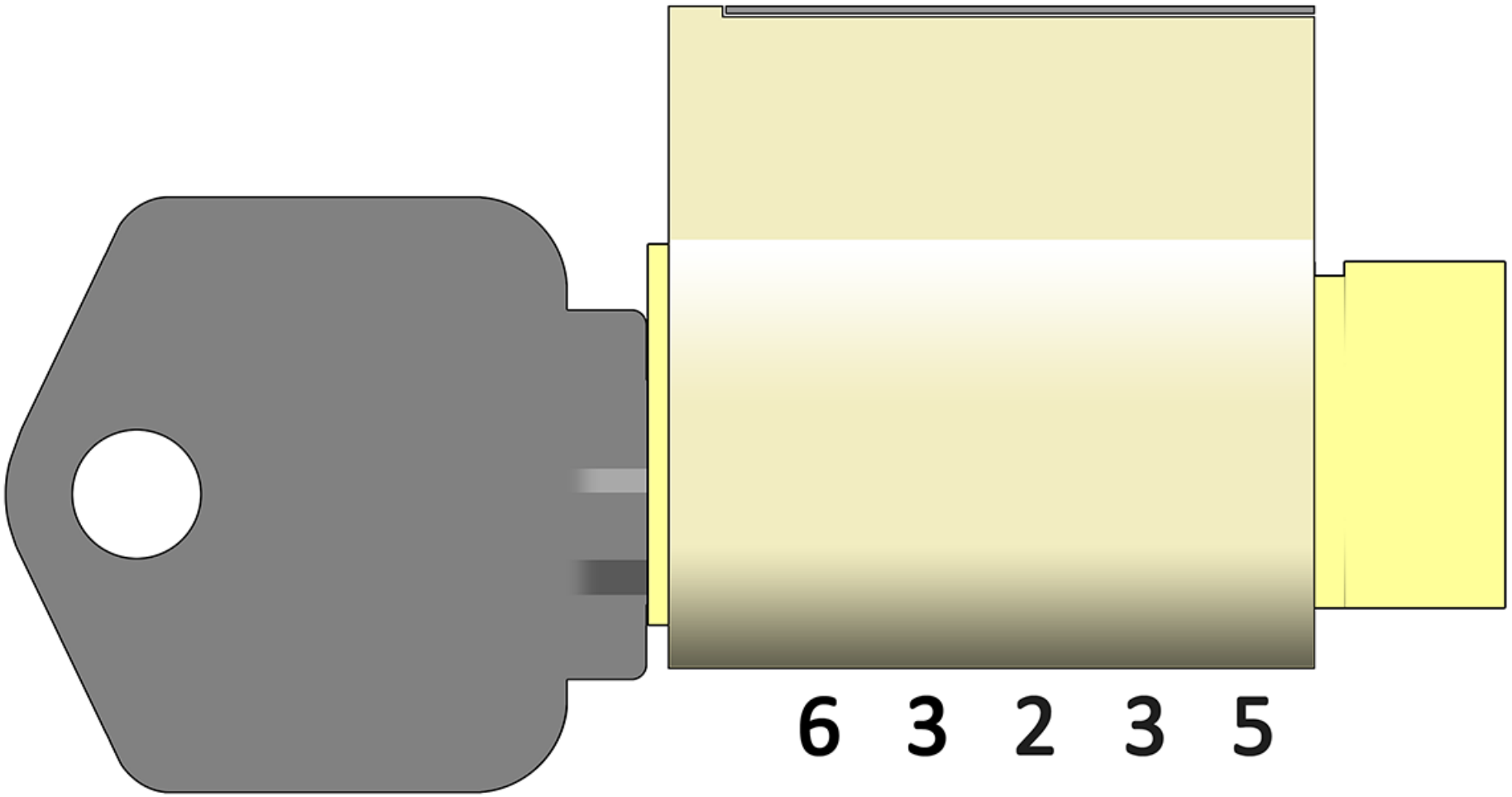
File Position Two Down by a



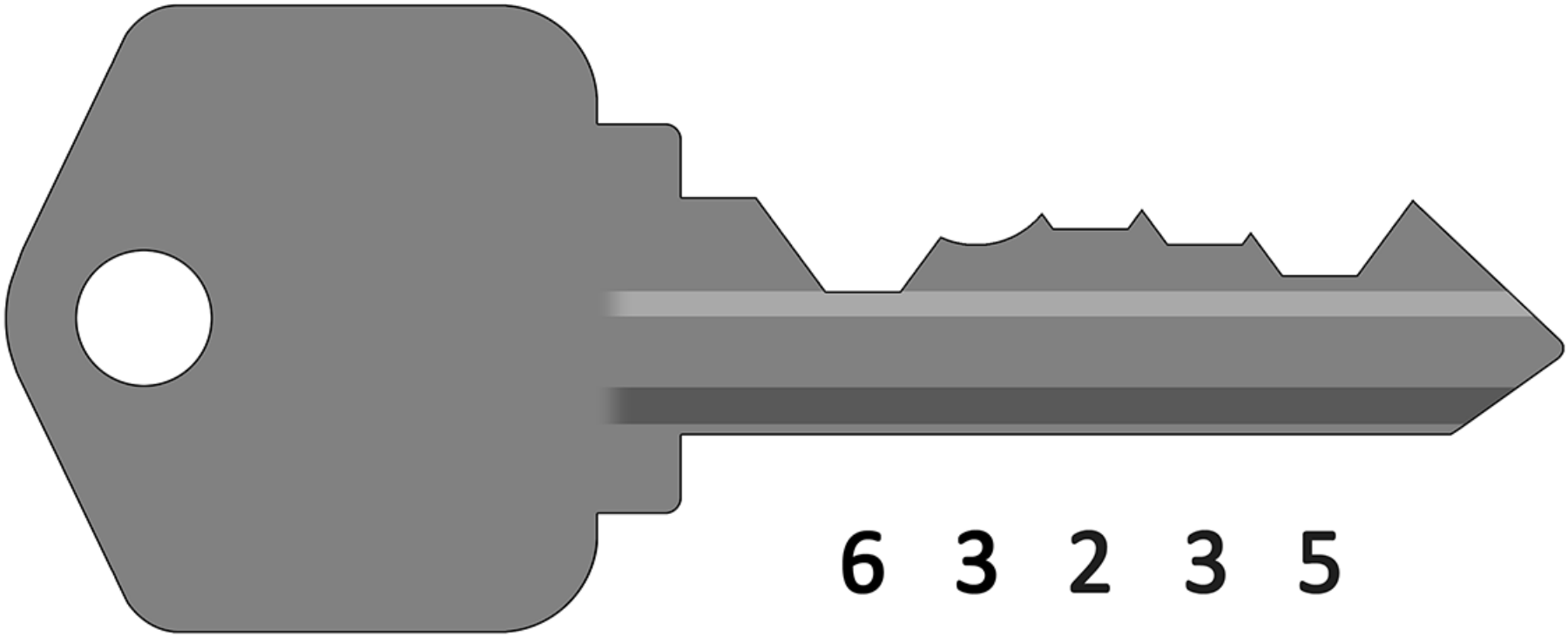
Try the Key…



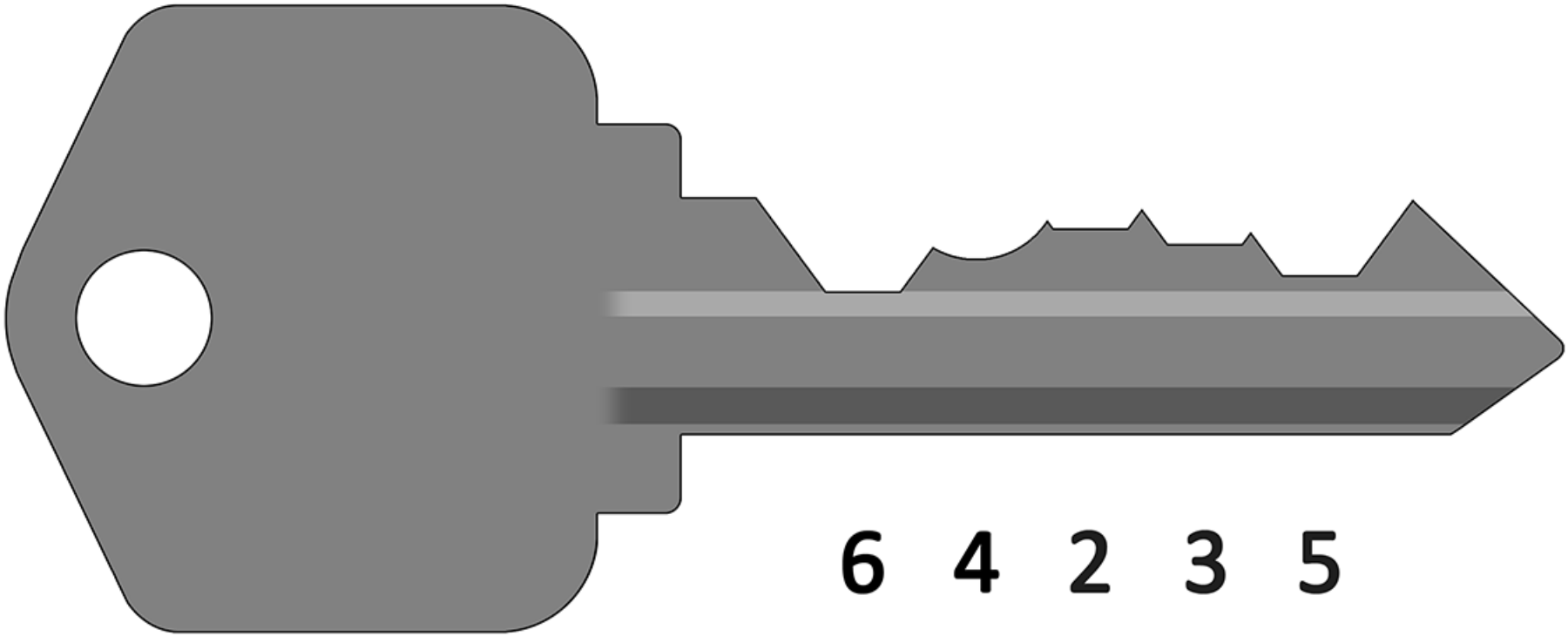
Try the Key… the Lock Doesn't



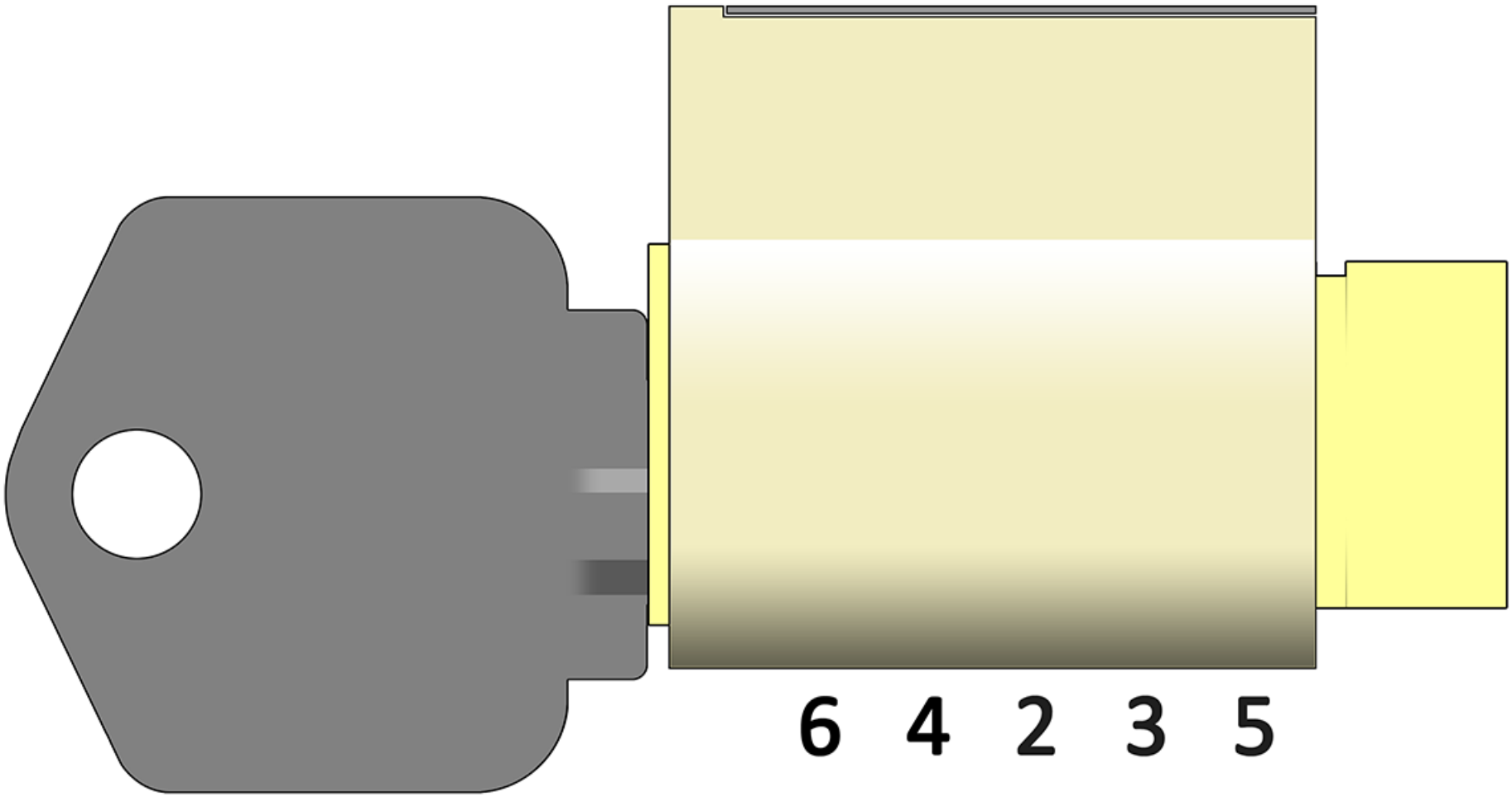
Remove the Key



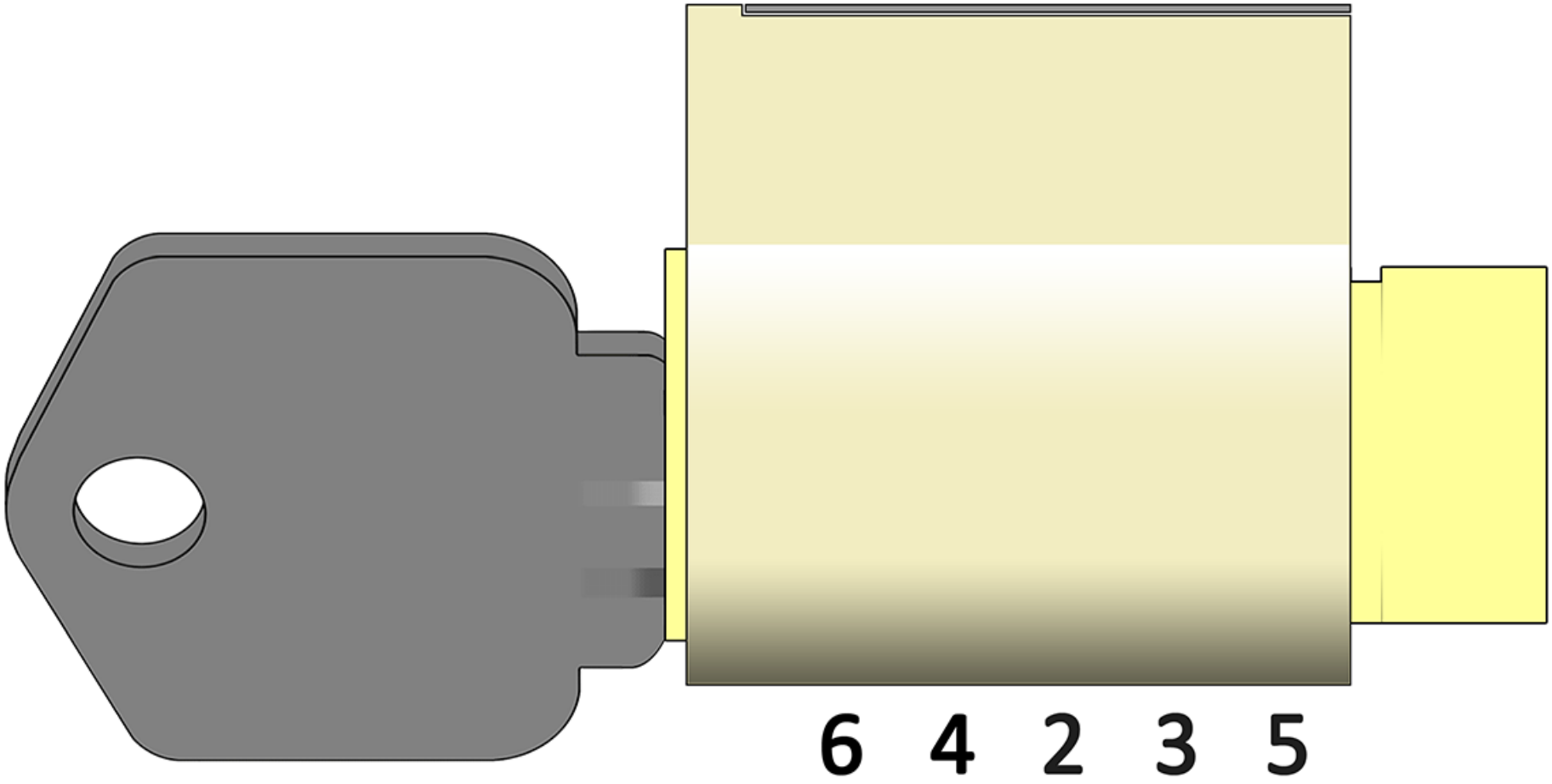
File Position Two Down by a



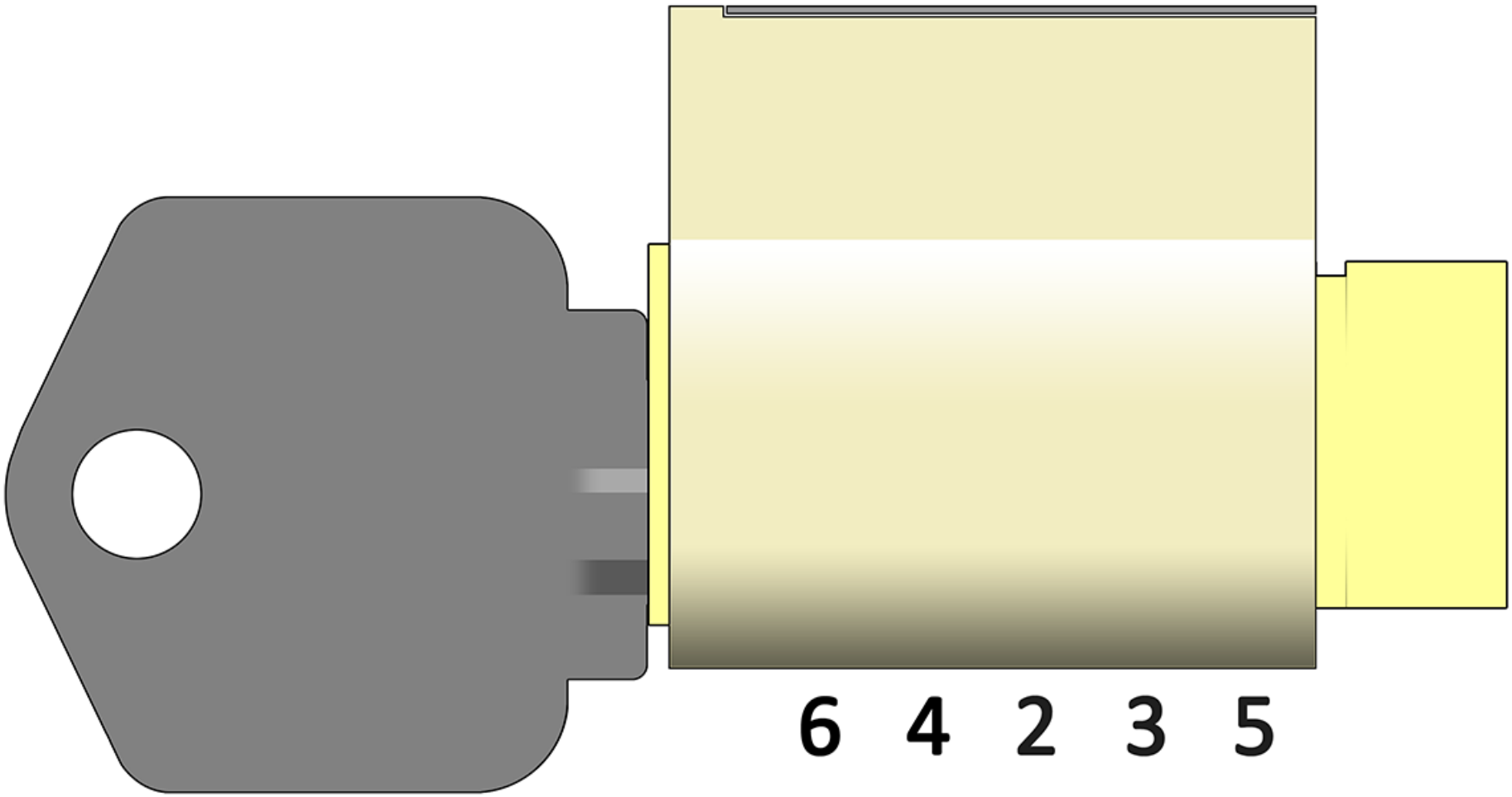
Try the Key…



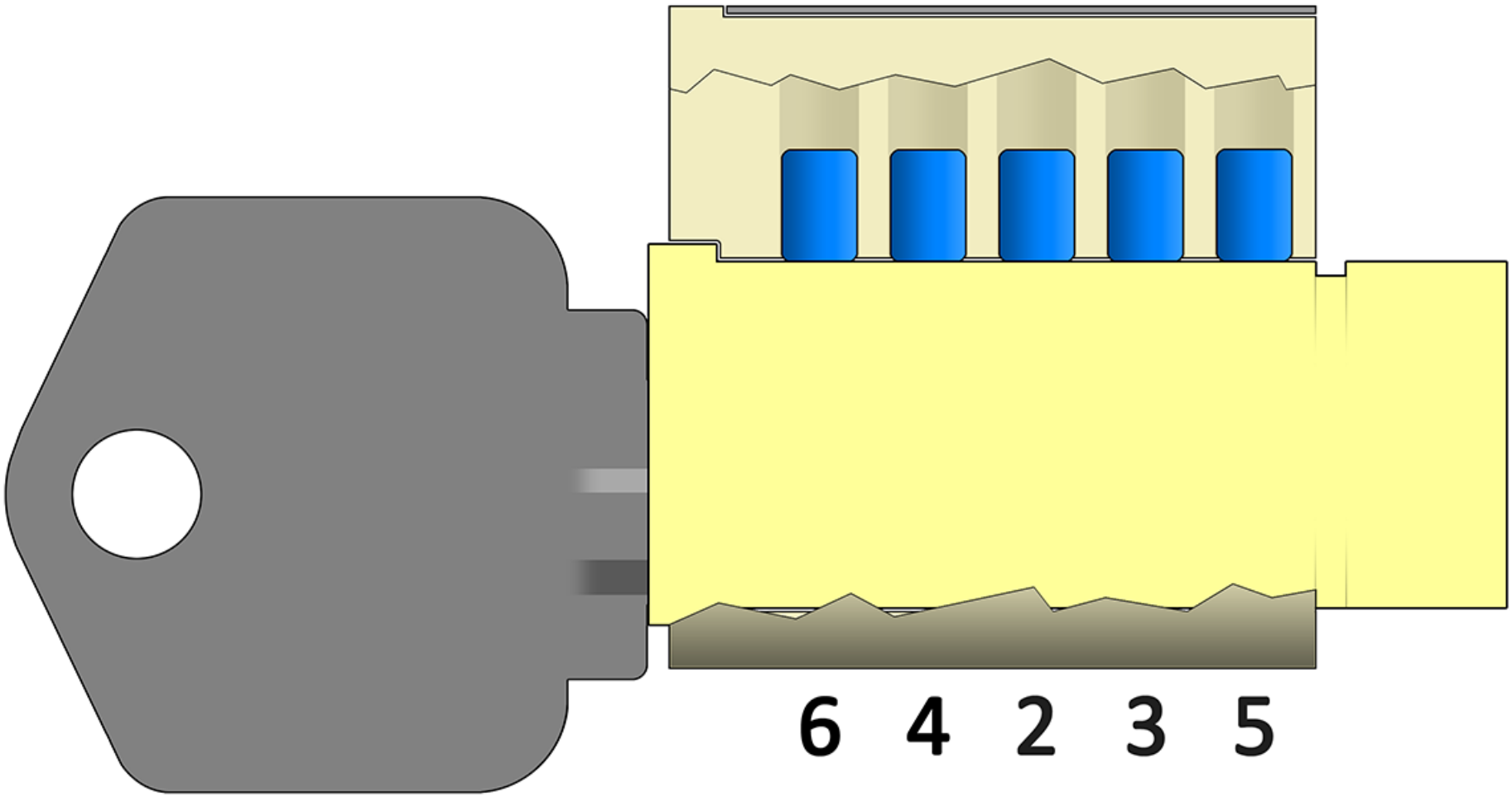
Try the Key… OPEN!



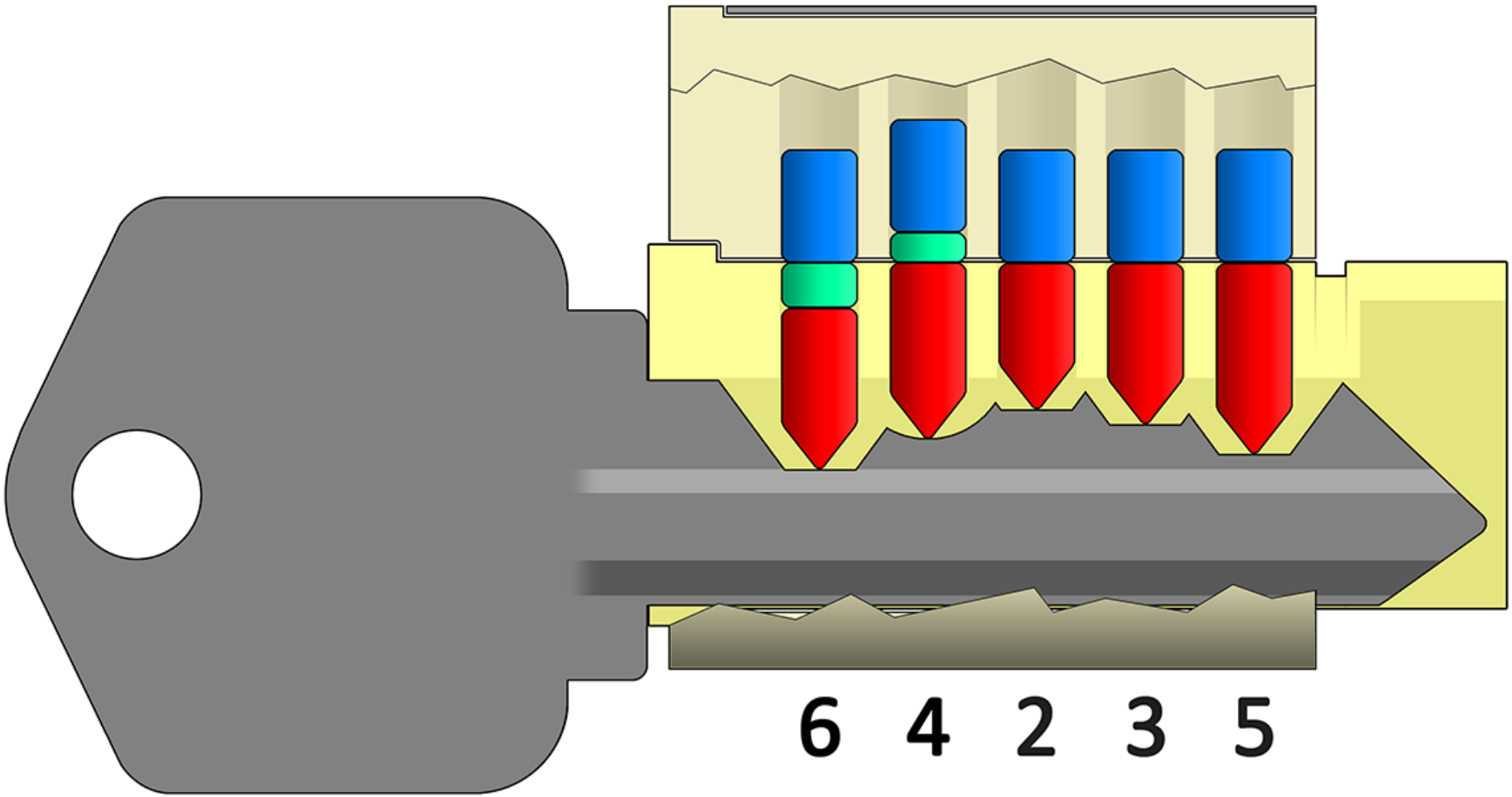
So What Have We Learned Now?



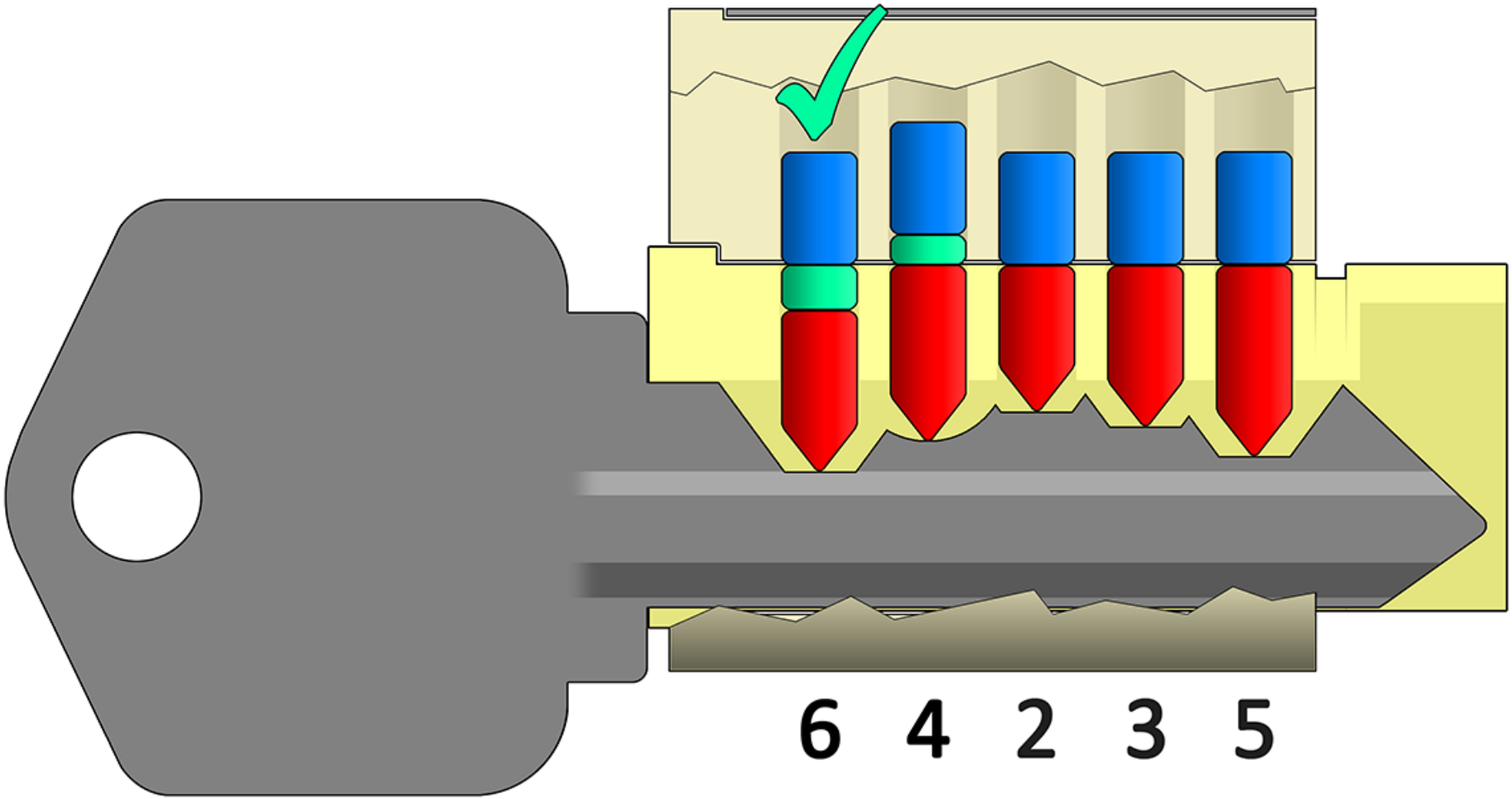
The Drivers Must be at the Plug's



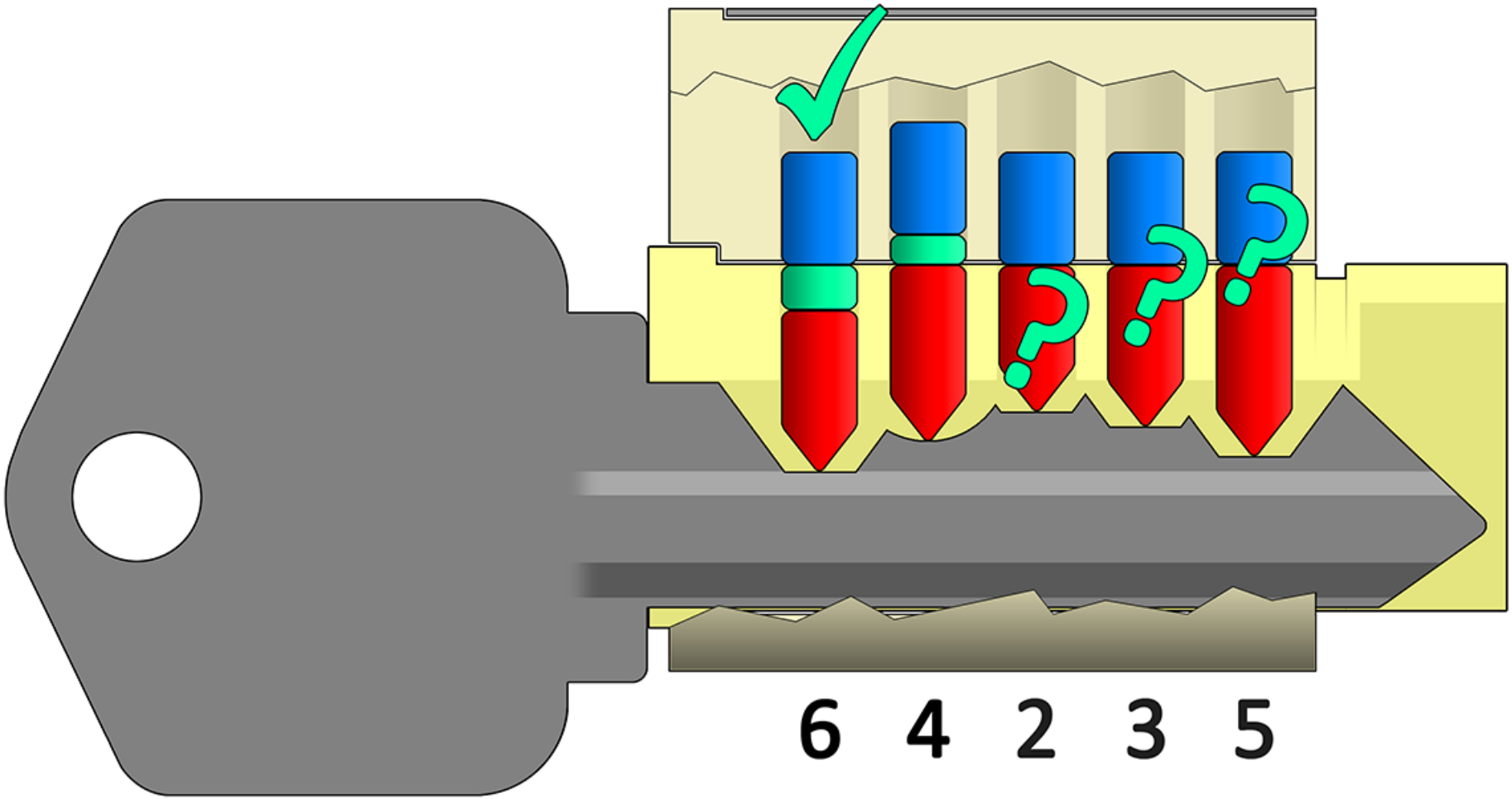
And Now We Know the Following…



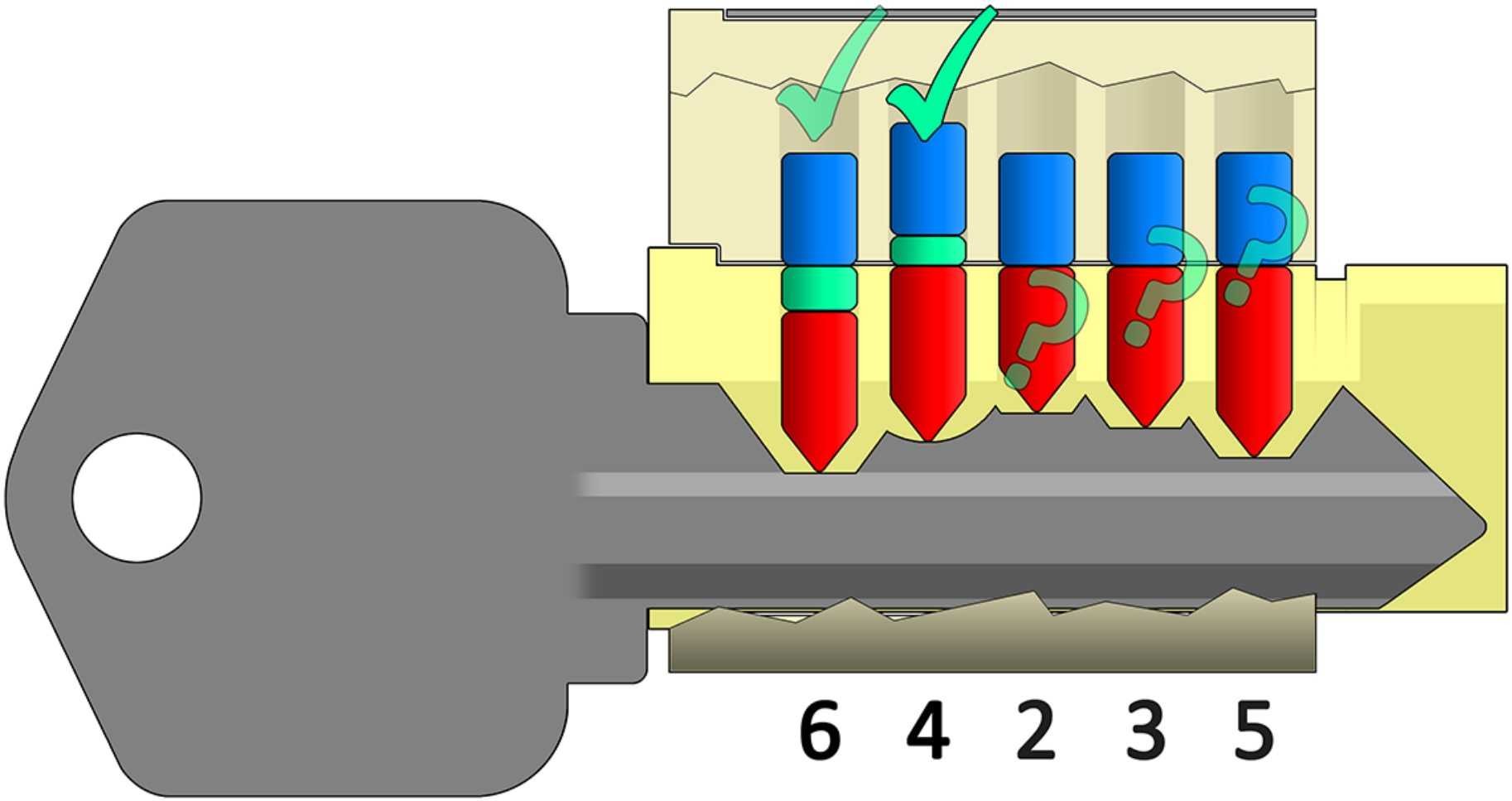
We've Learned This Earlier



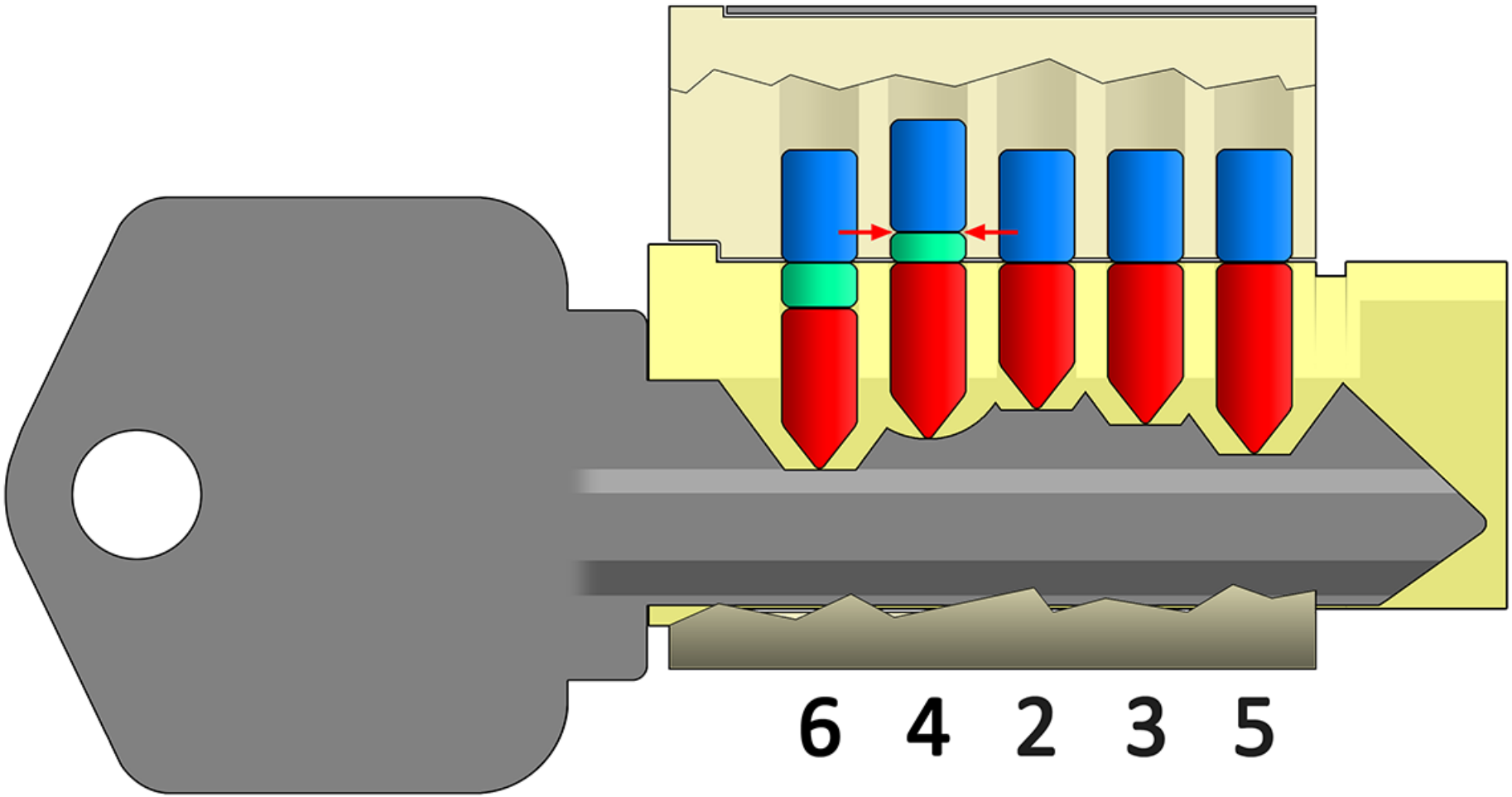
We Don't Know About These



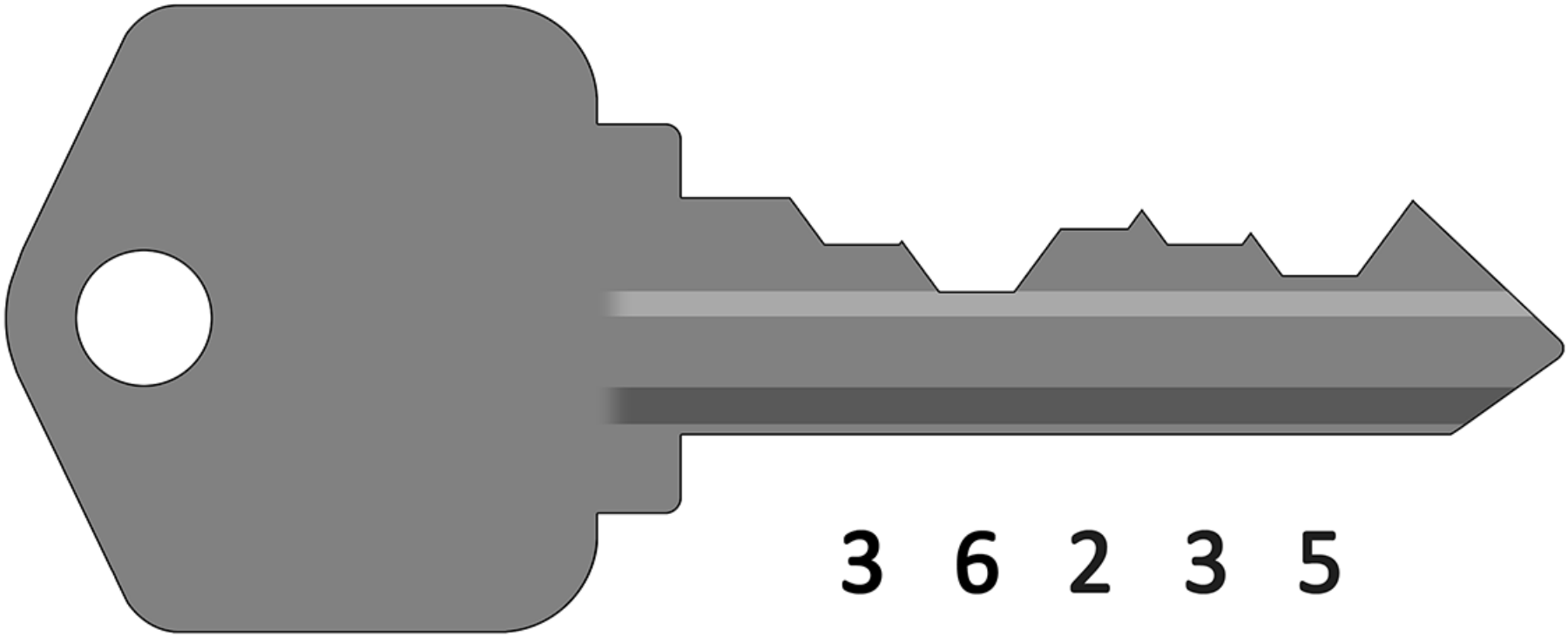
But Now Our Exploring Here is



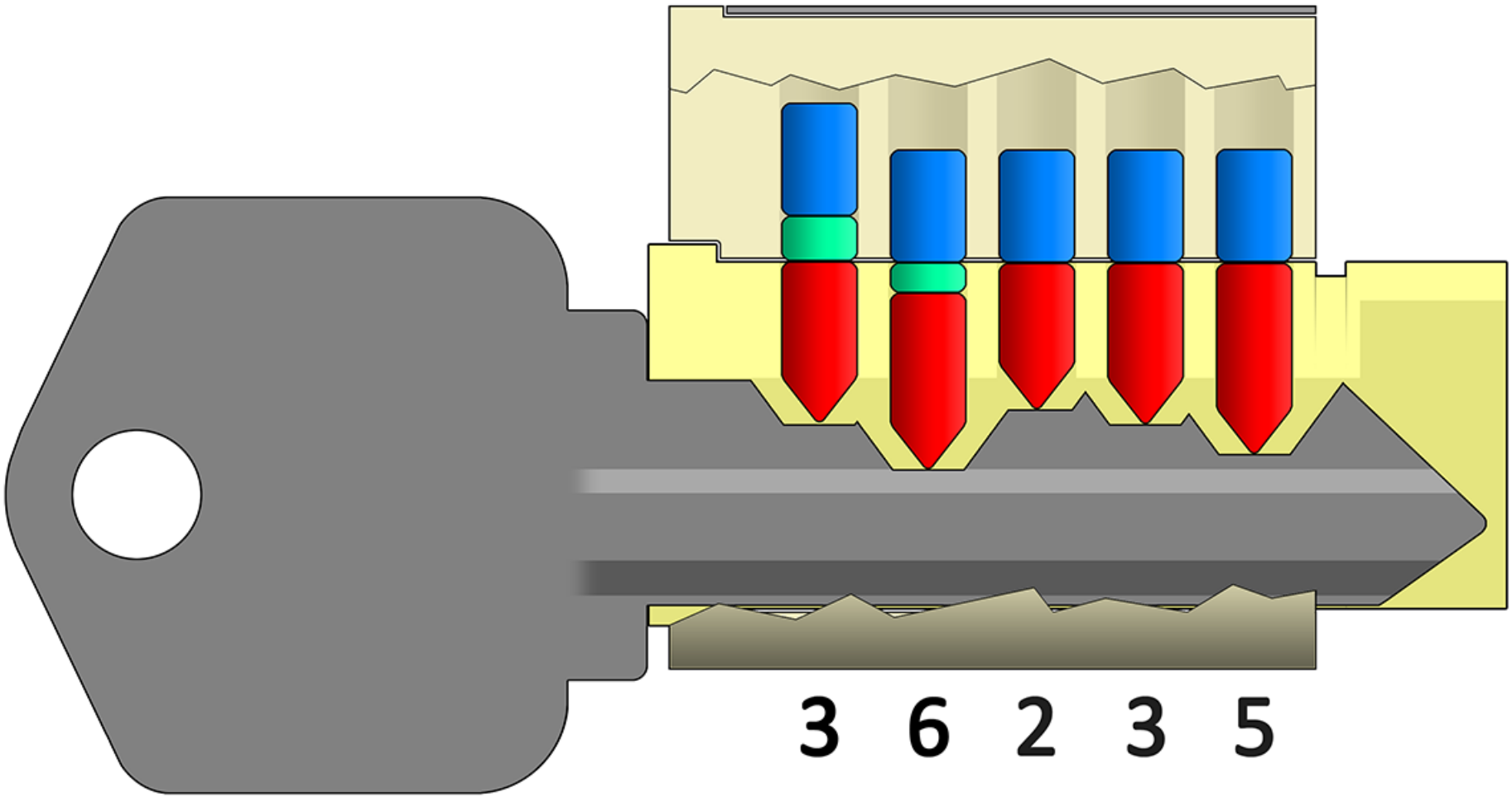
There is a Shear Line Here



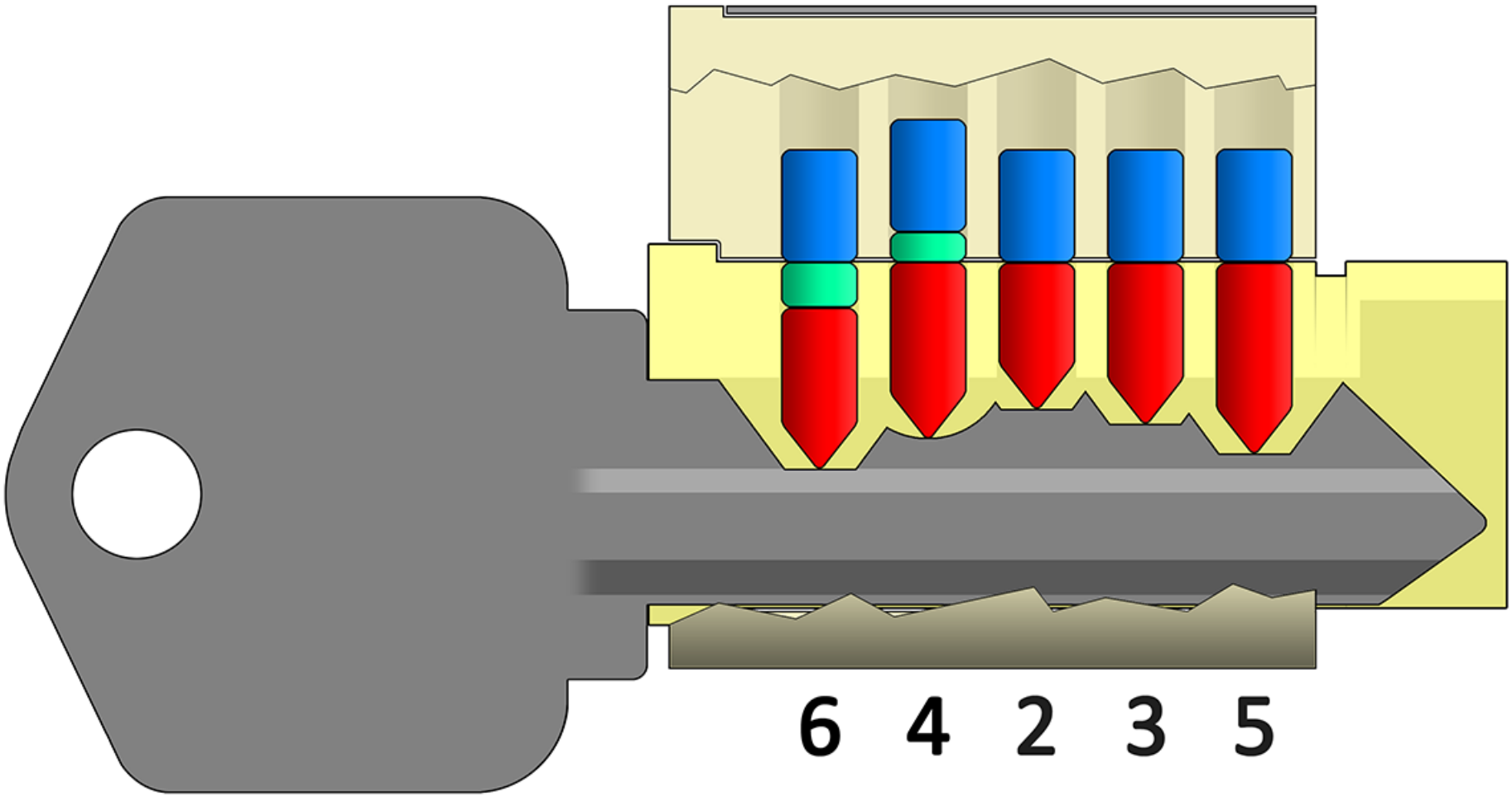
There is a Shear Line Here, We



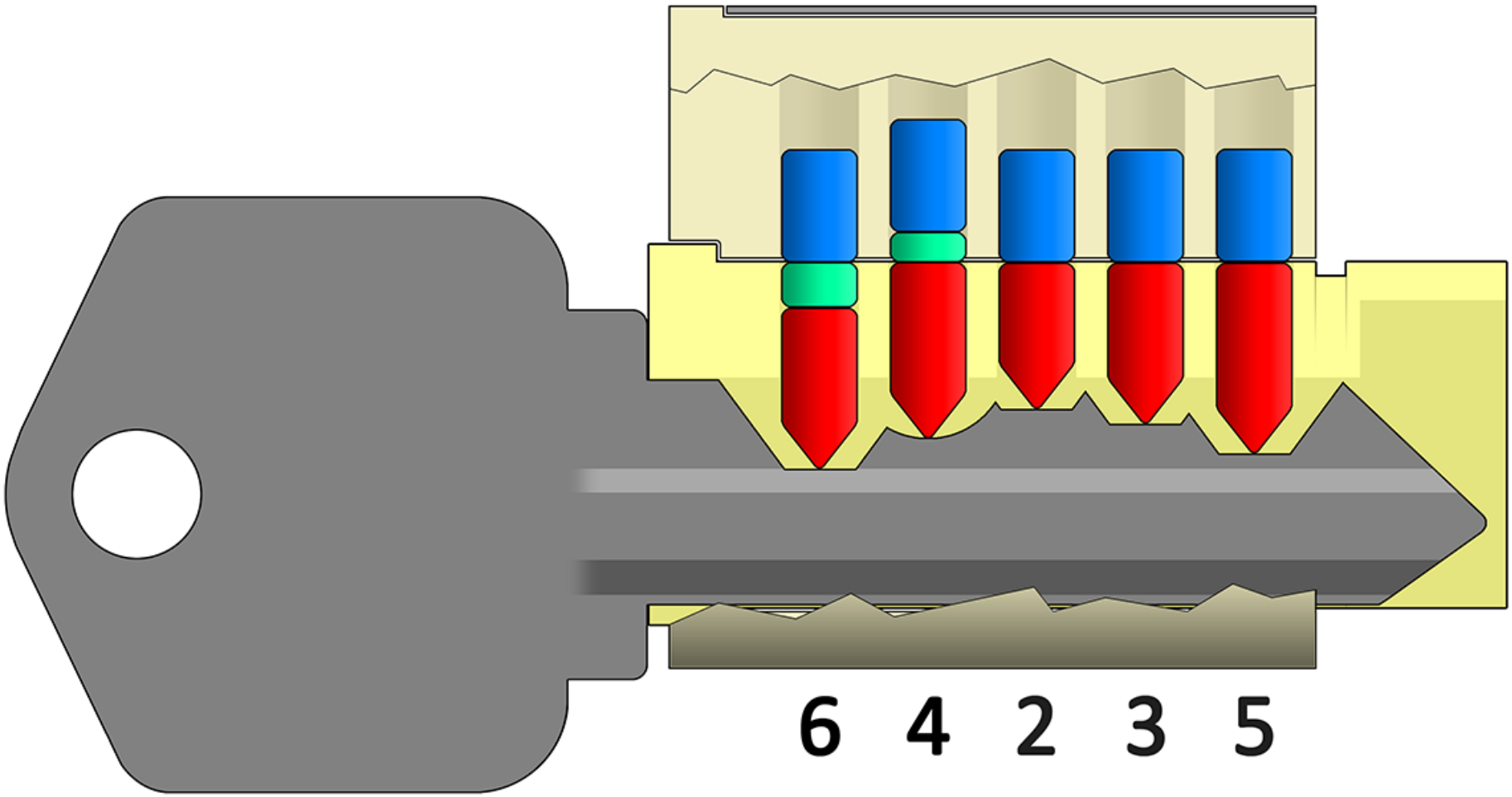
There is a Shear Line Here, We



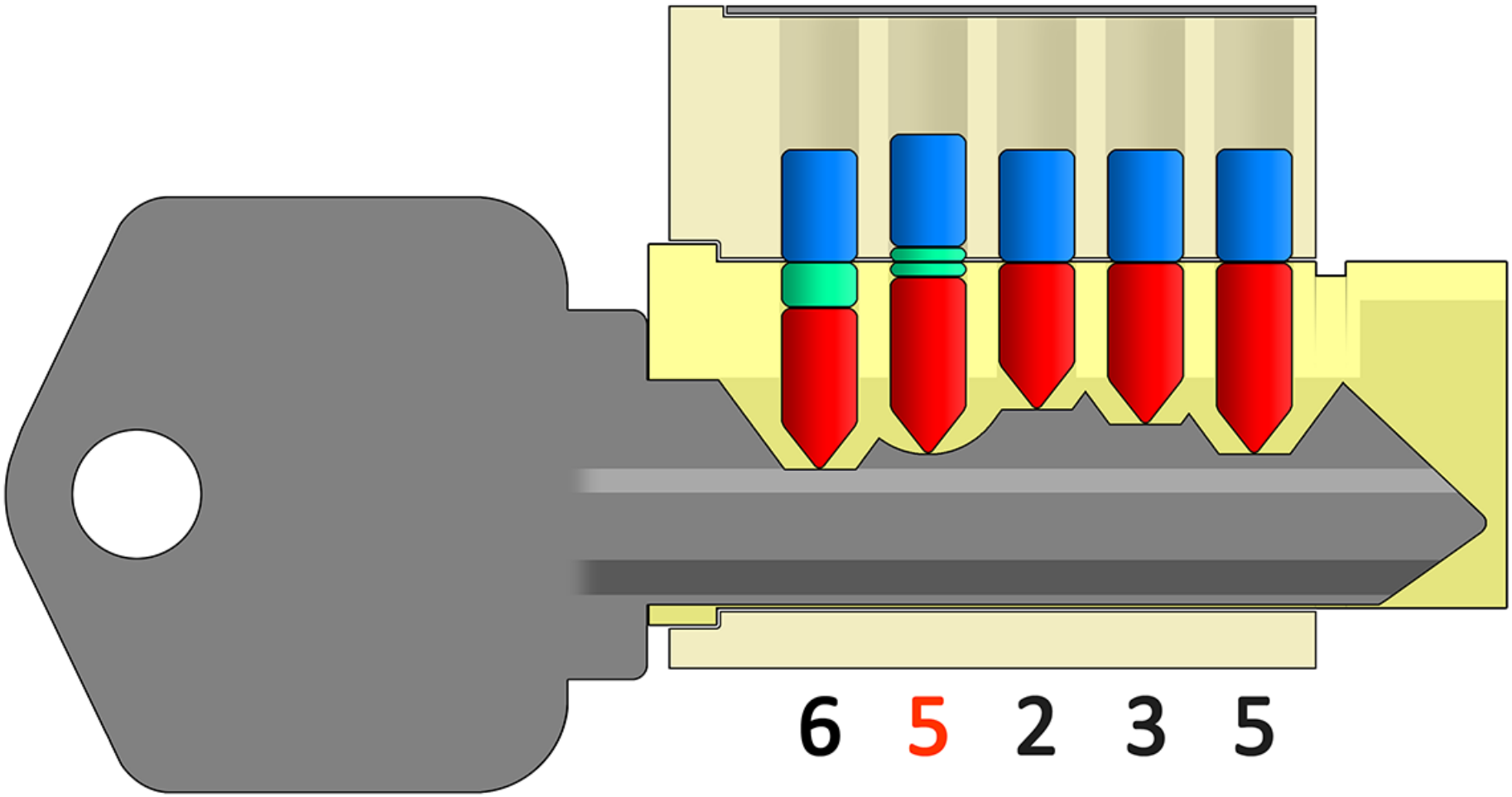
So We're Basically Done with



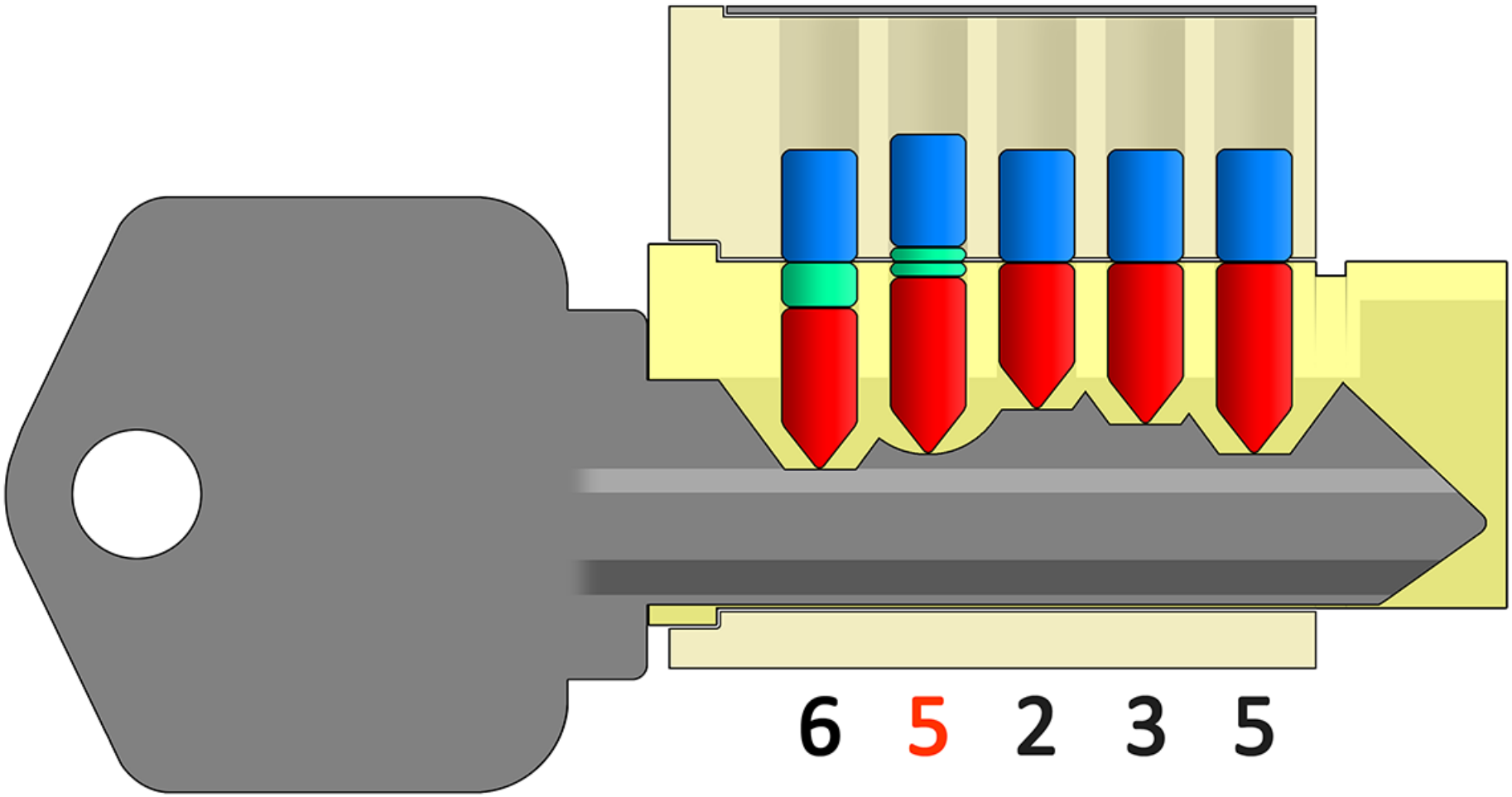
So We're Basically Done with



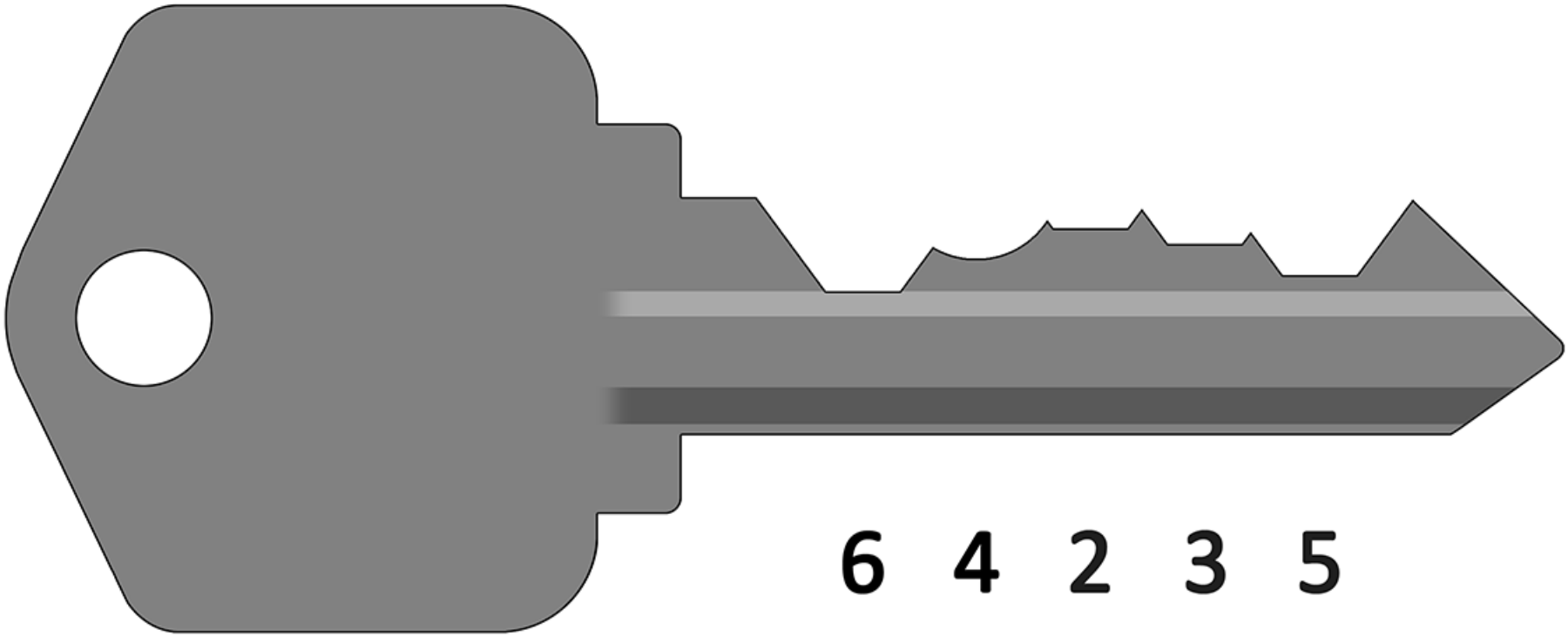
Single Depth Mastering Pins are



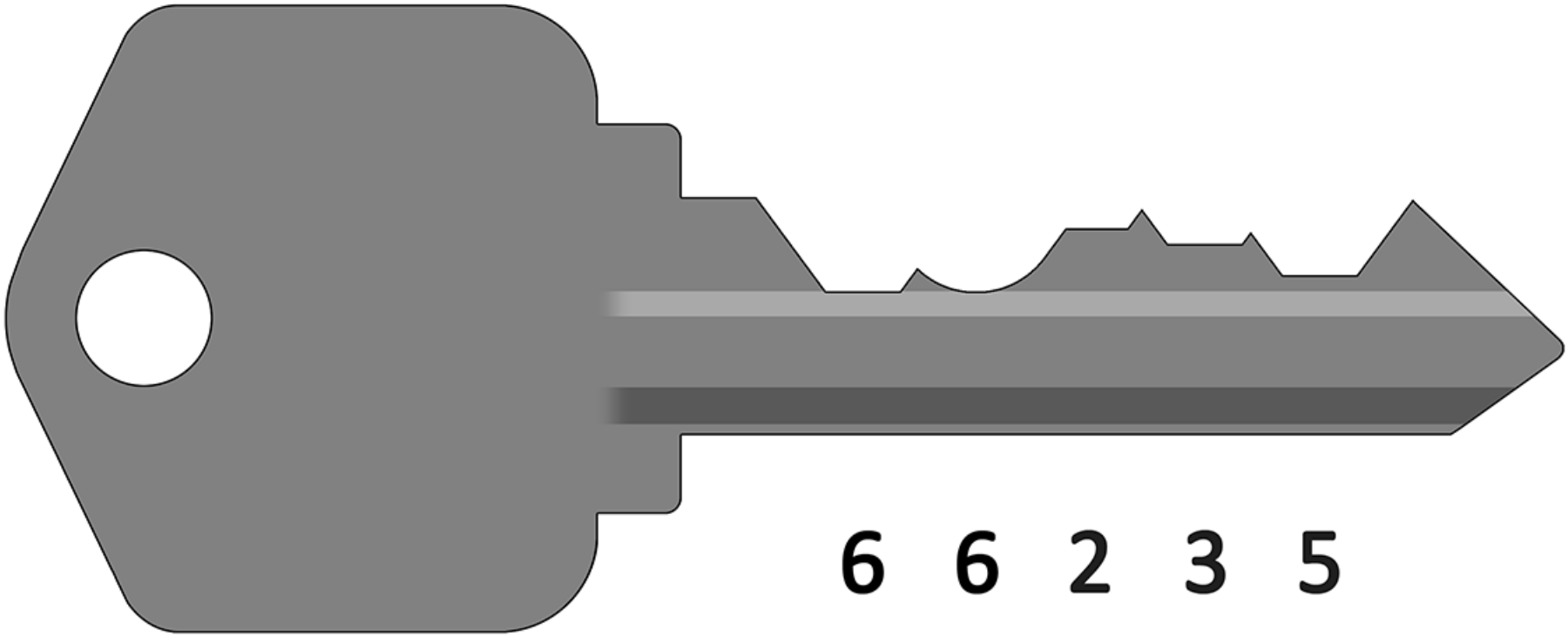
So, a Five Depth is Highly



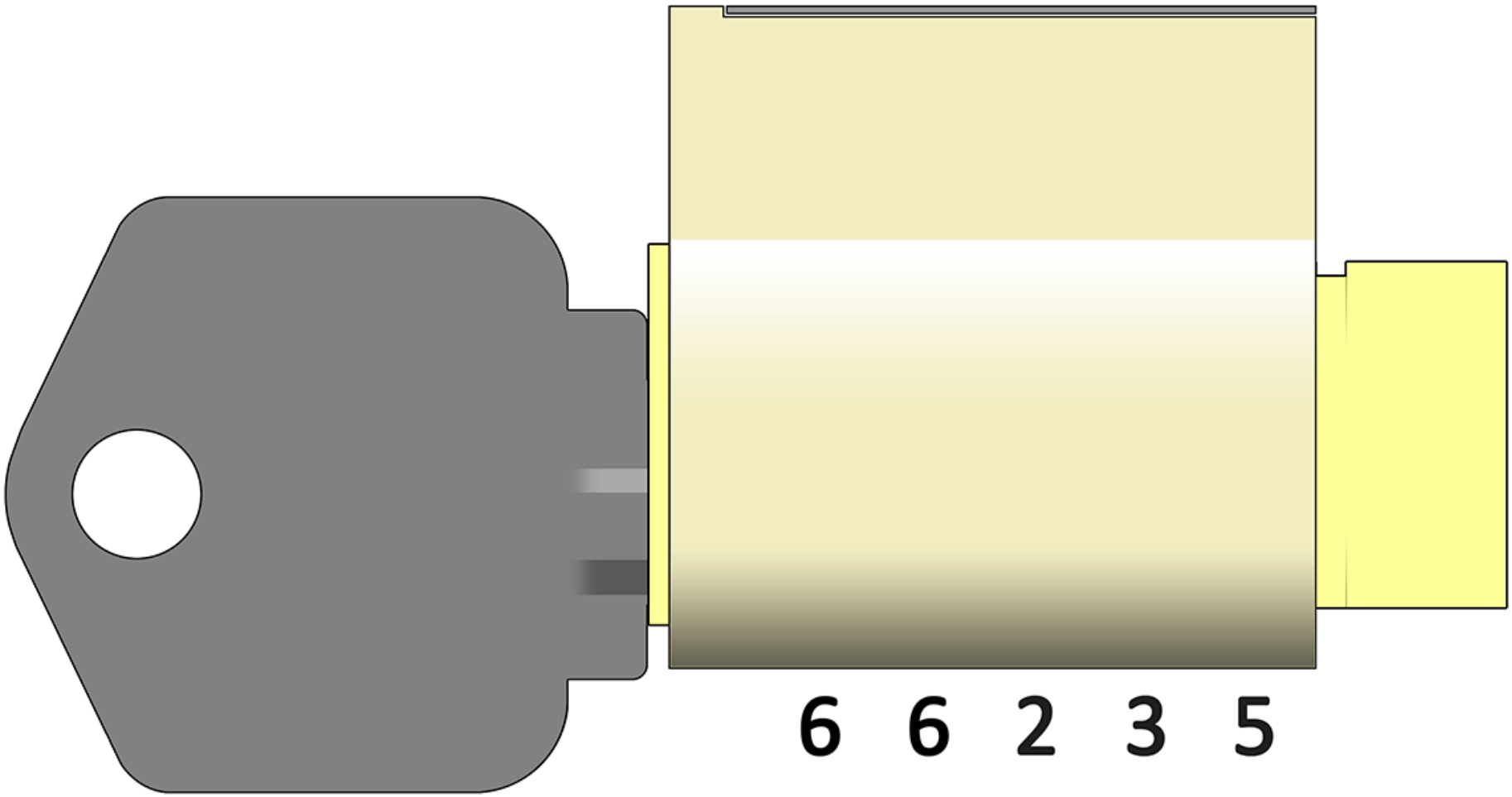
If We Wanted, We Could Take Our



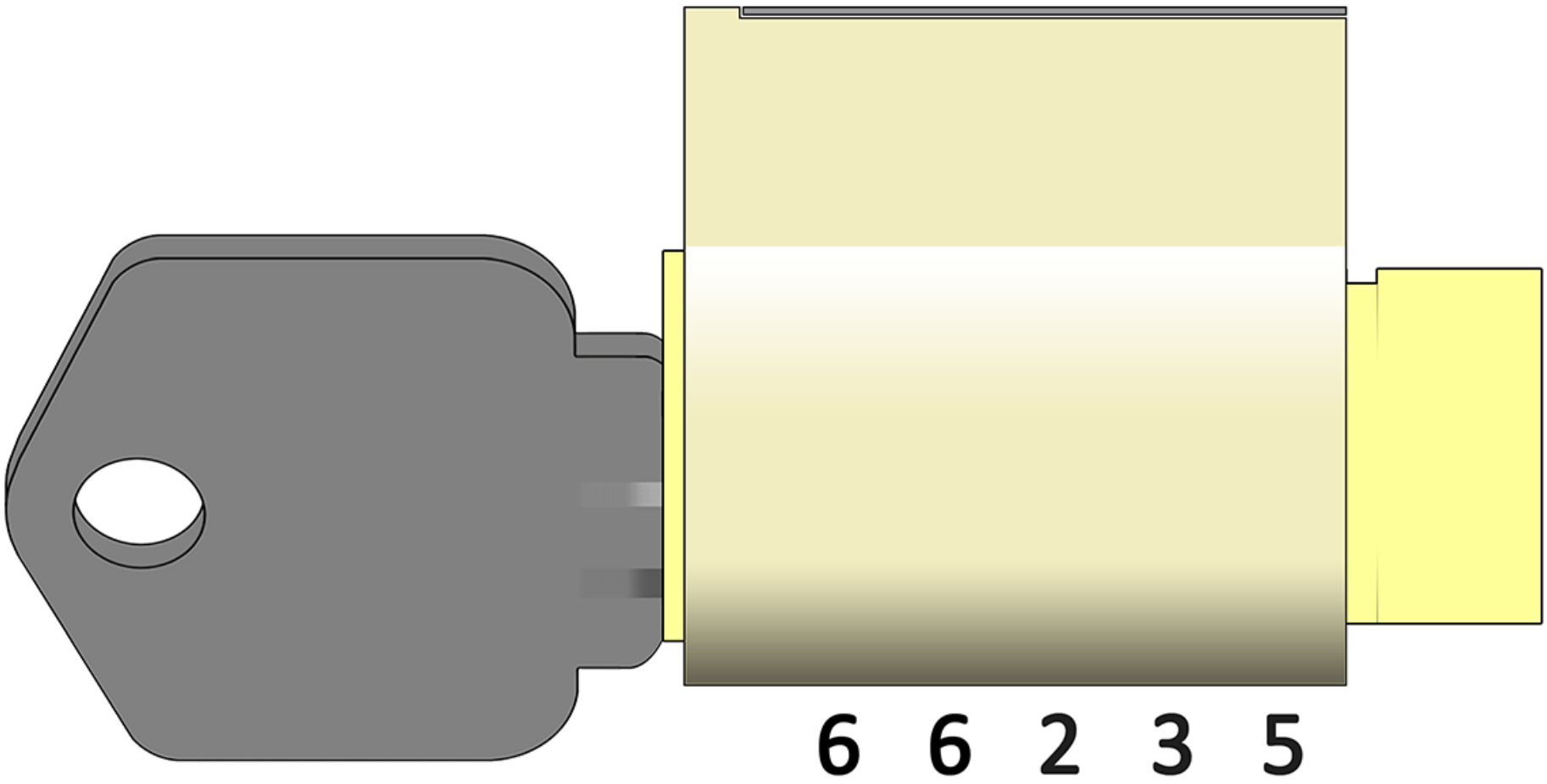
And File Down to the 6th Bitting



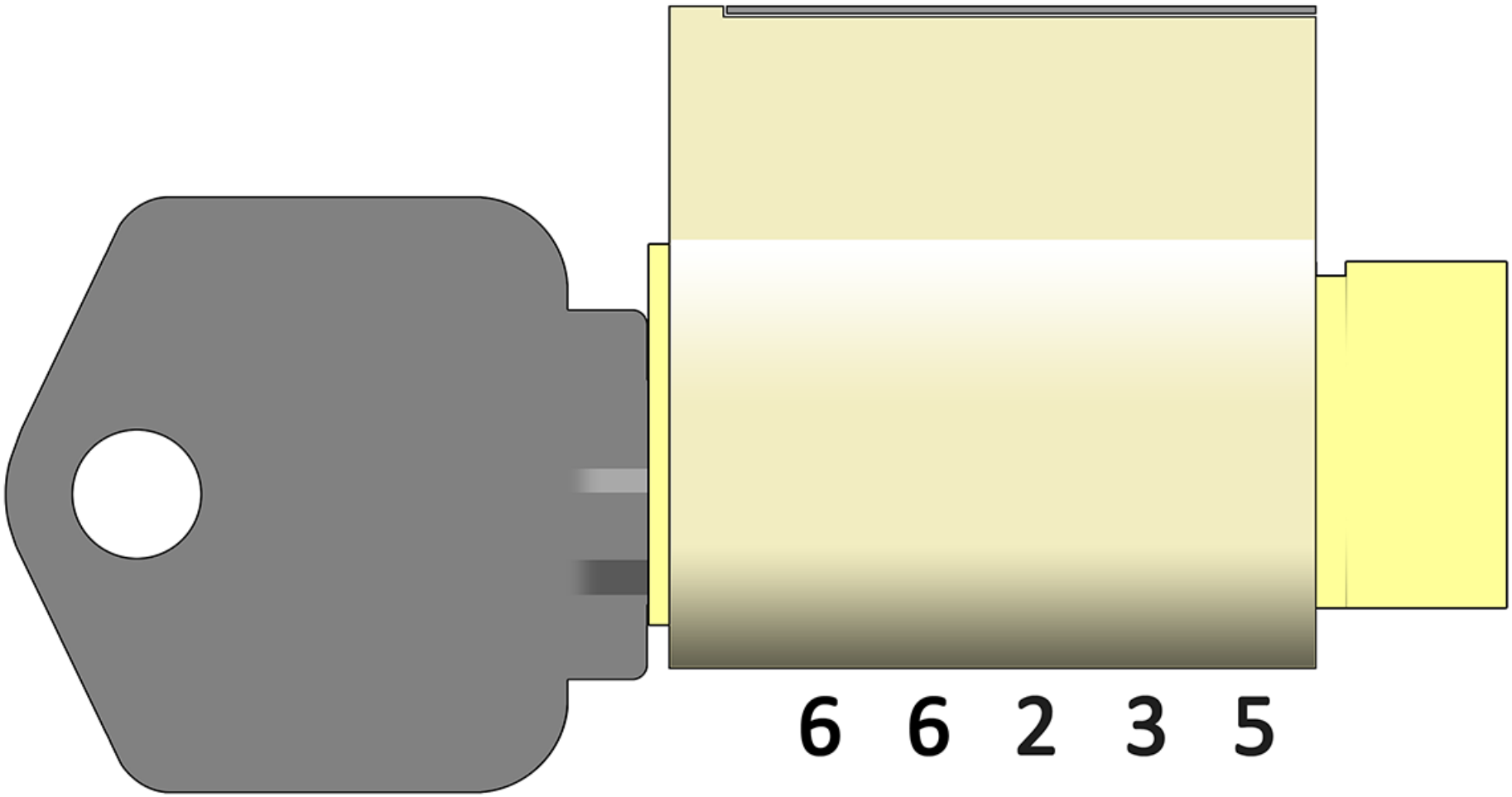
Try the Key…



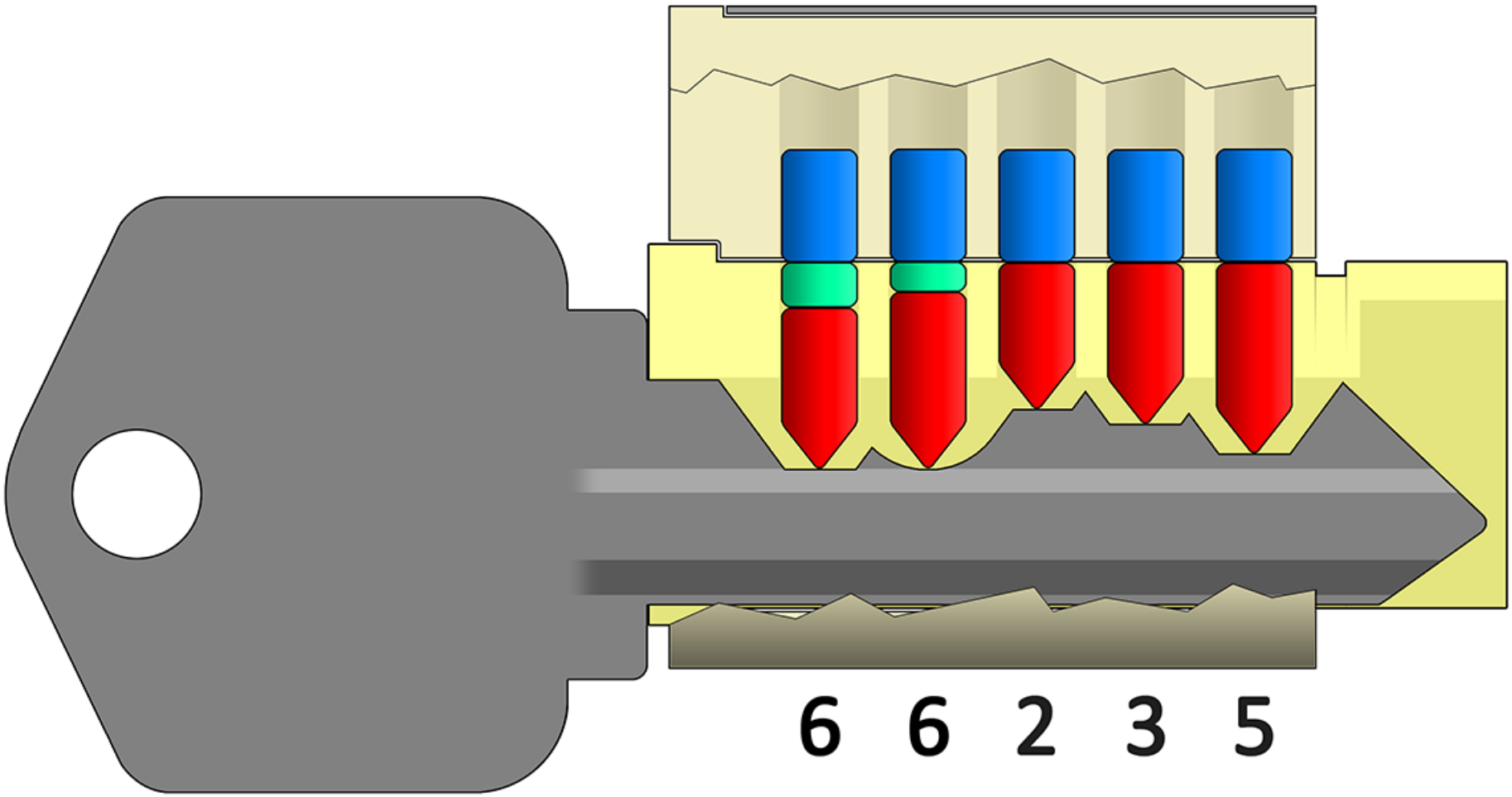
Try the Key… It Surely Should



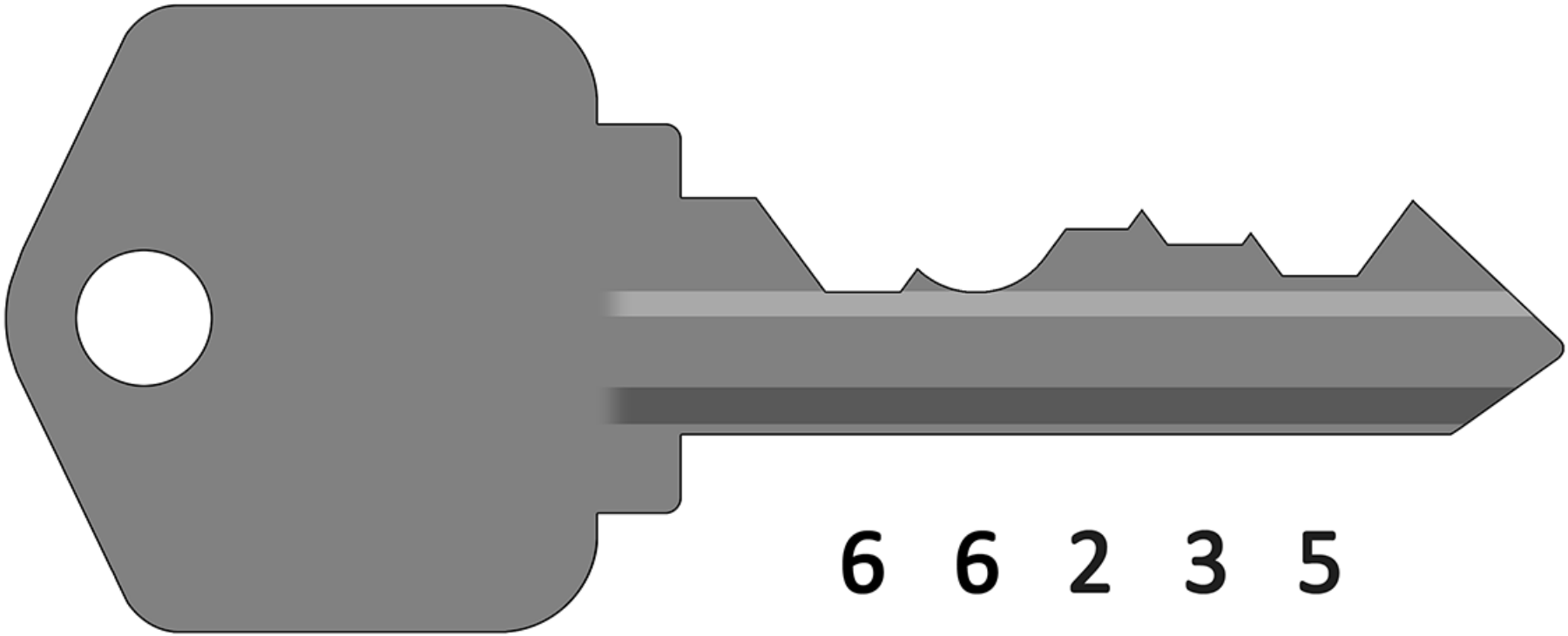
After All…



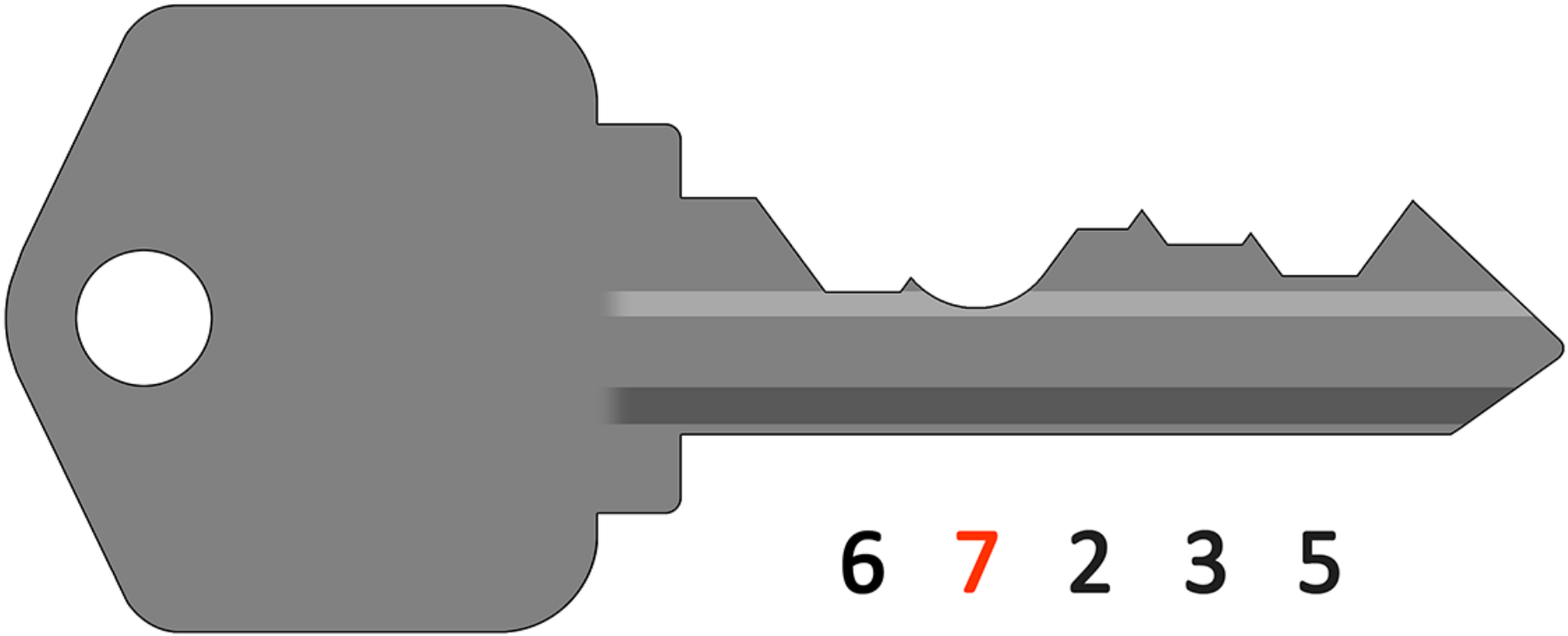
After All… Depth 6 was Known in



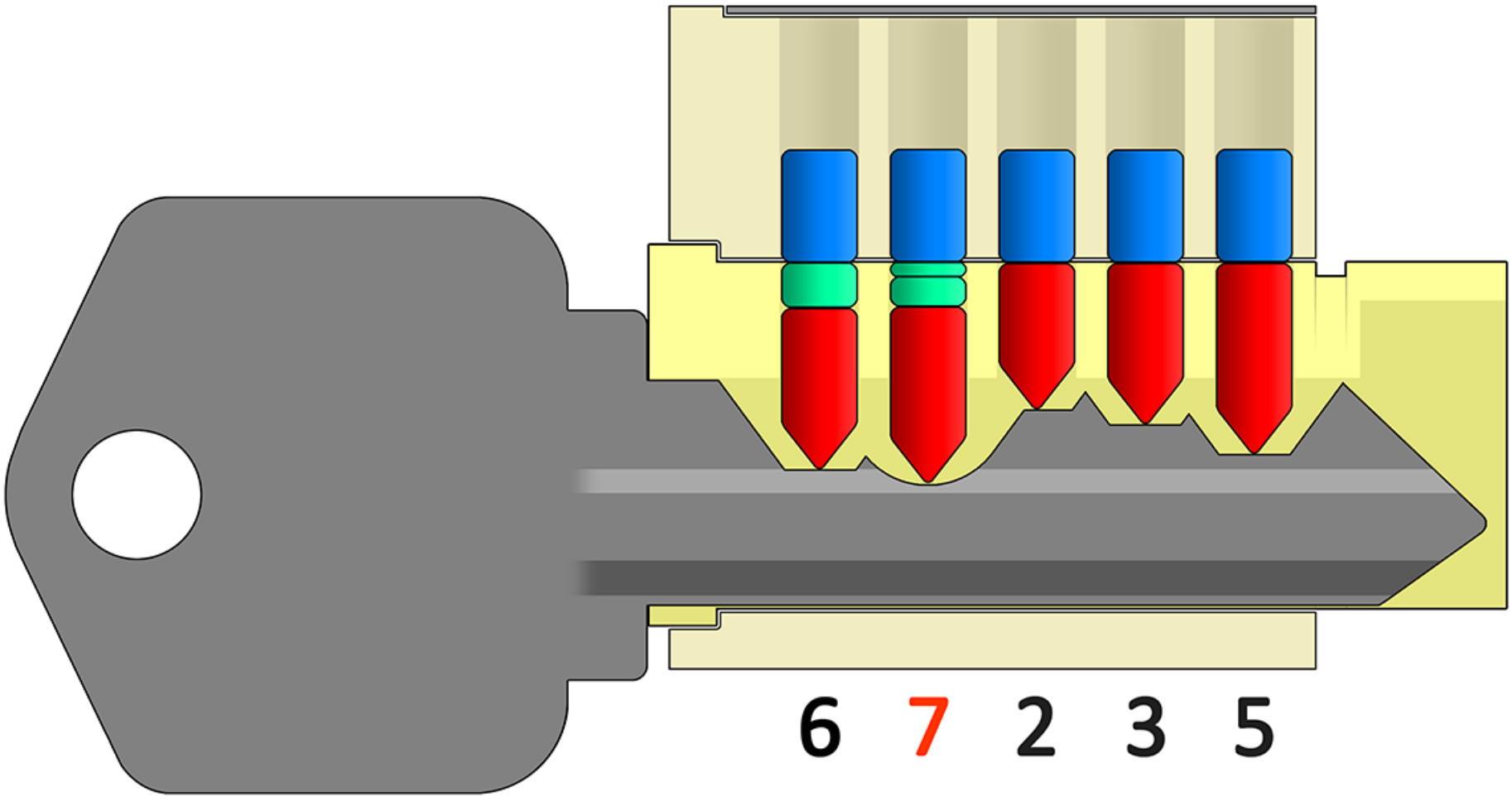
Further Exploring Is Not Really



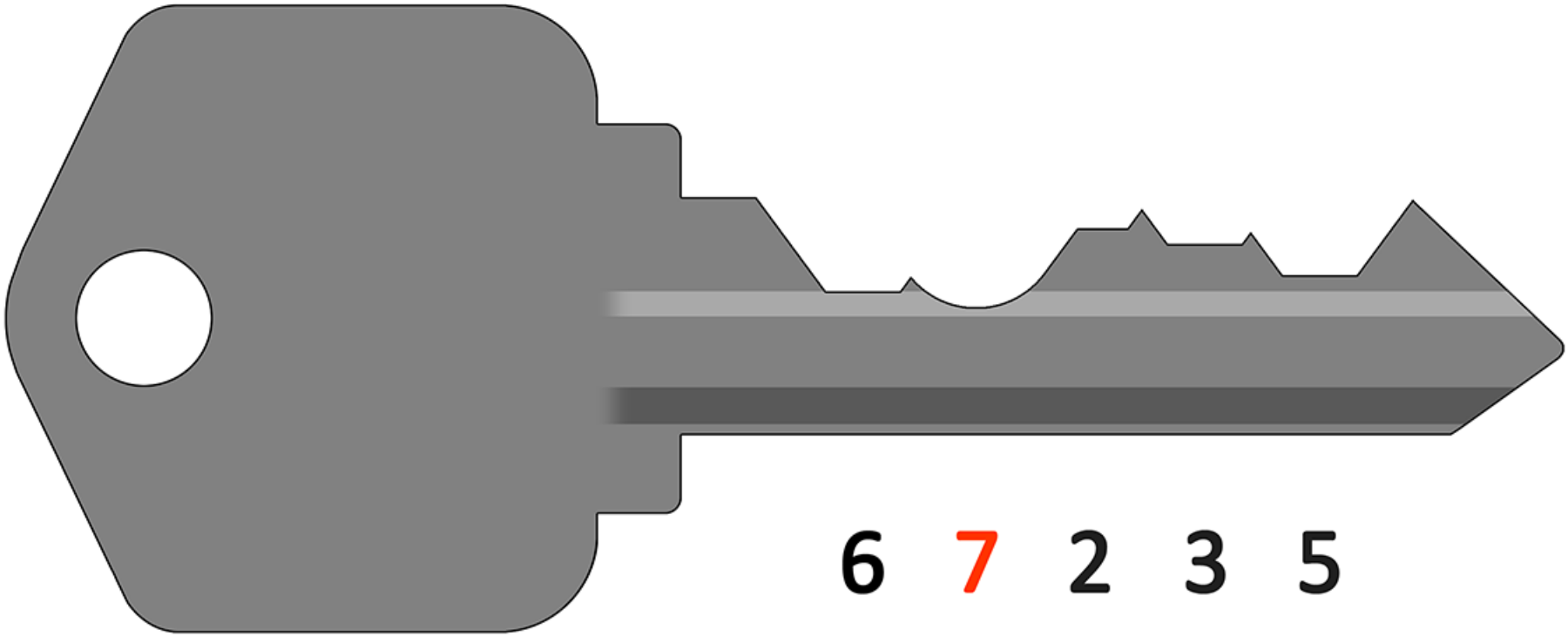
A Depth of Seven?



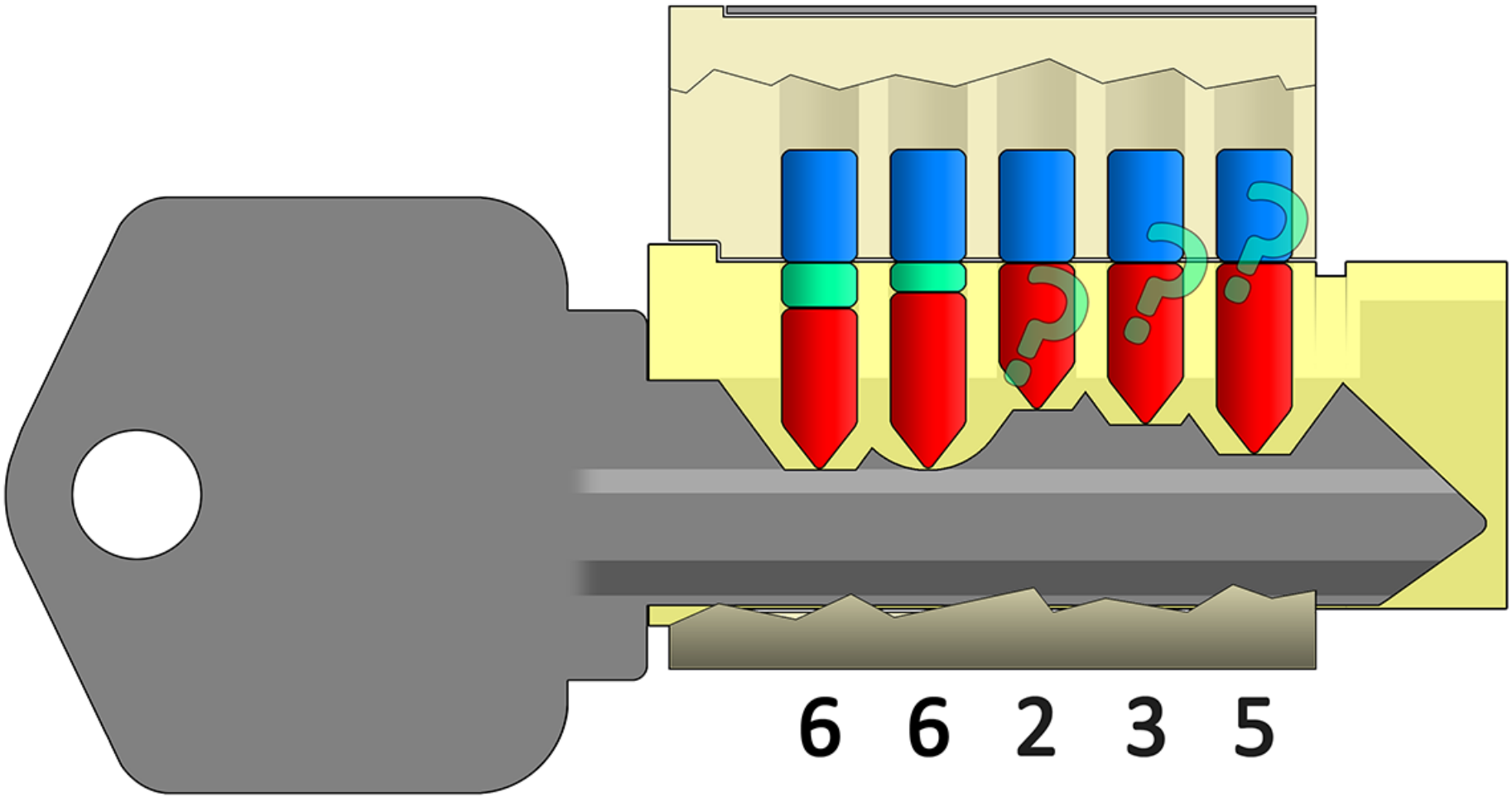
A Depth of Seven Would Mean



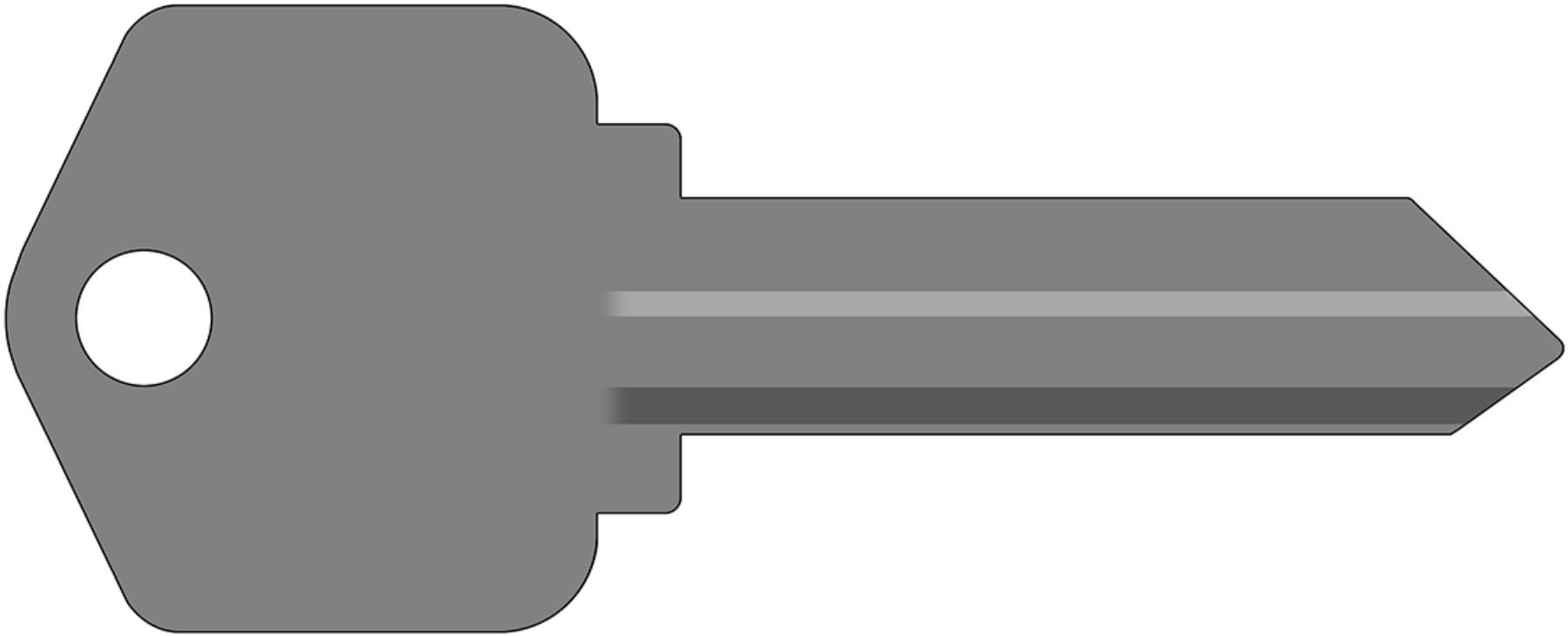
… And Kwikset Locks Don't Go



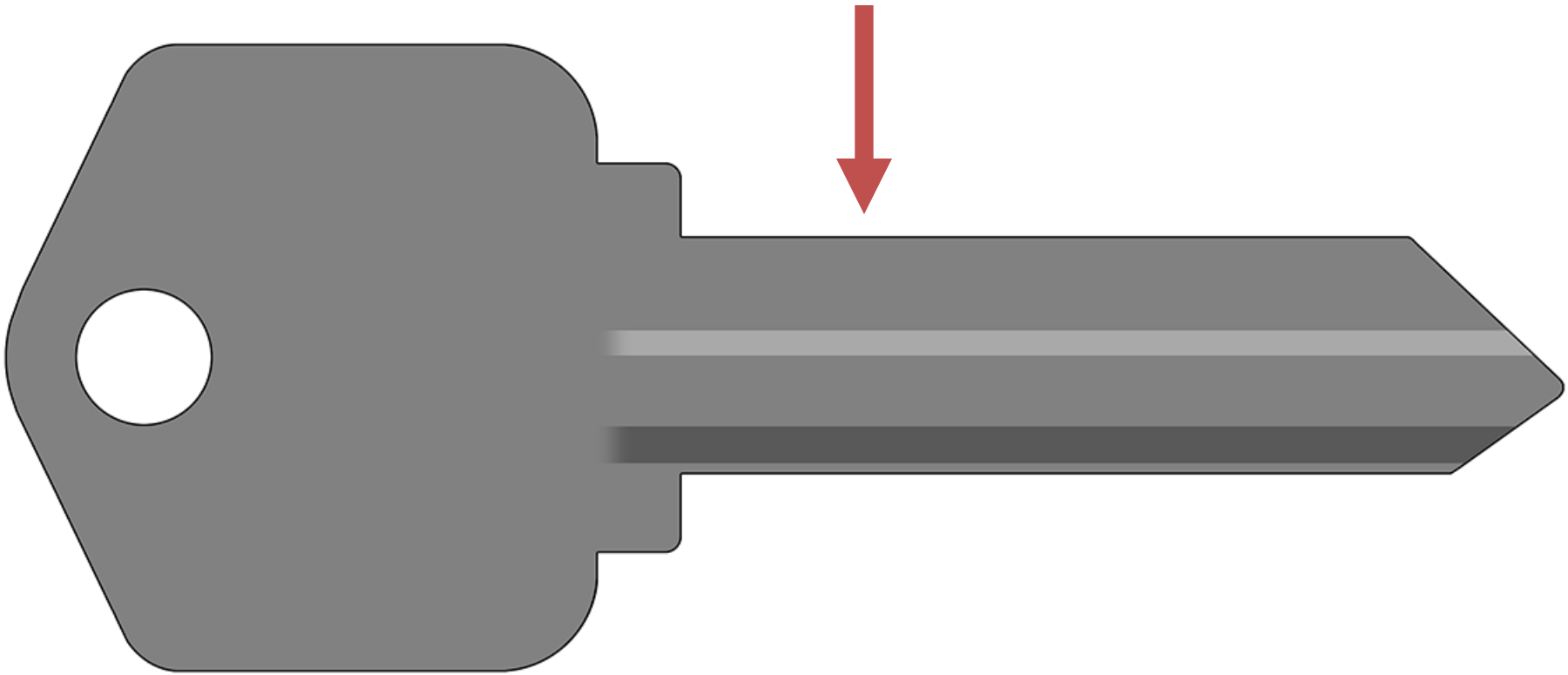
So… Now Three Chambers Remain



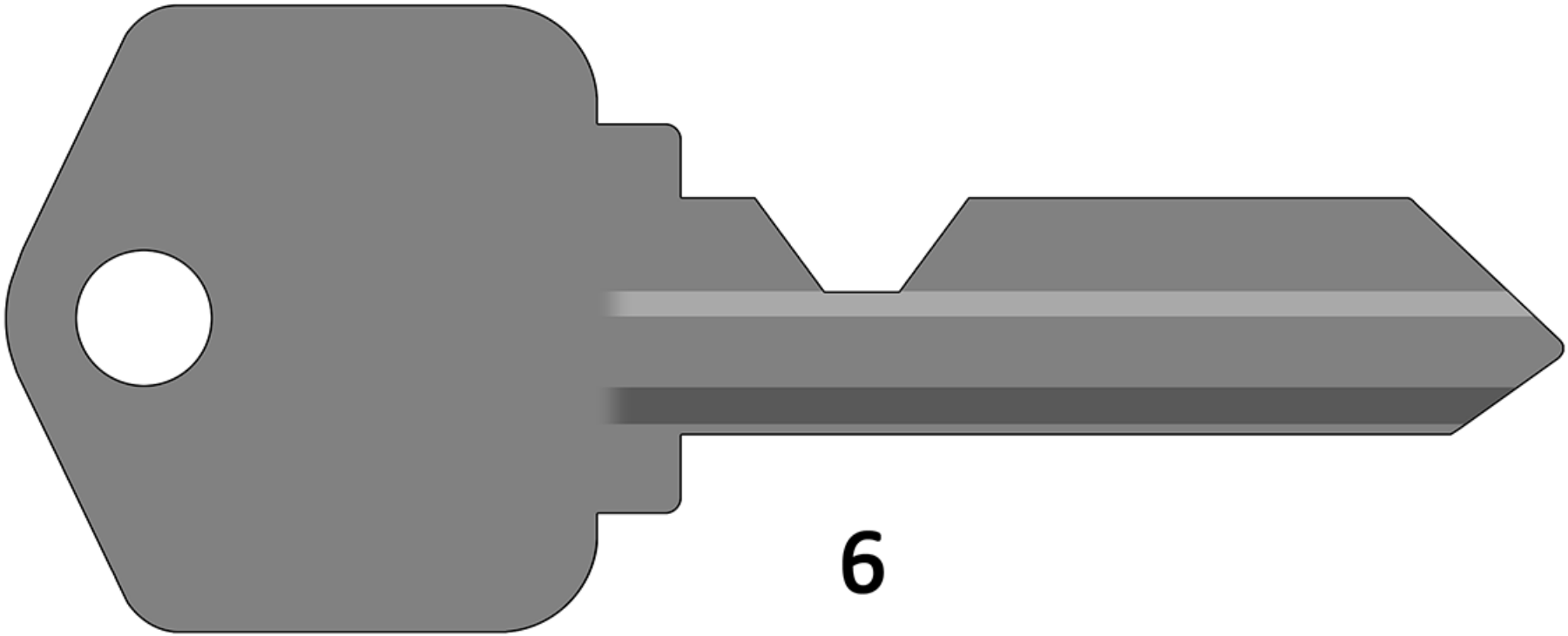
Let's Prepare a Third Exploring



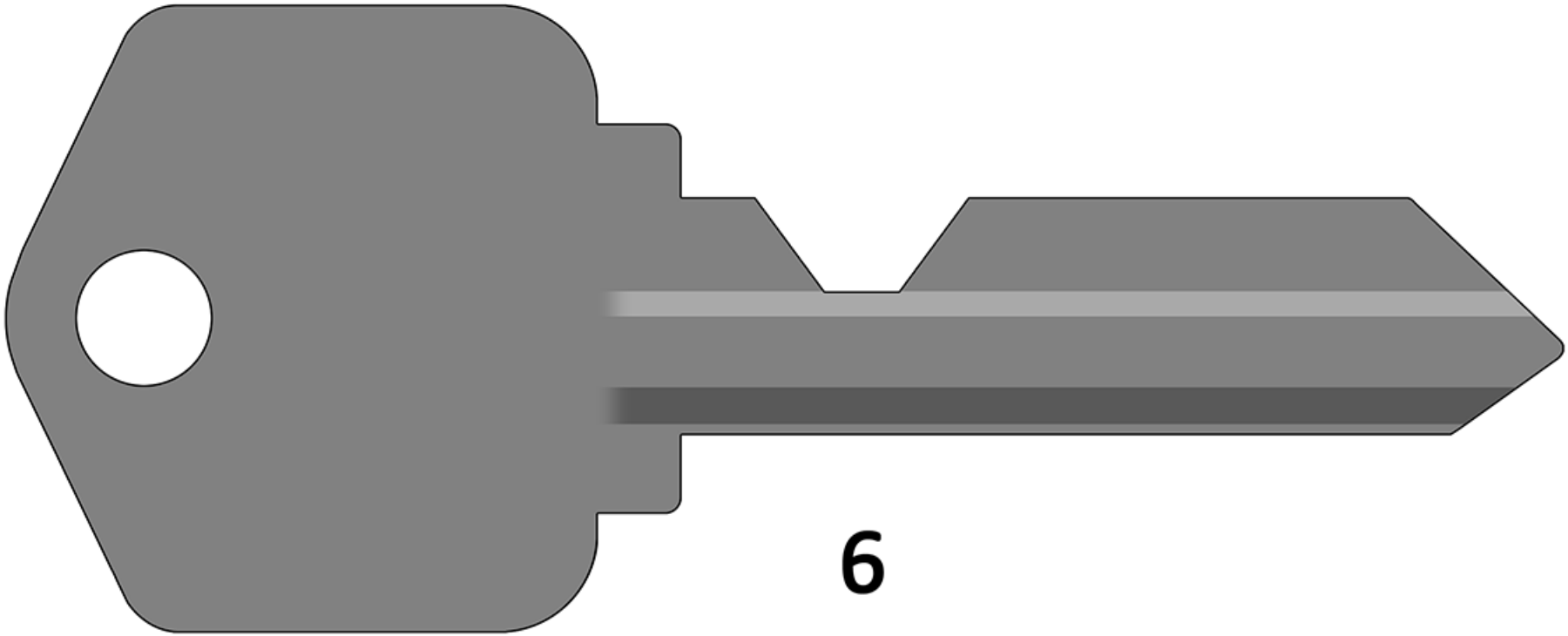
What Cut Will be in Position



A #6 Depth, The Mastering Depth

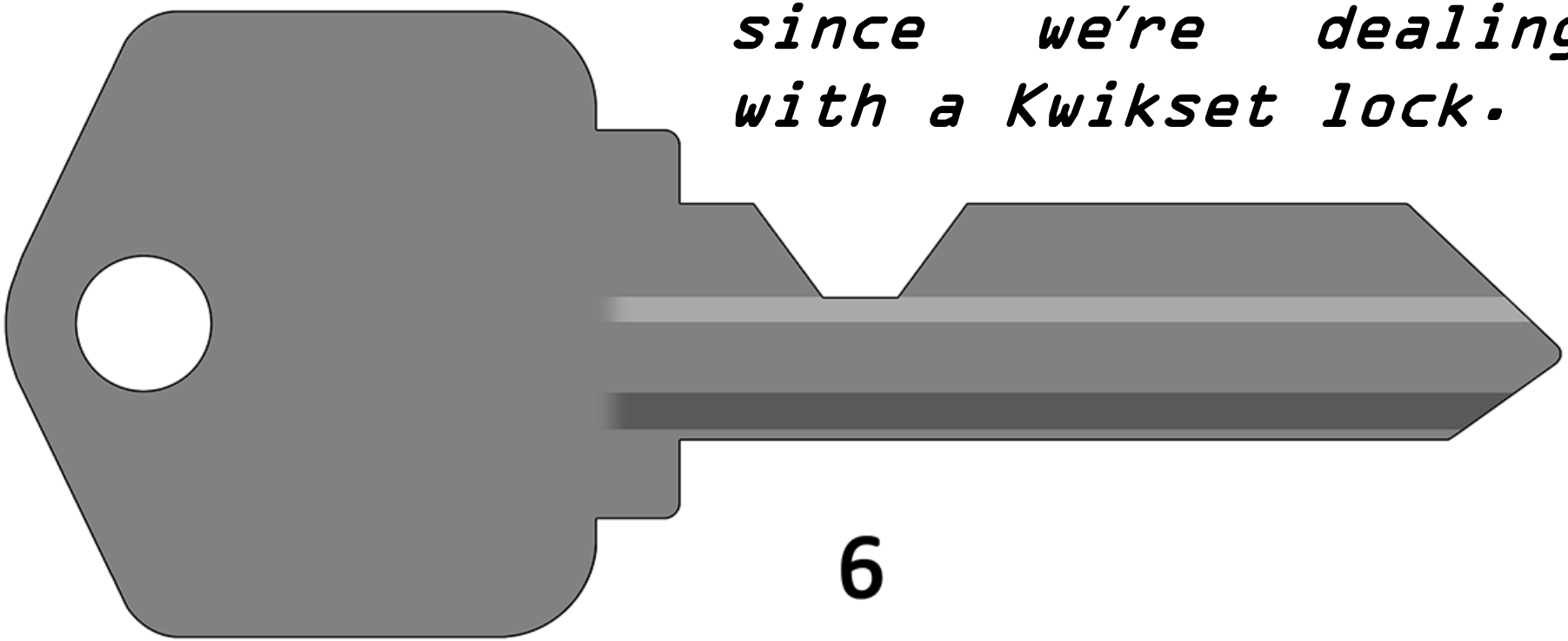


(By the Way… Is This a Valid

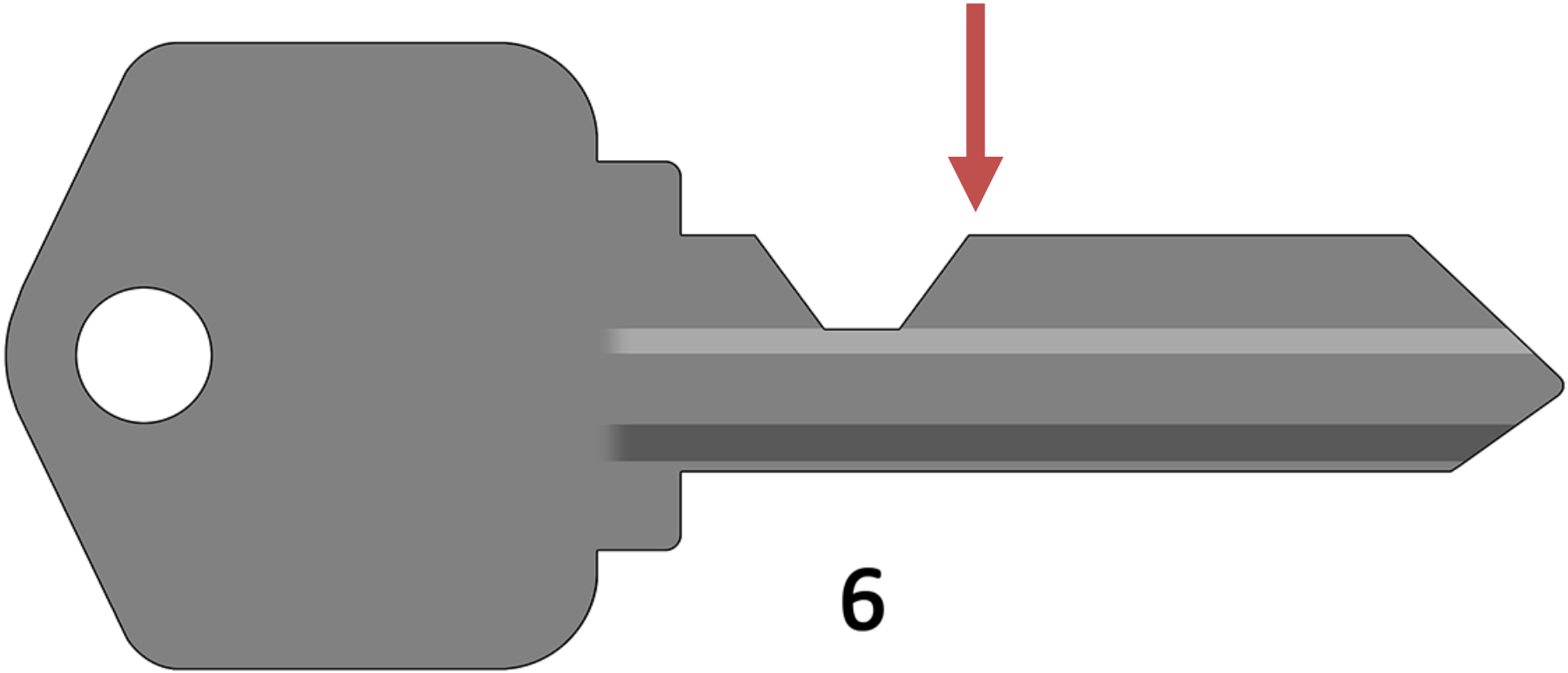


(By the Way… Is This a Valid

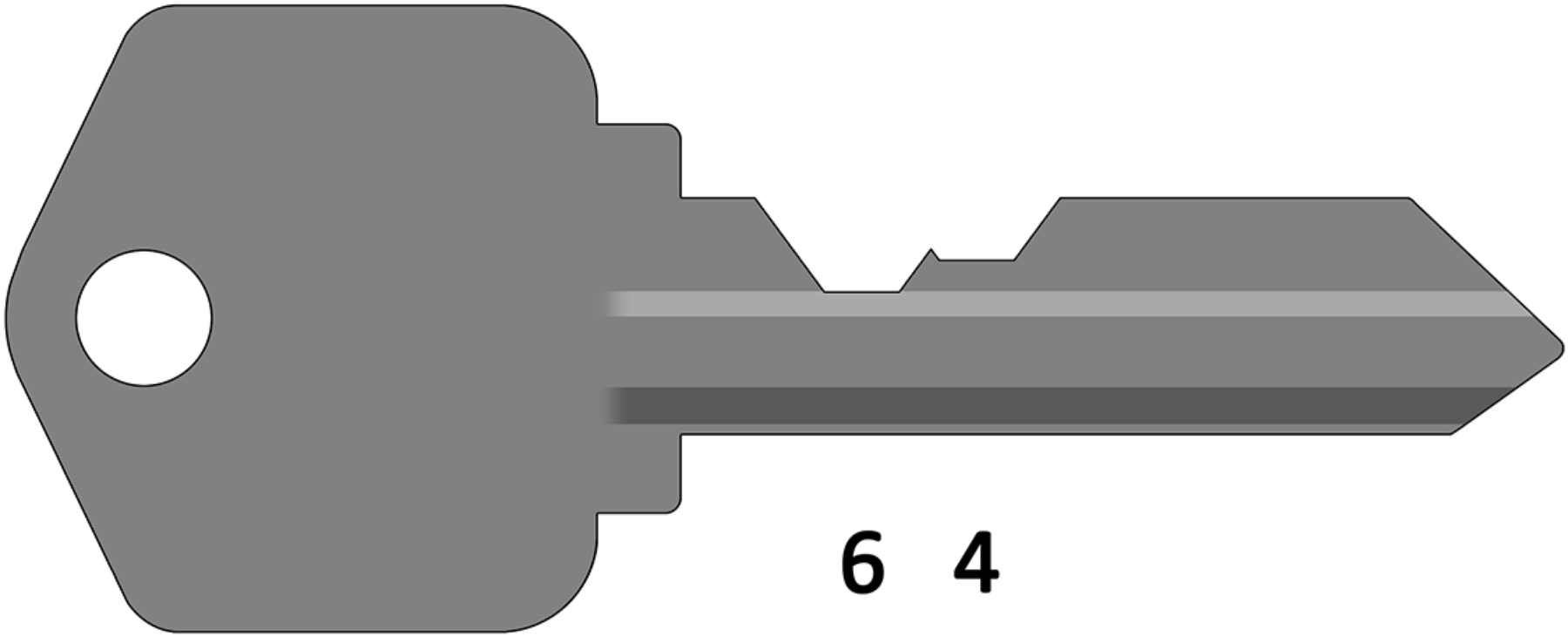
ANSWER - No. This would violate MACS since we're dealing with a Kwikset lock.



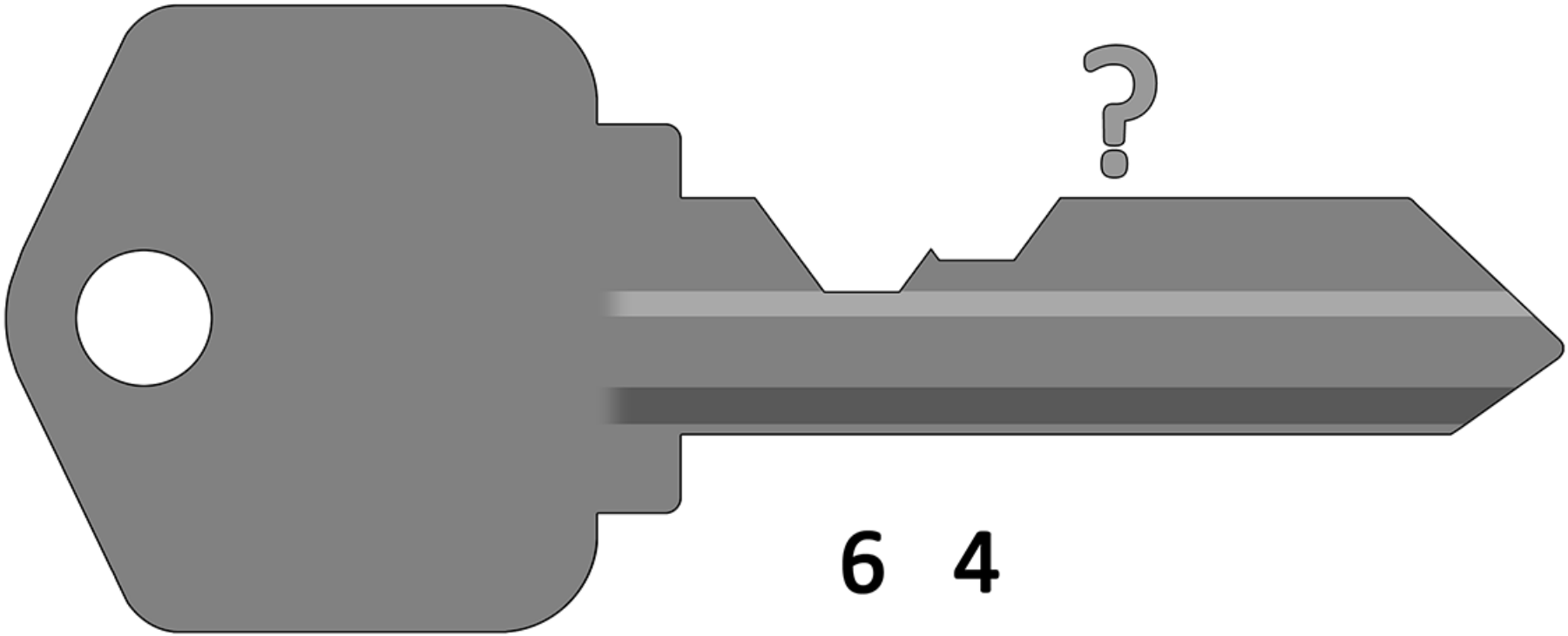
What Cut Will be in Position



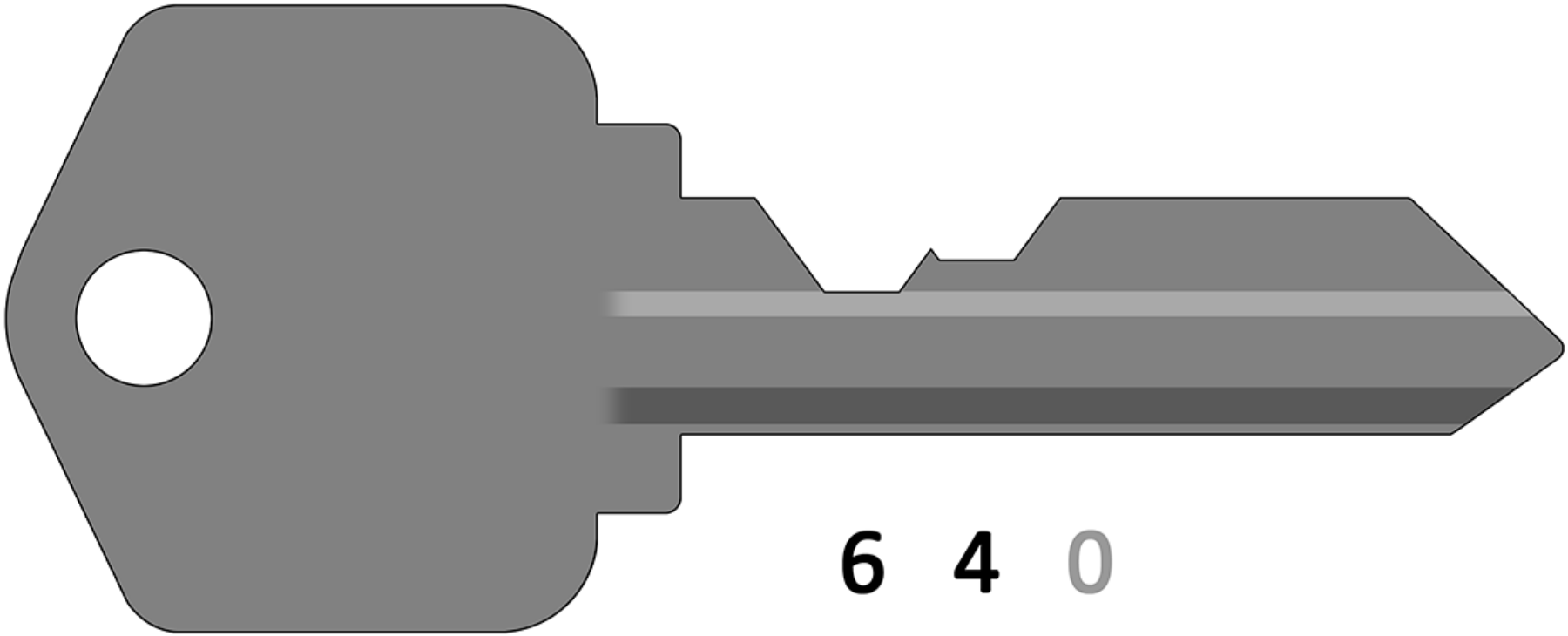
A #4 Depth Will be There… The



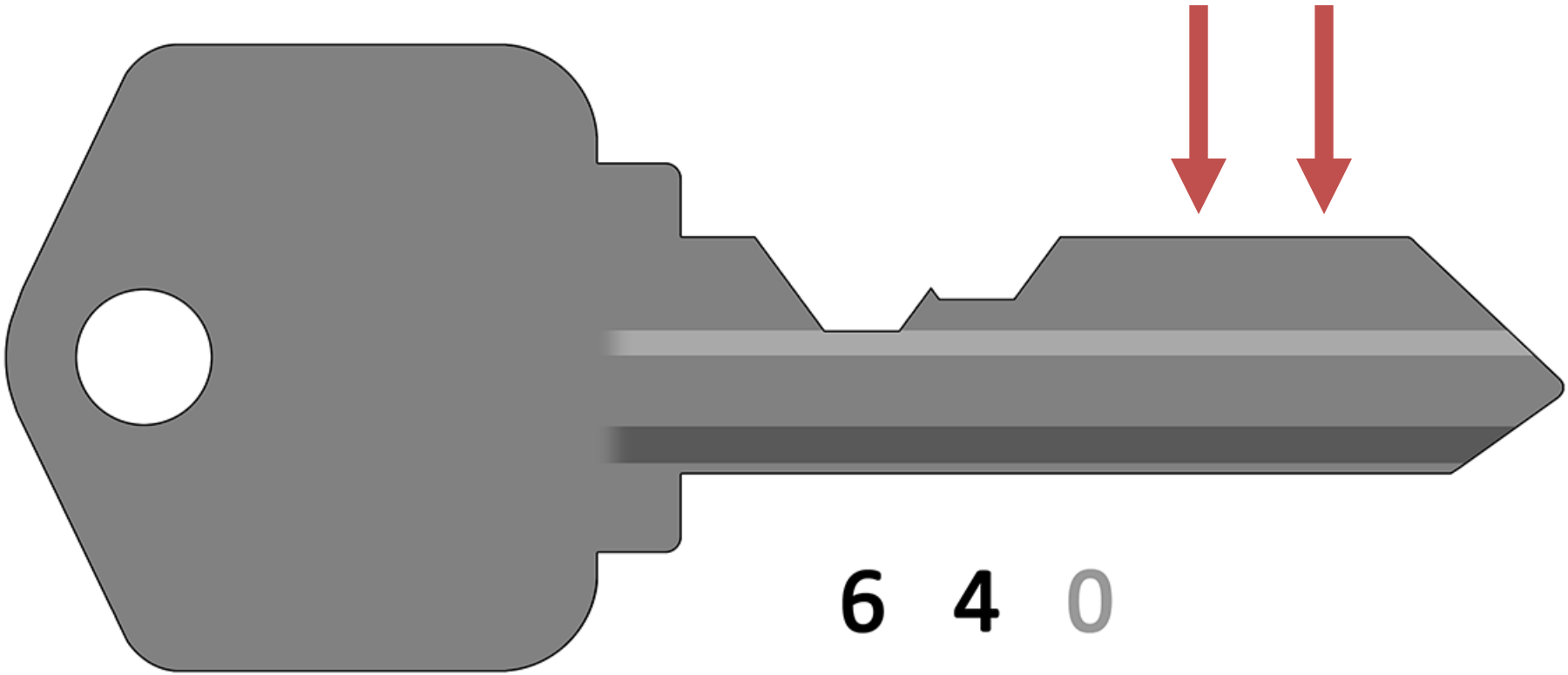
What Will We Do in Position



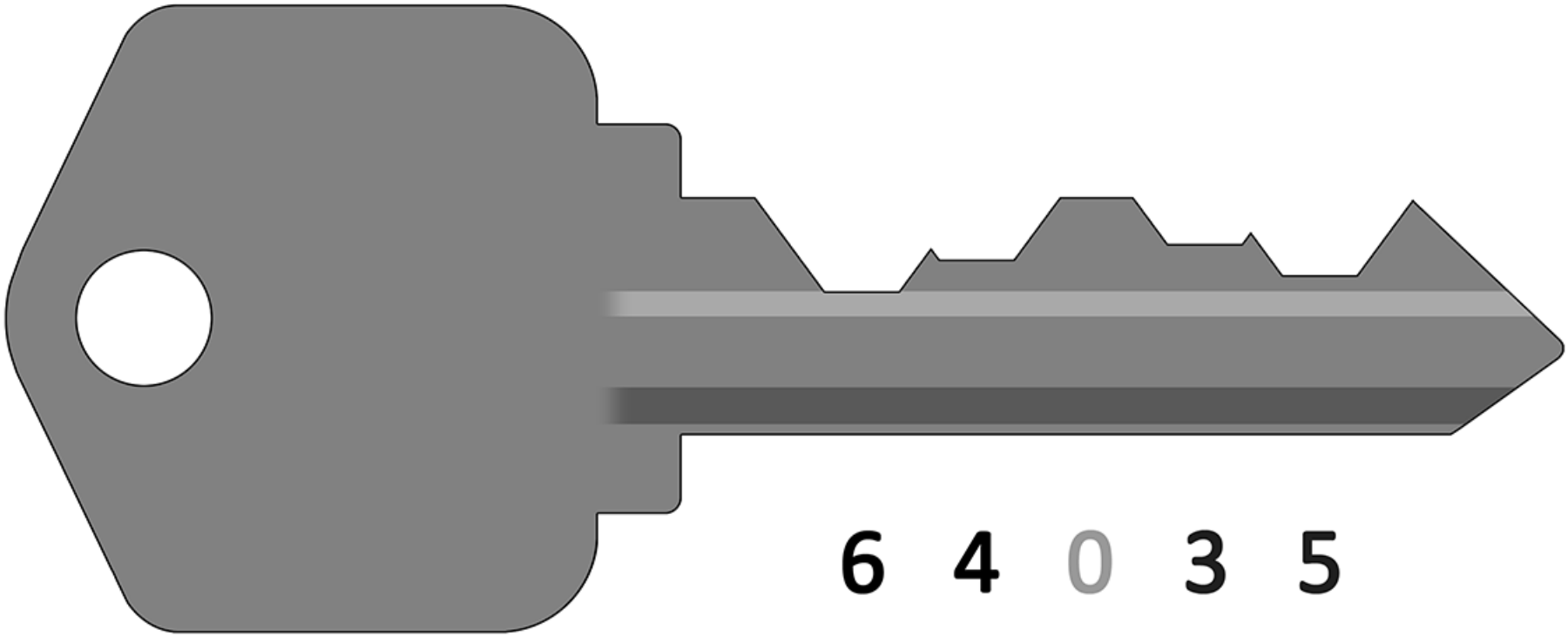
Leave Position Three Blank For



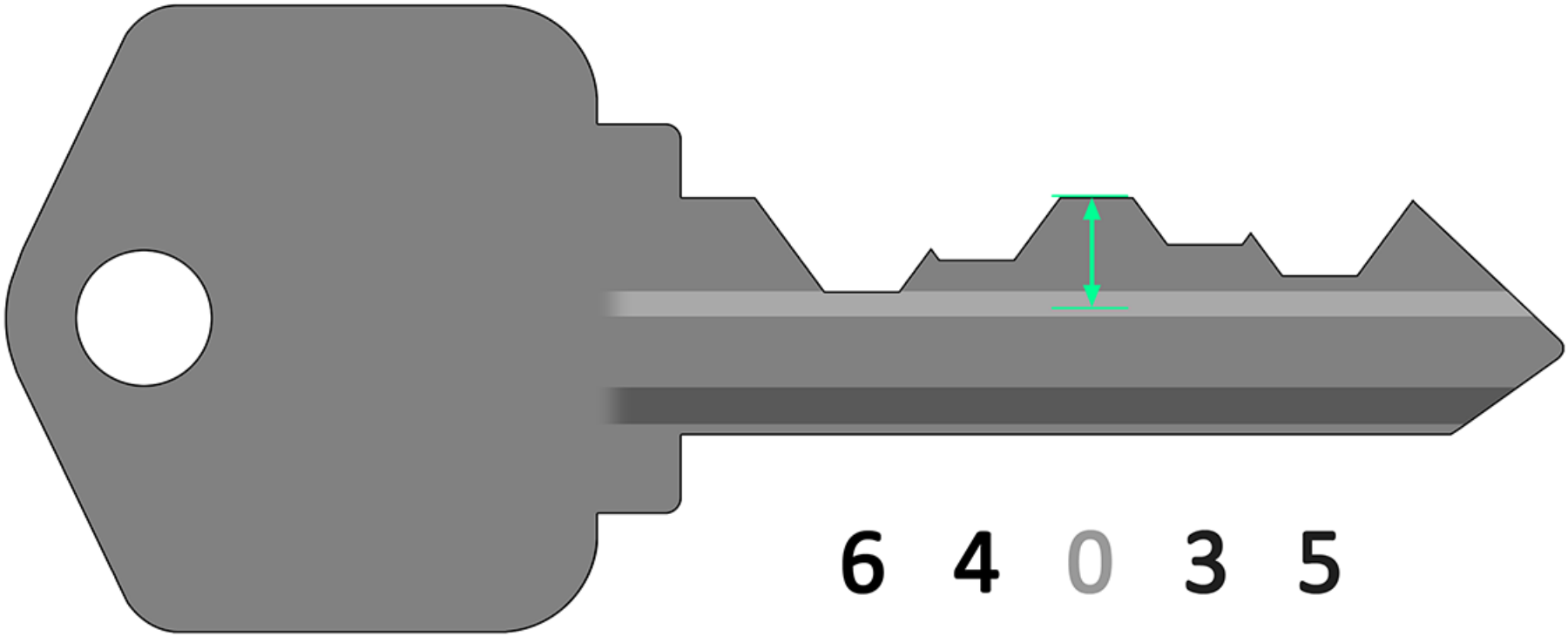
And For the Rest of the Key?



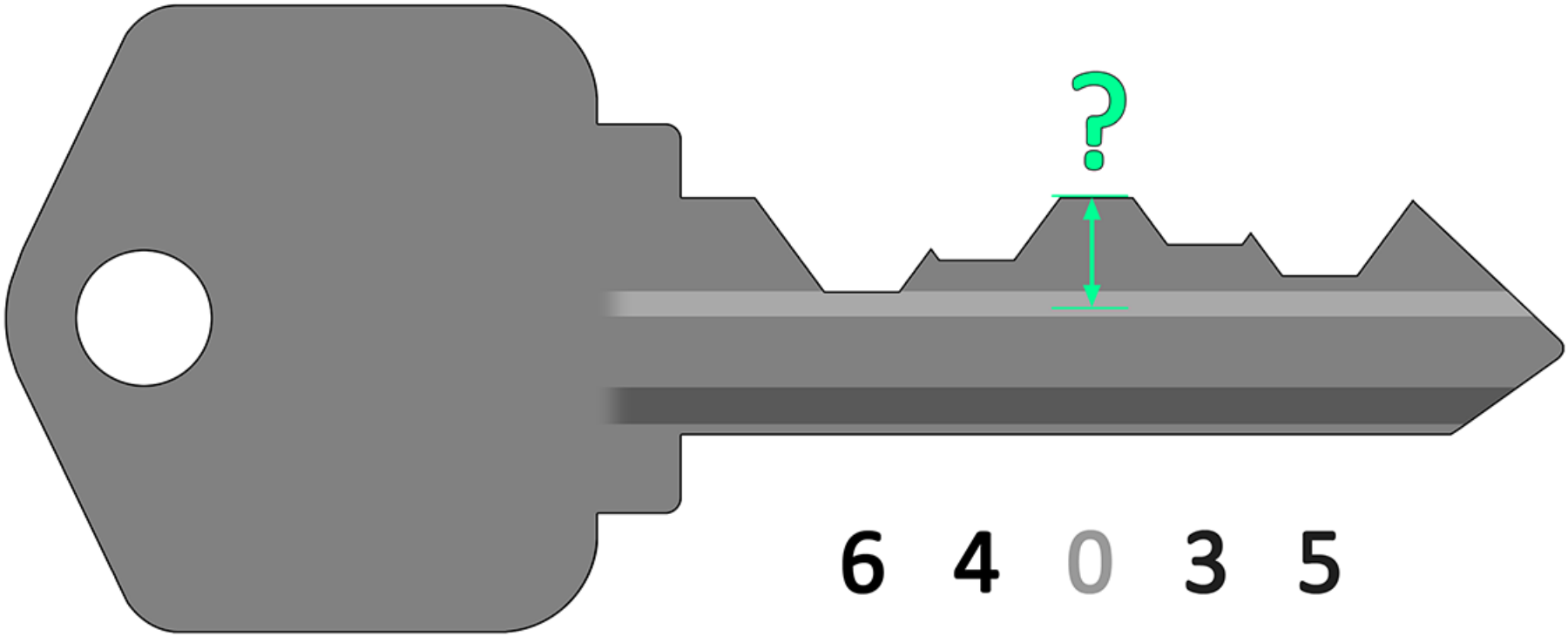
Finish Off with Depths Known



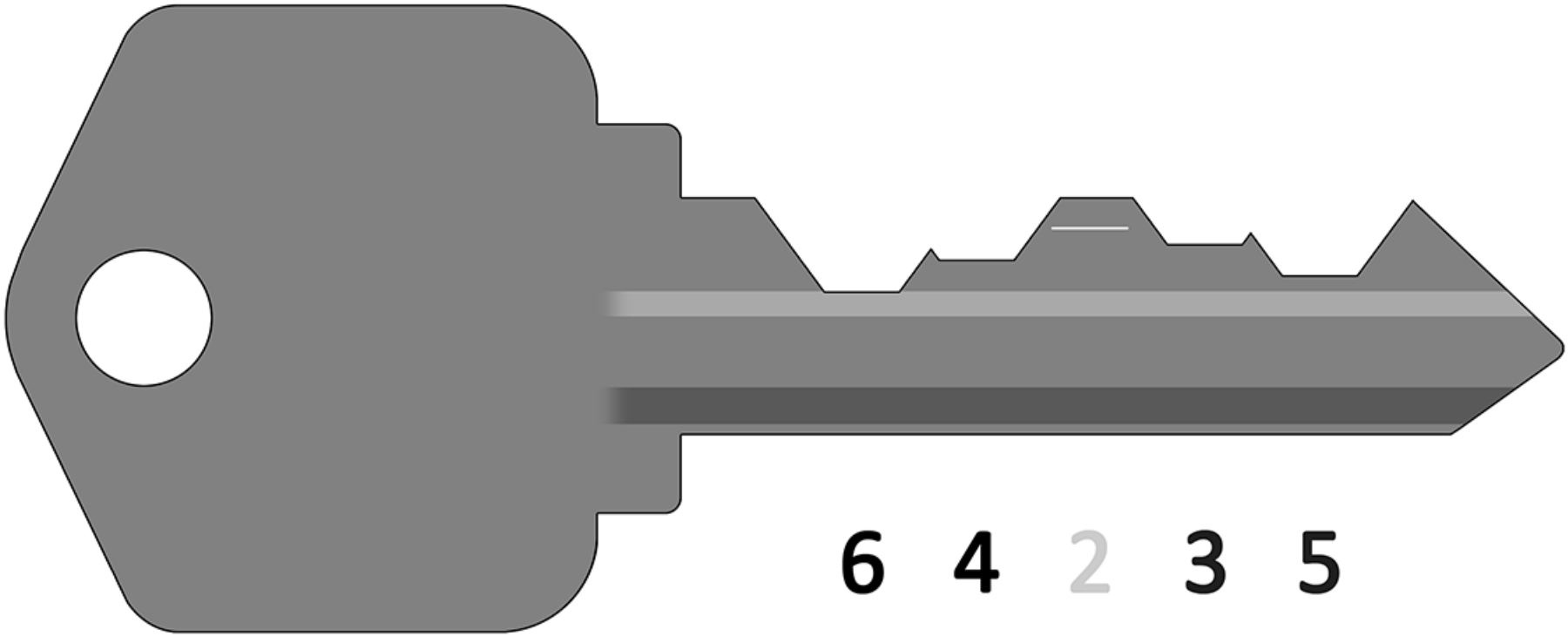
So, Now it's Time to Explore…



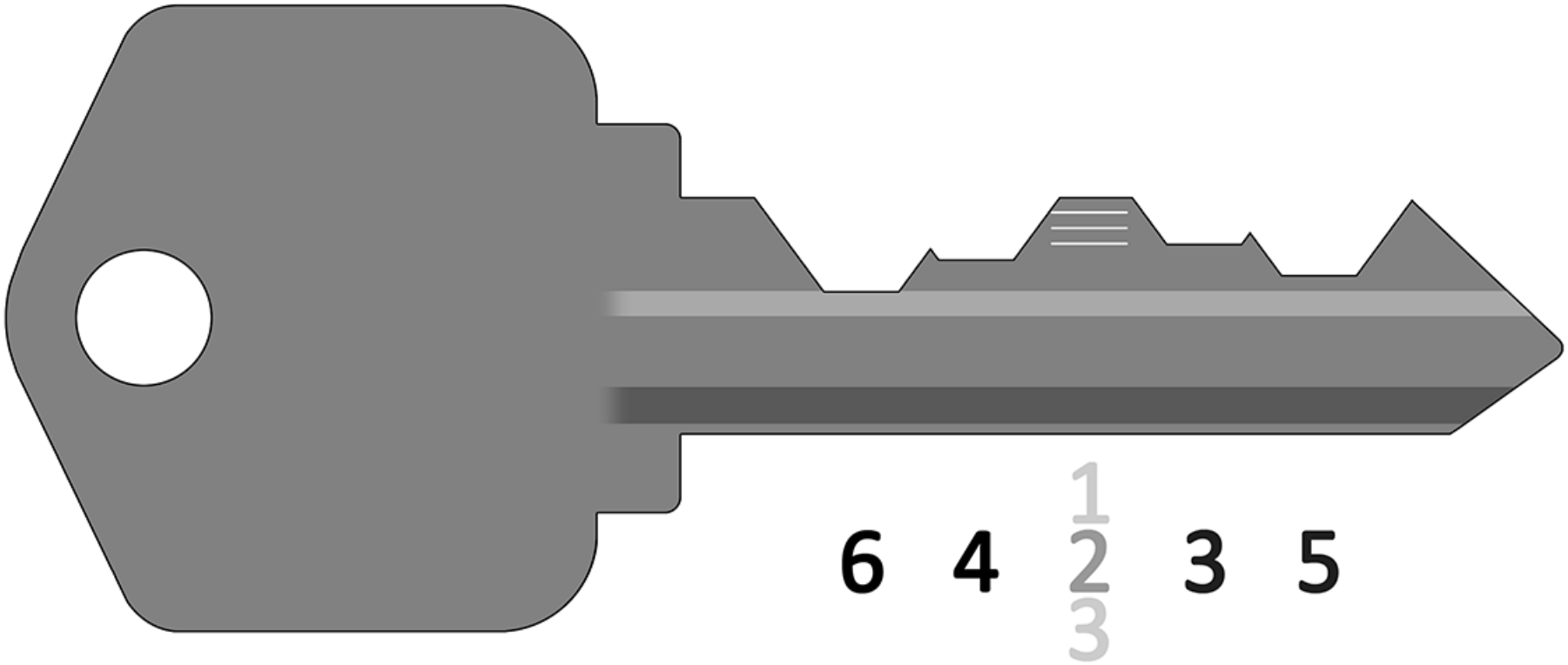
So, Now it's Time to Explore… Or



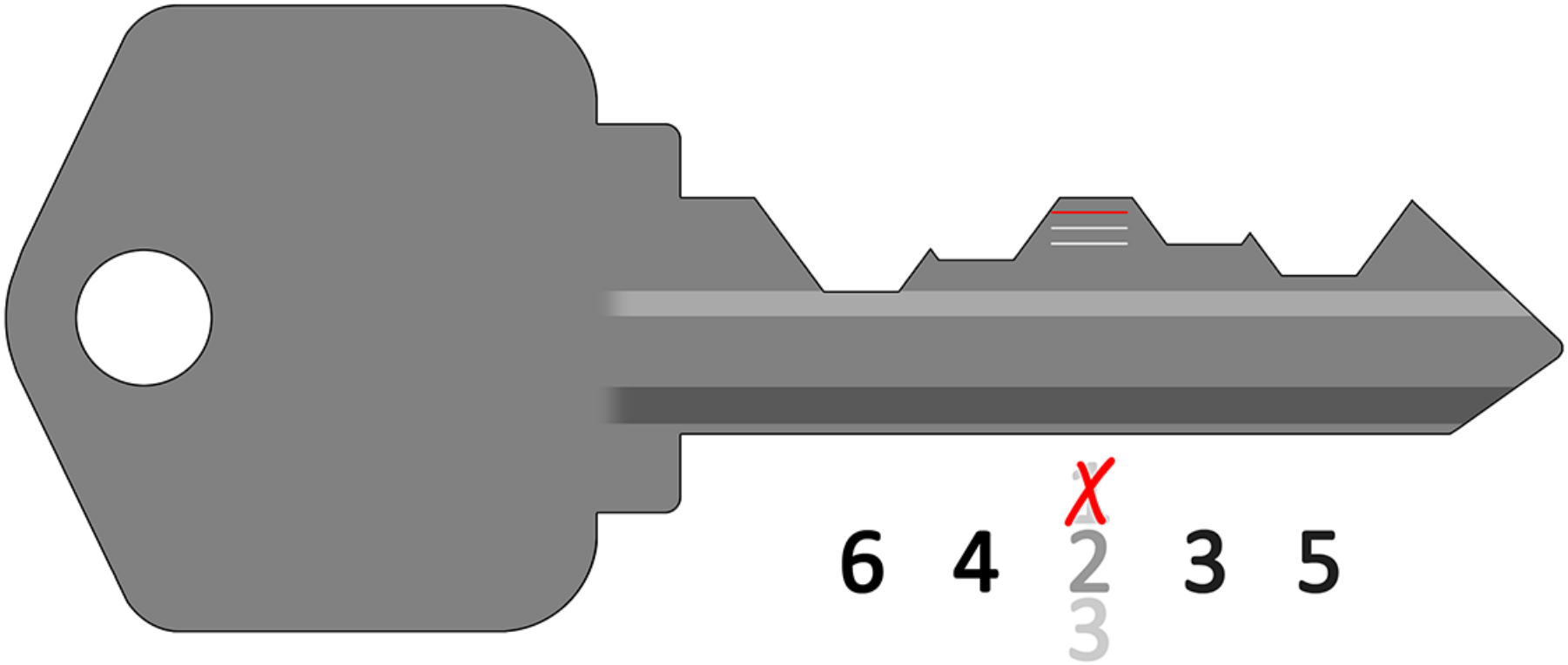
Remember the Change Key's Known



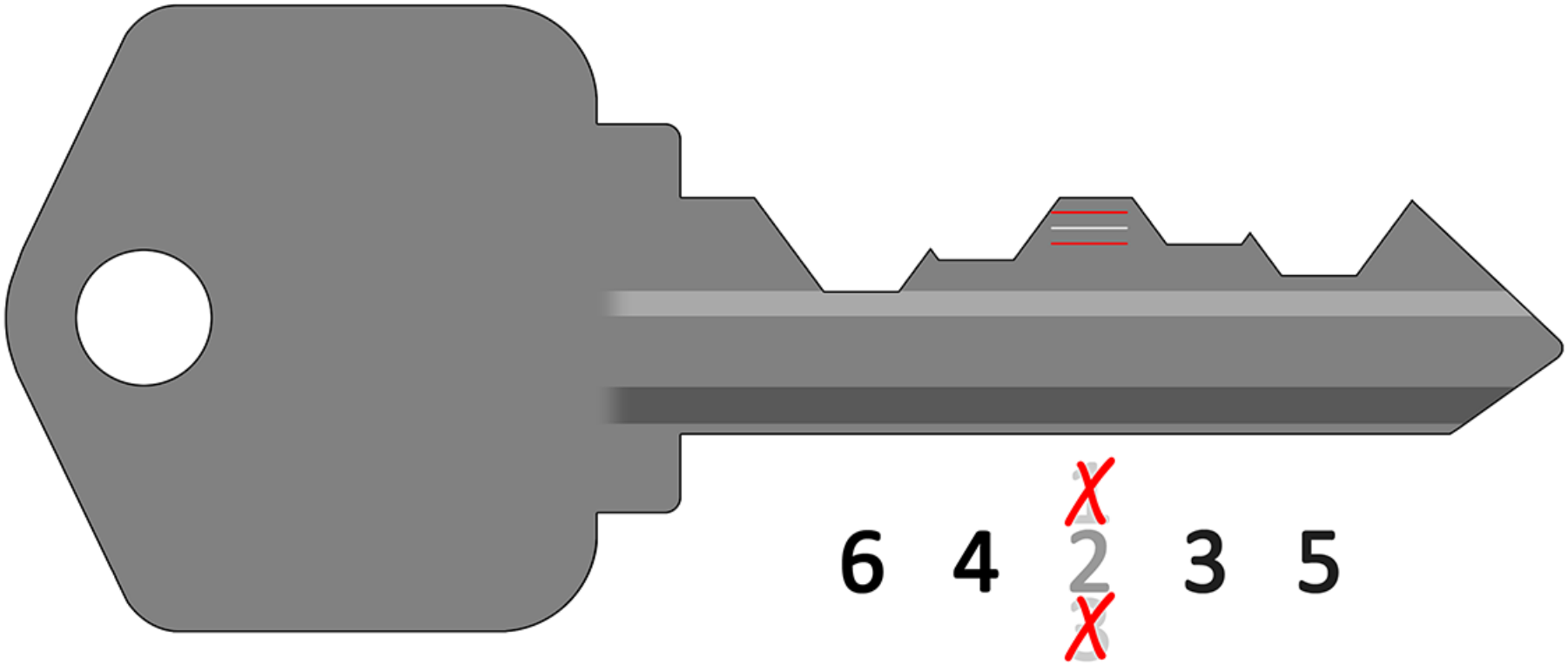
So What About #1 and #3 Depths?



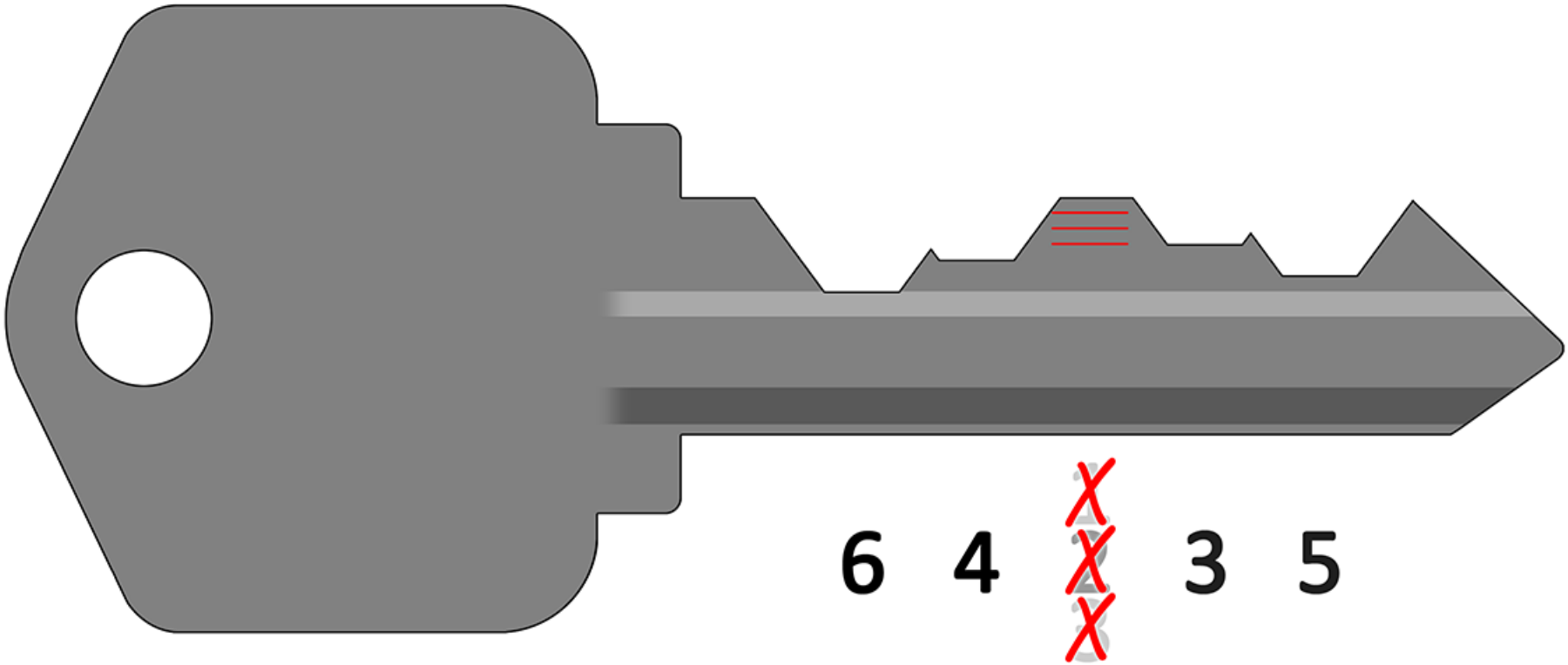
A #1 Depth Would be Unwise



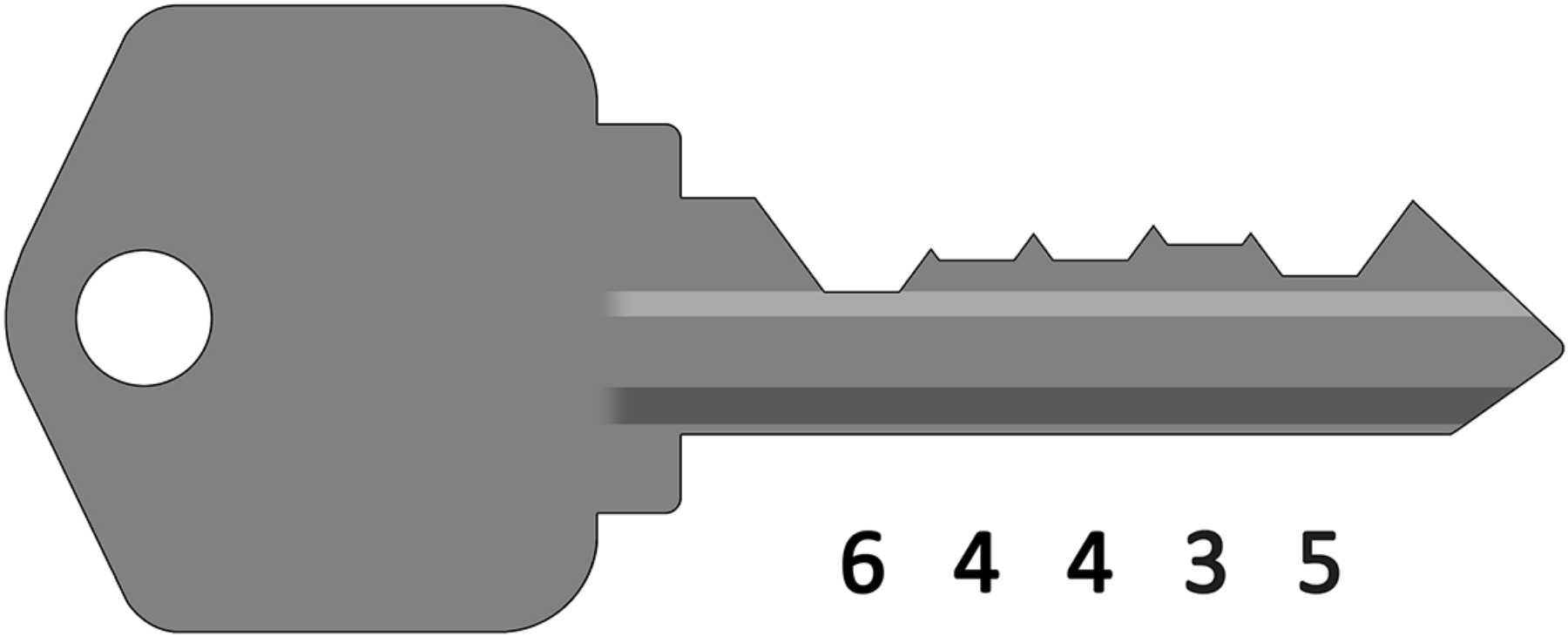
A #3 Depth Would be Unwise, Too



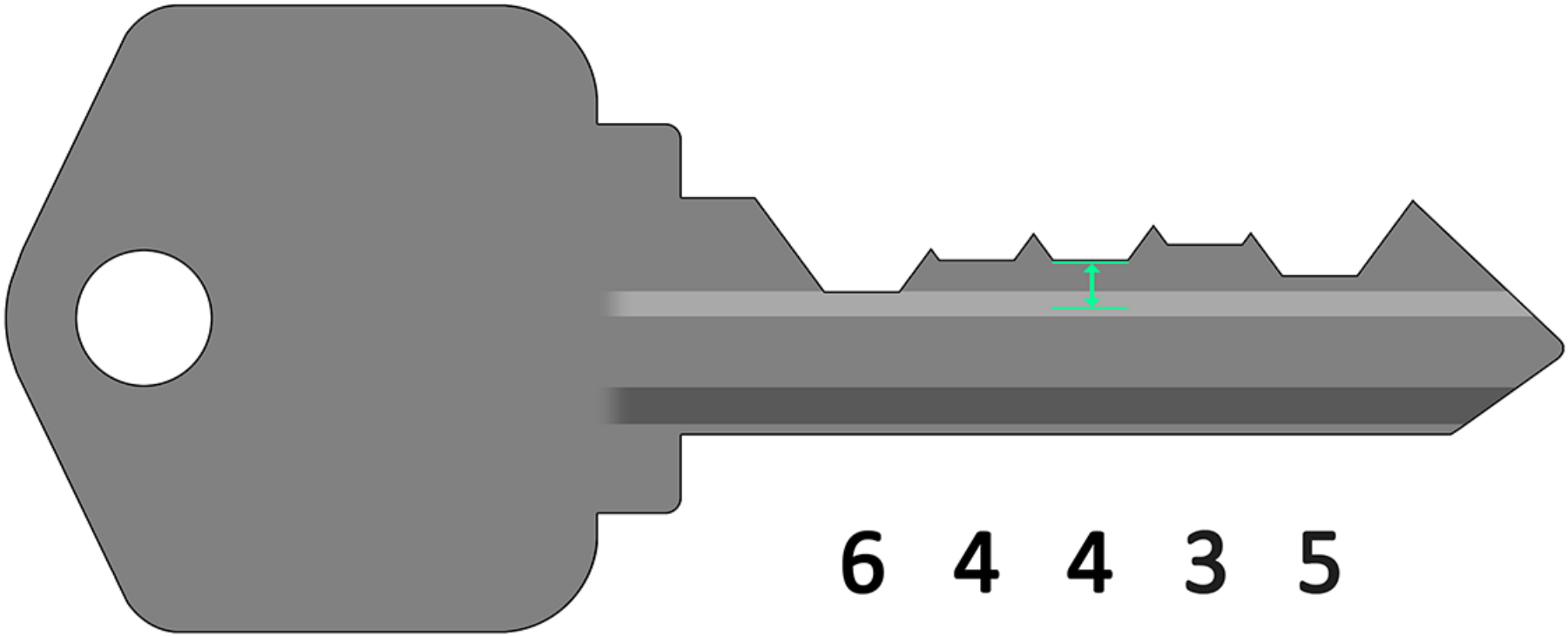
And #2 Depth Was Already Known,



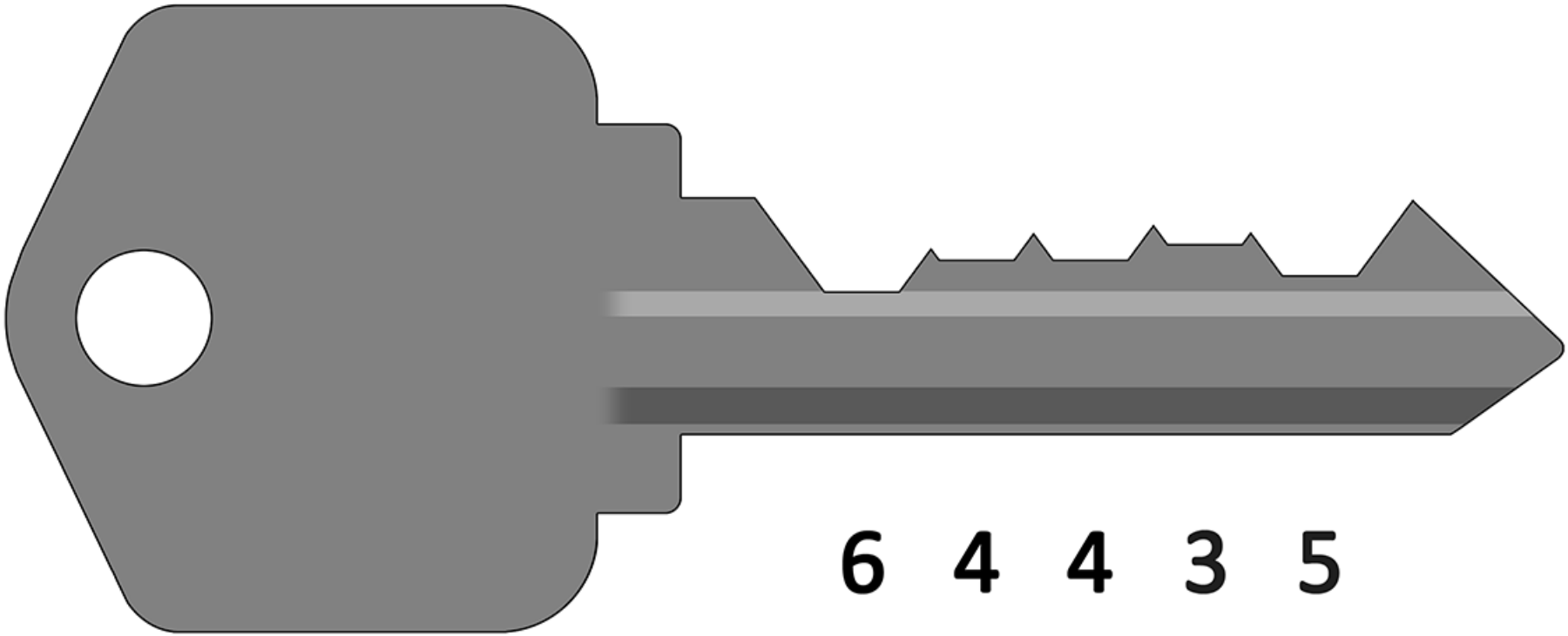
Thus, #4 Depth is an Ideal



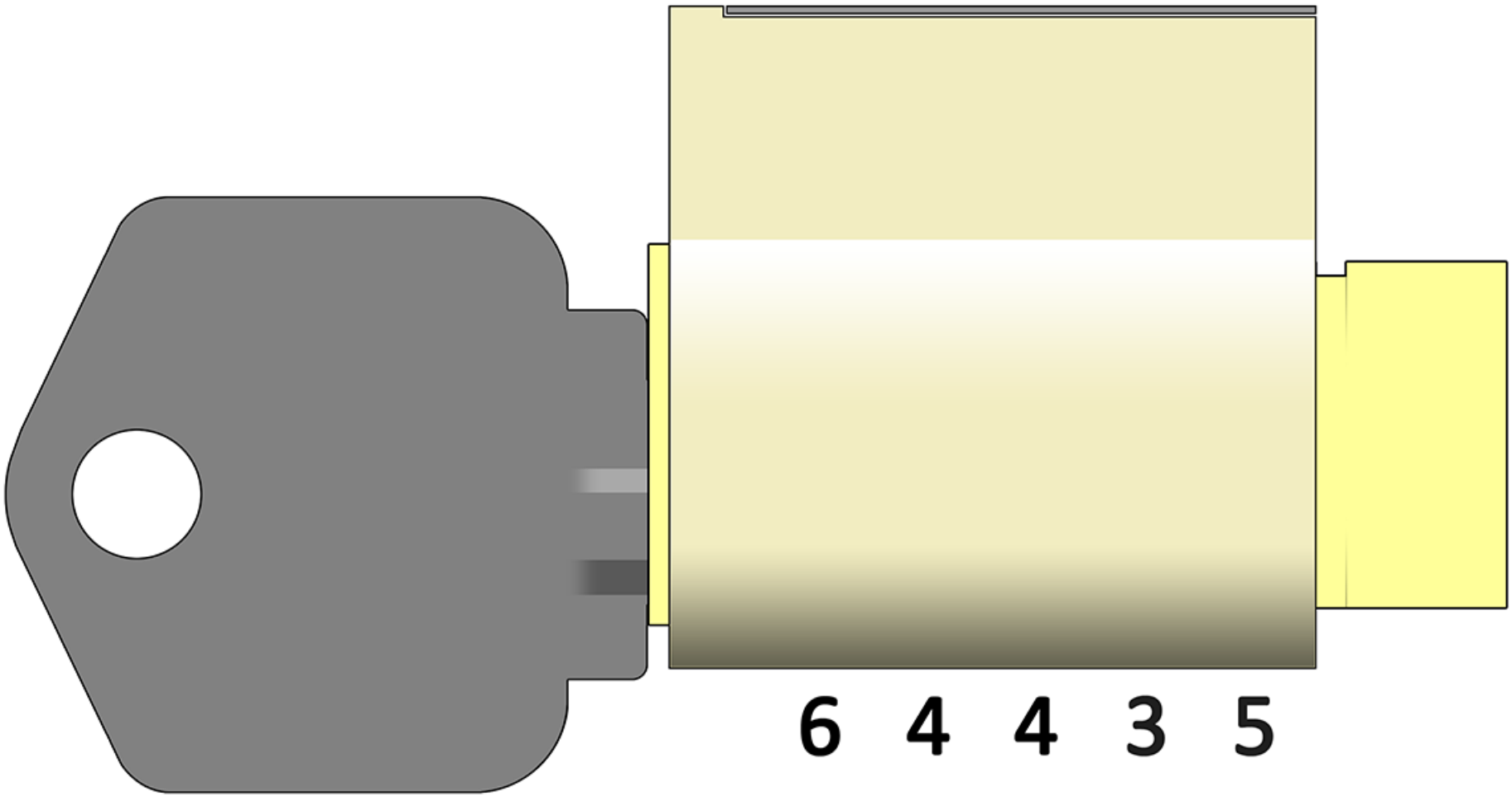
This is a Much More Efficient



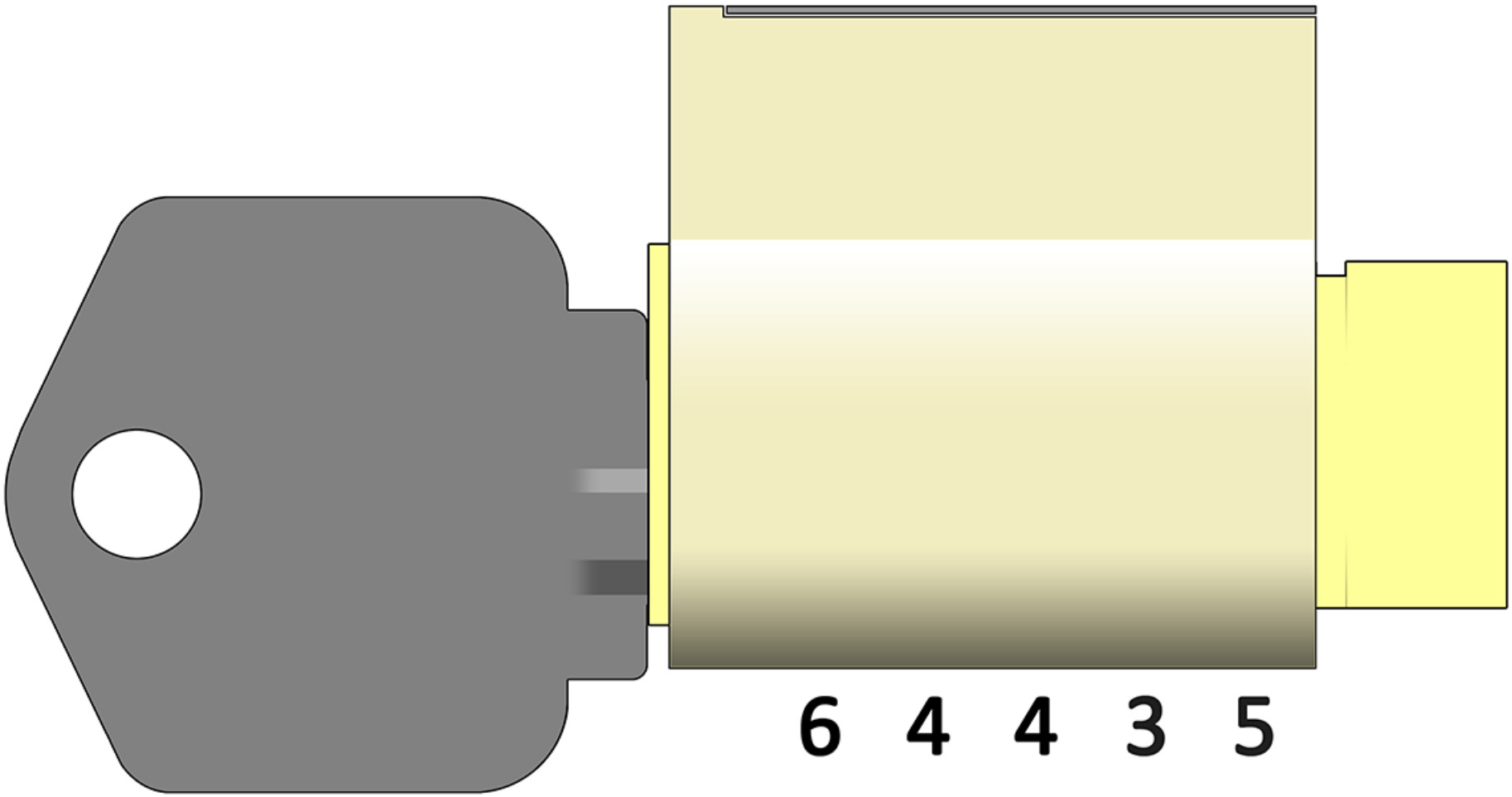
Key 3 is Prepared



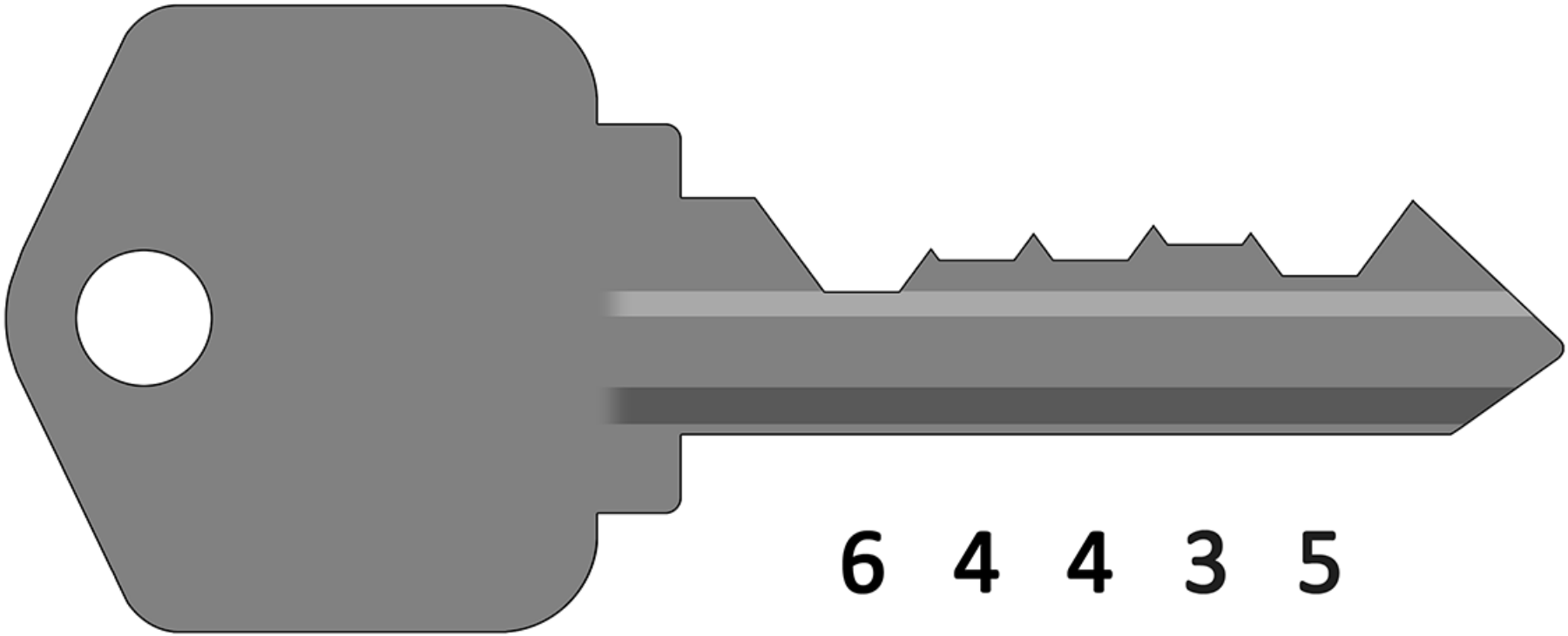
Key 3 is Tried…



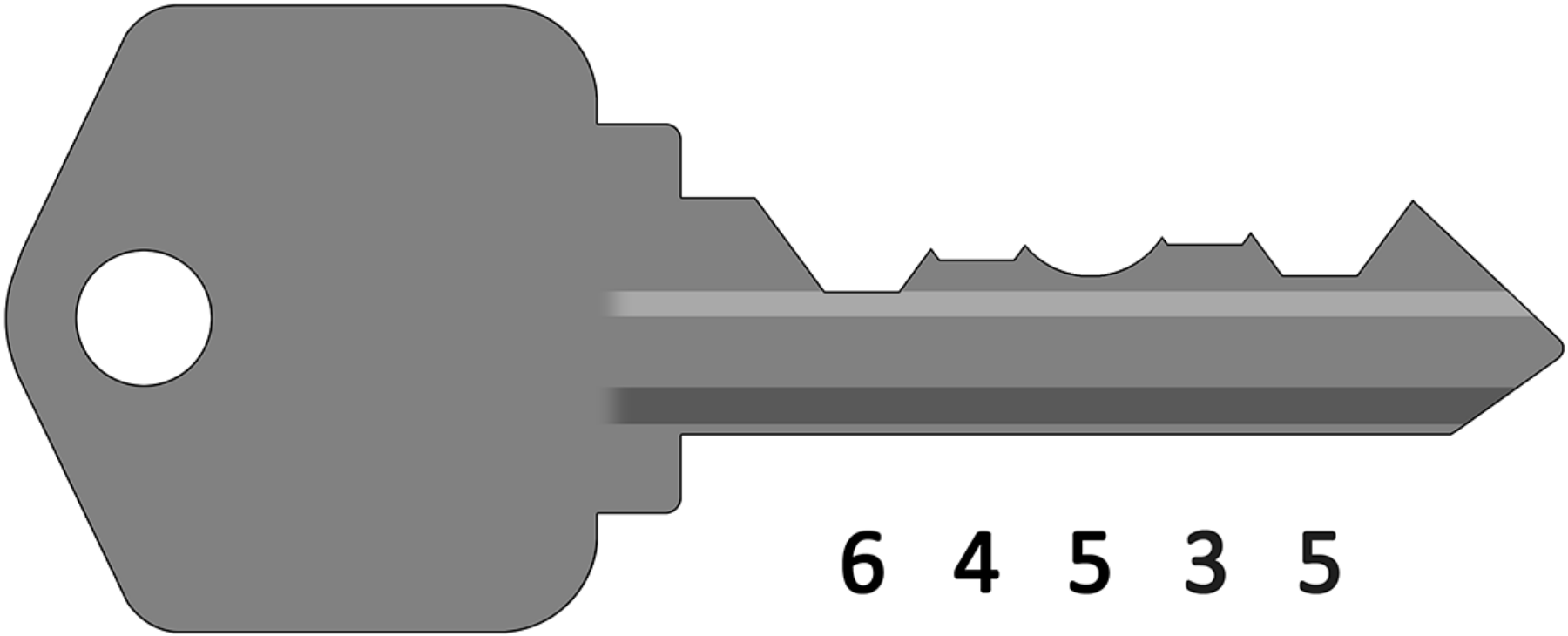
Key 3 is Tried… It Doesn't Turn



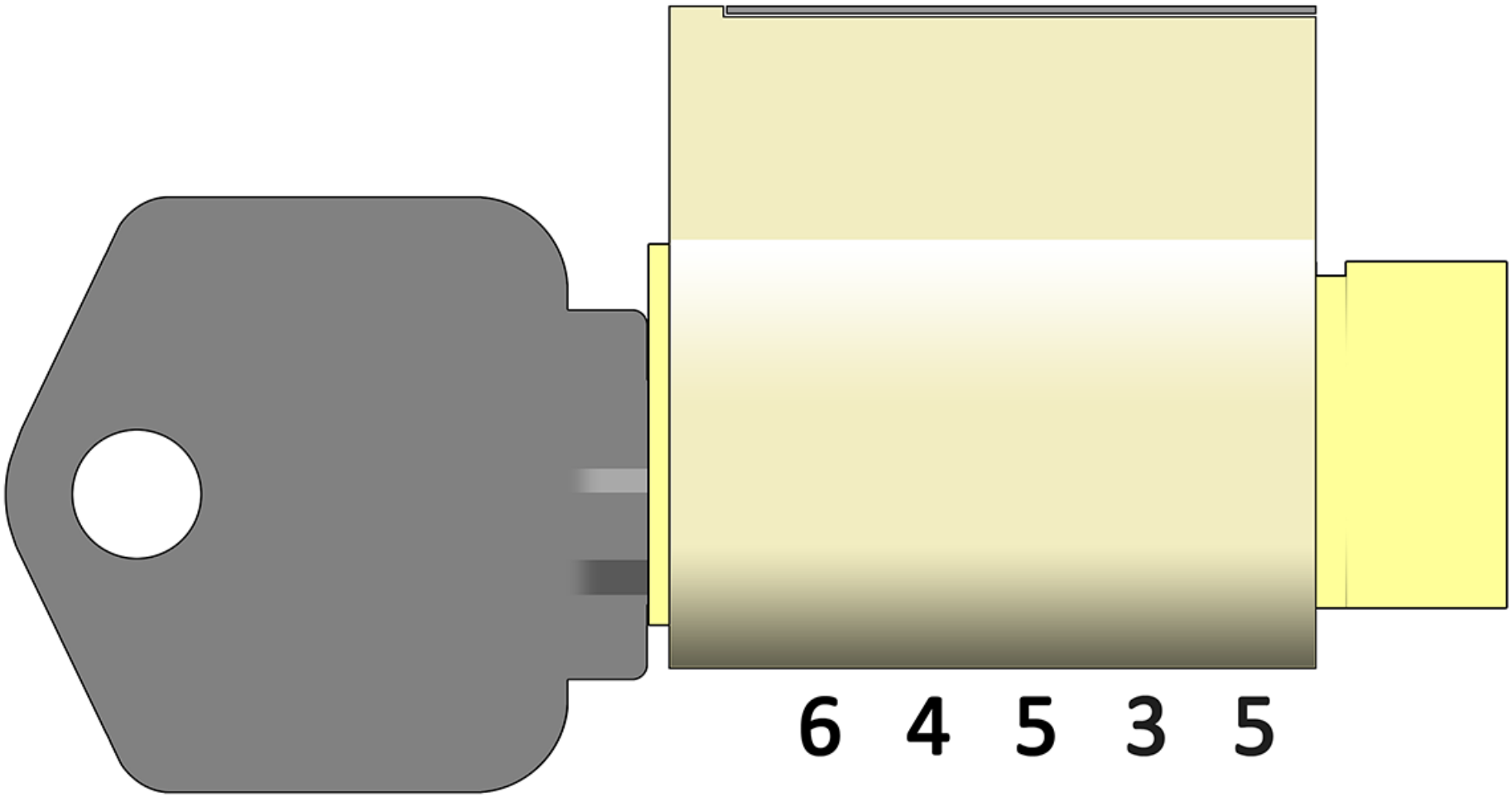
Remove the Key



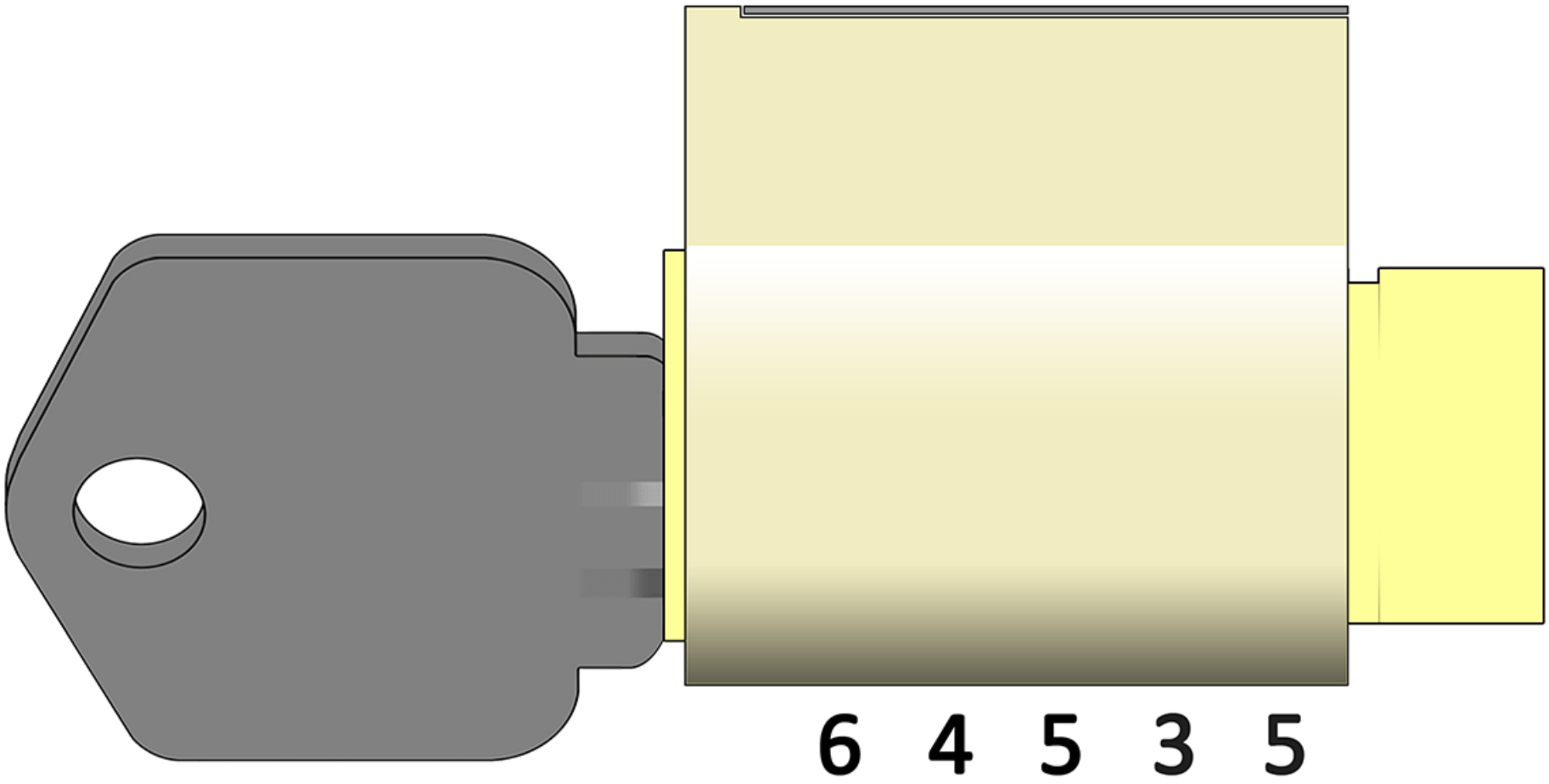
File Down by One Cut Depth



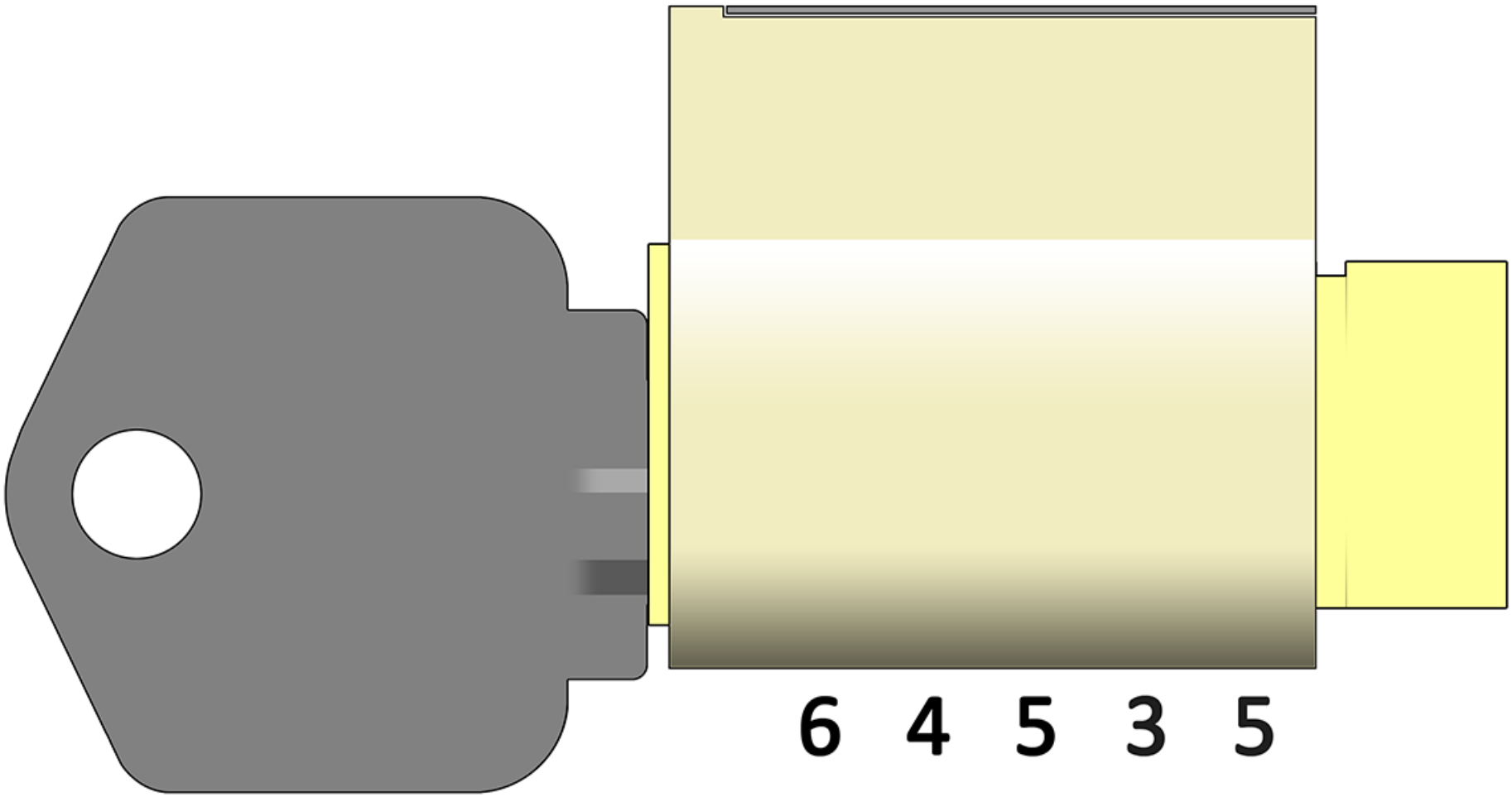
Try the Key…



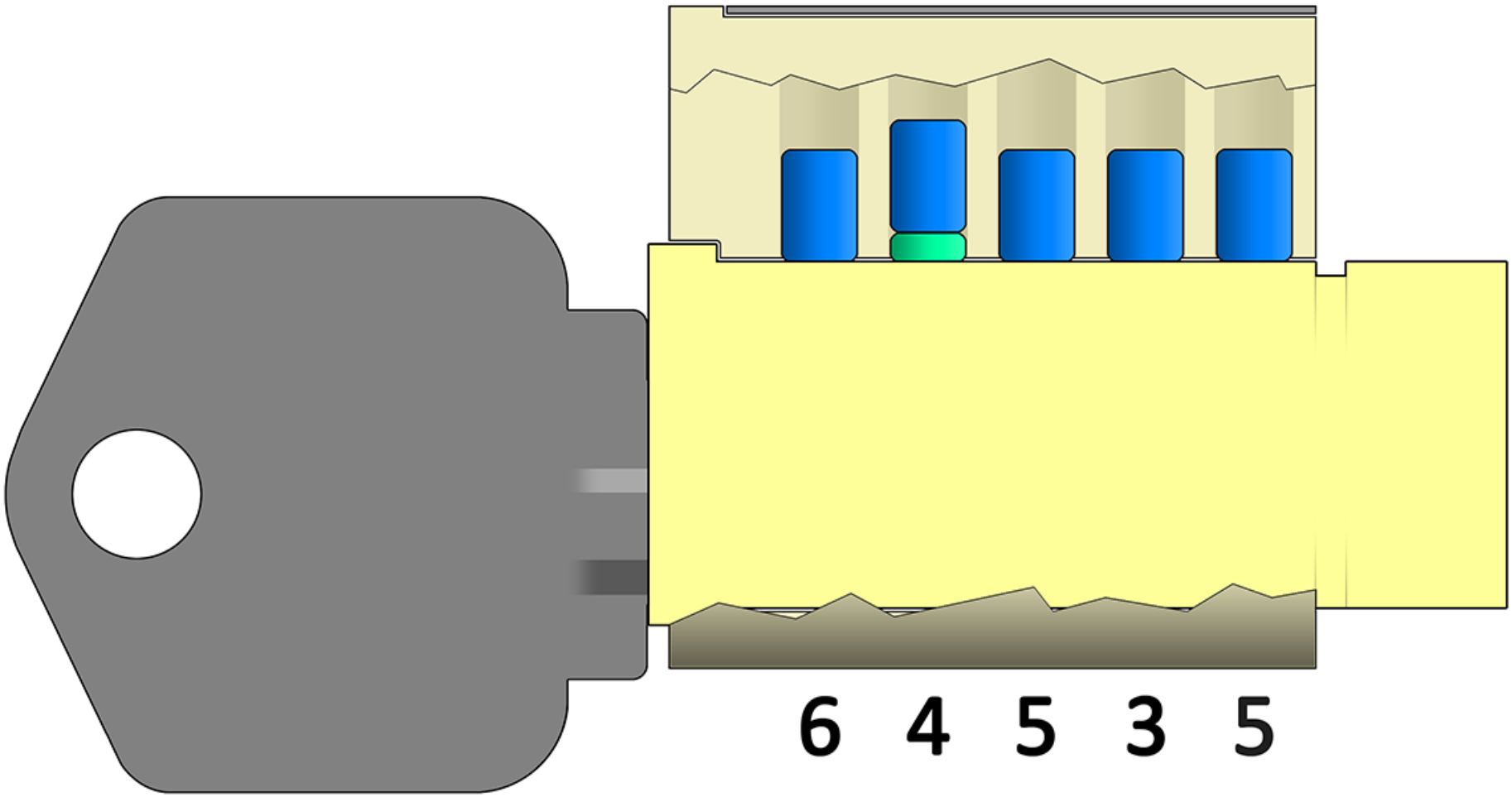
Try the Key… OPEN!



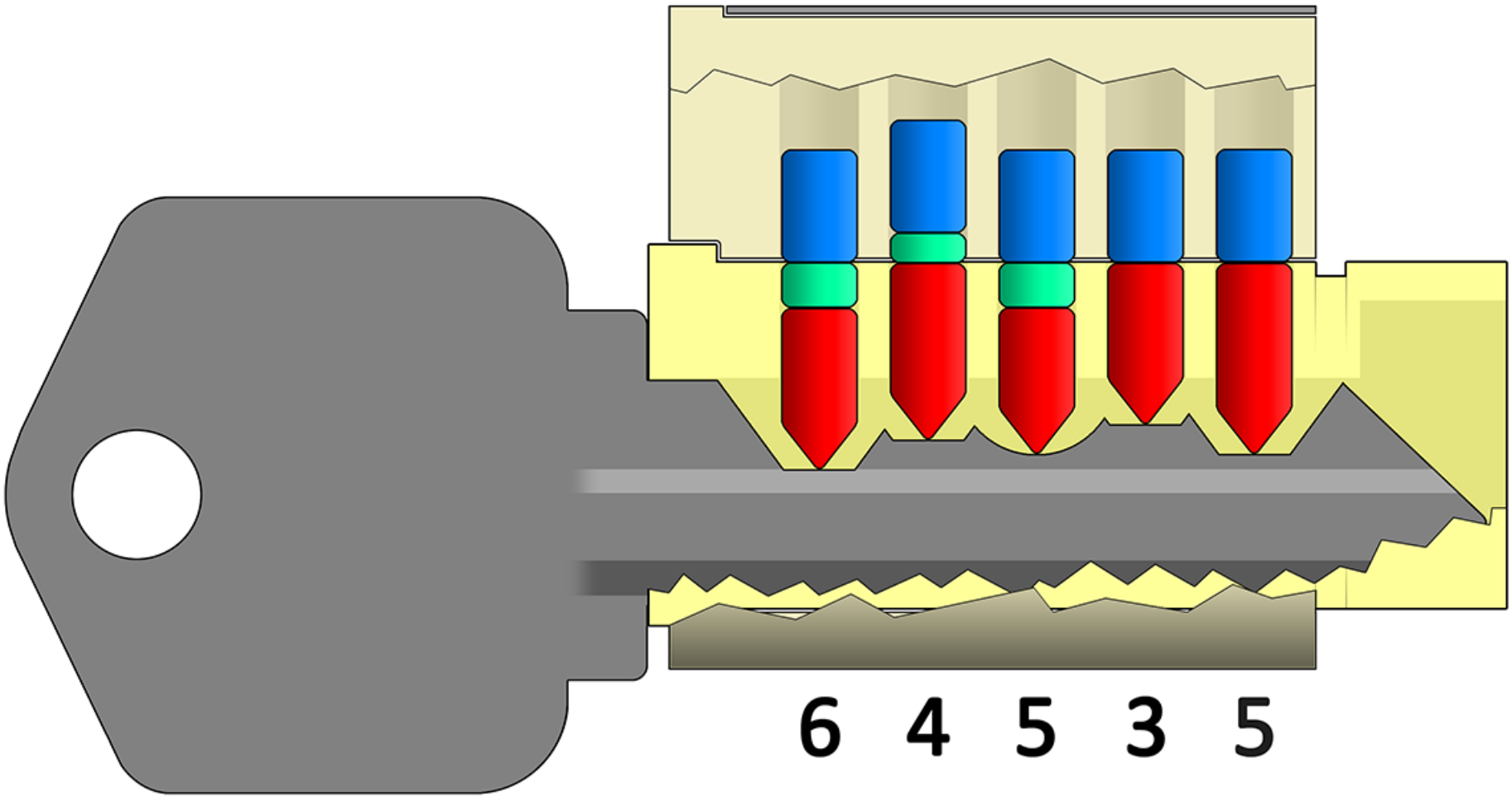
This Tells Us Quite a Lot



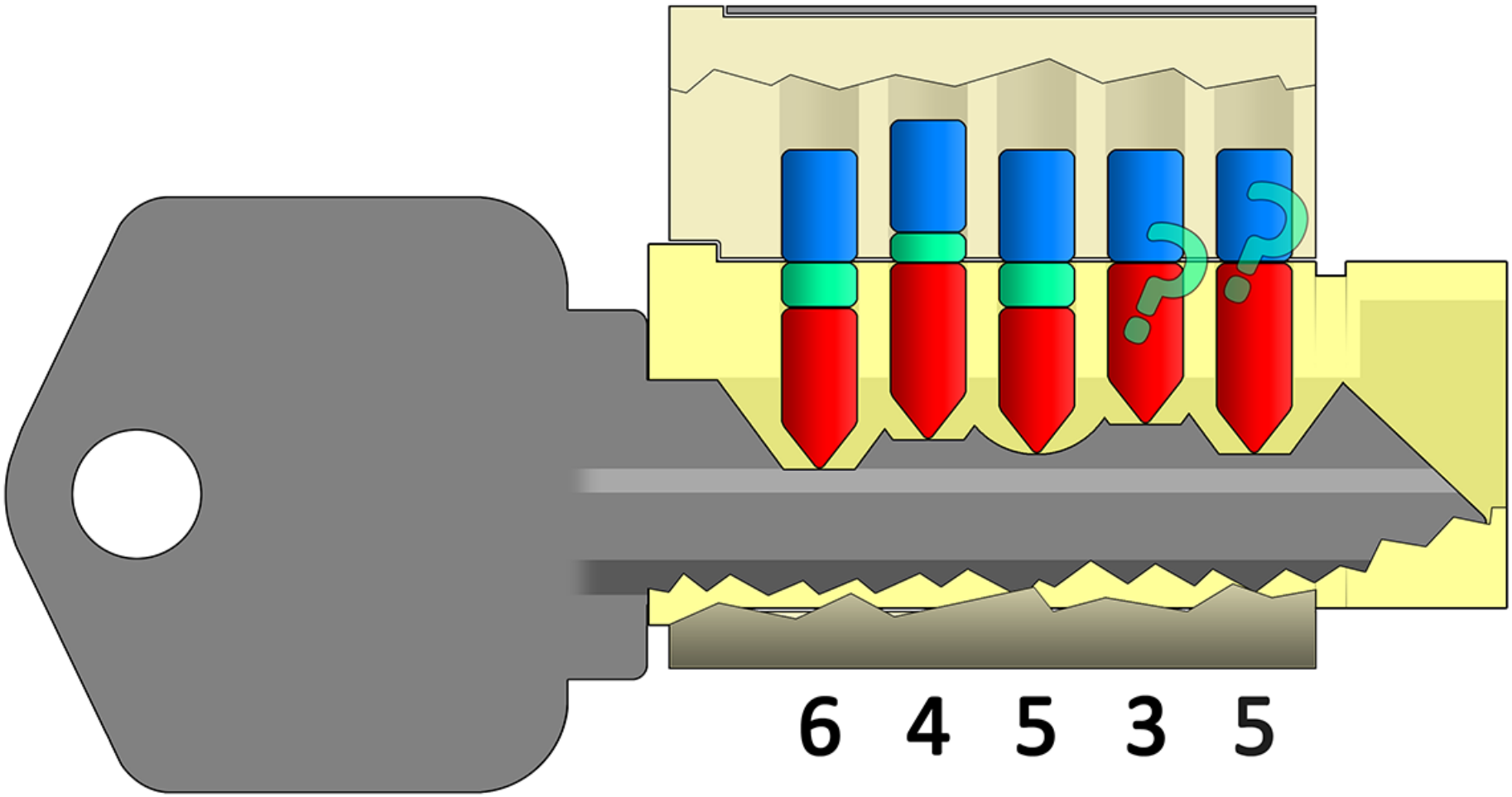
So, Let's Discuss What We Know



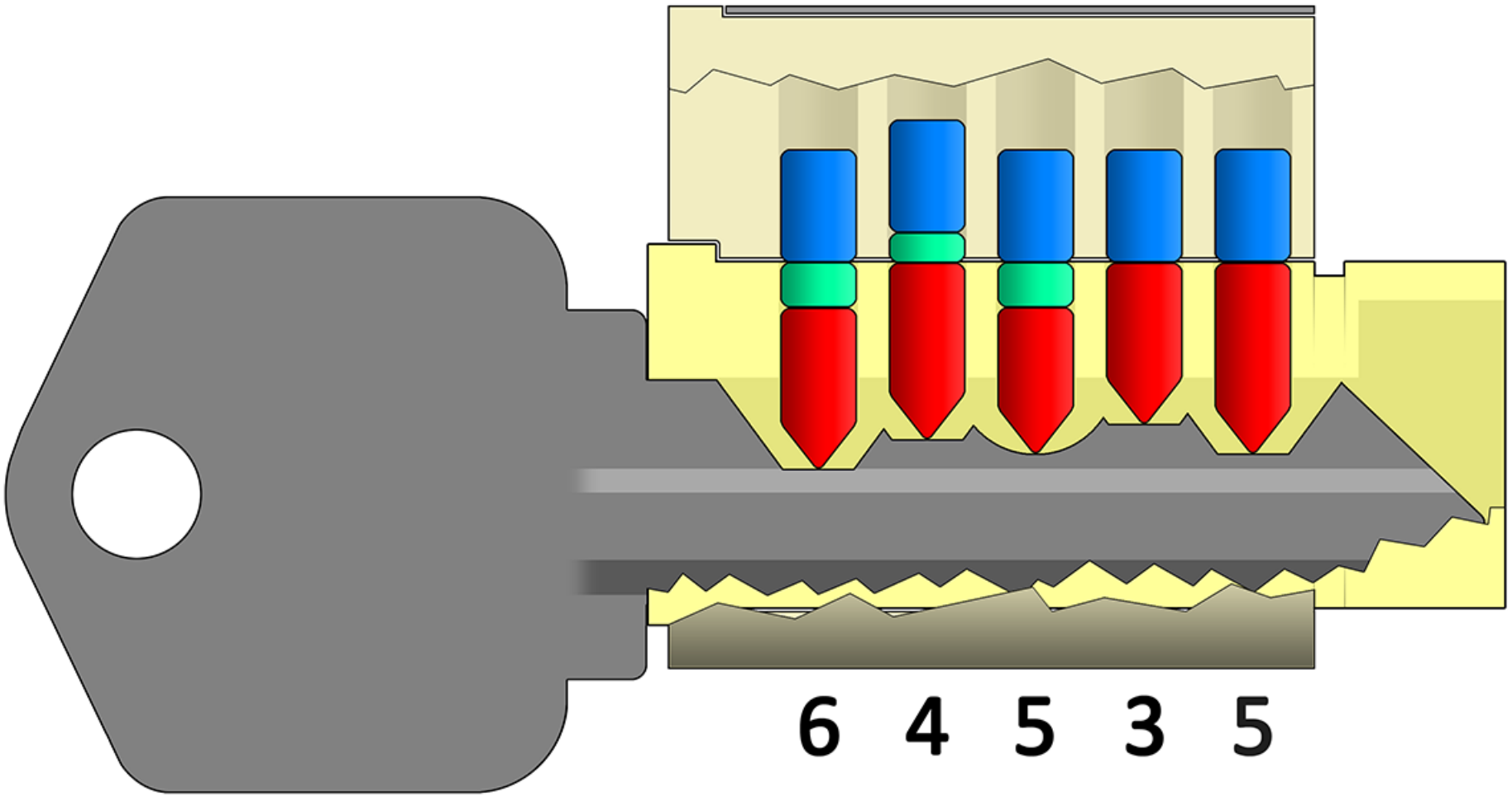
Mastering in Position Three



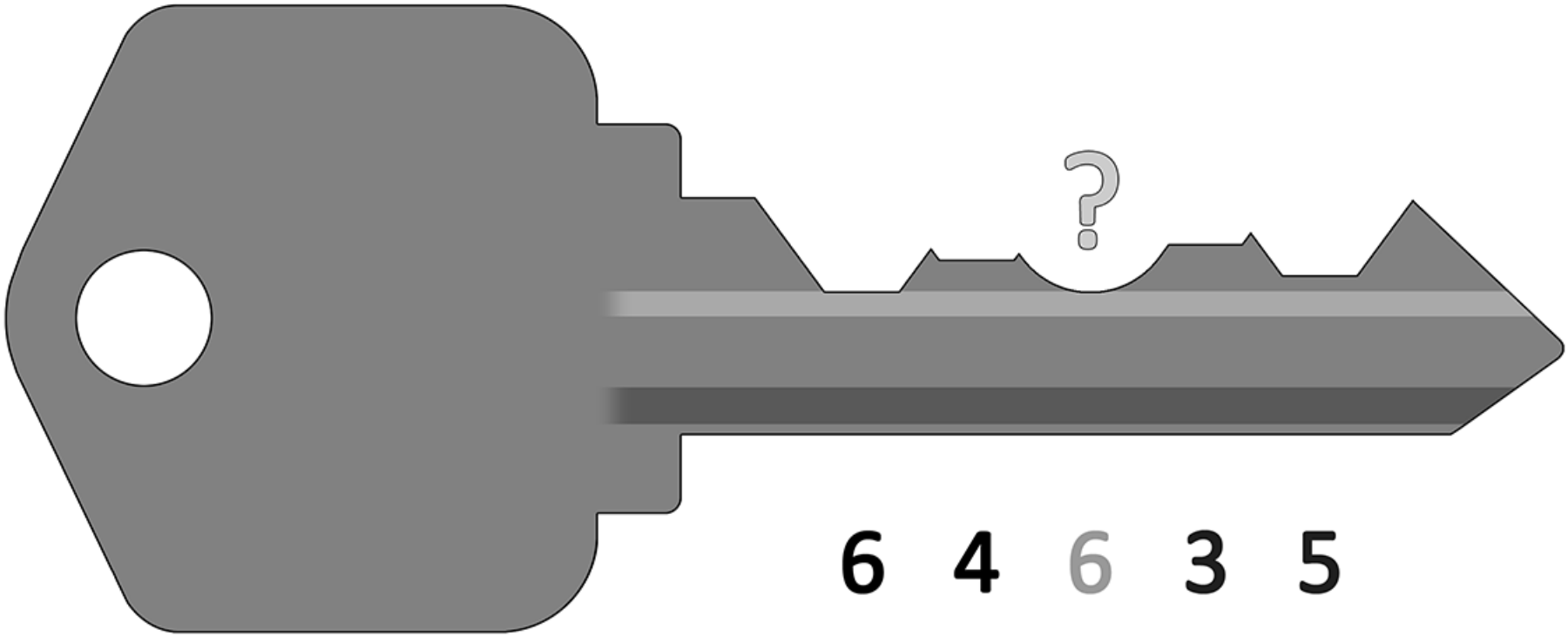
No News Yet Back Here



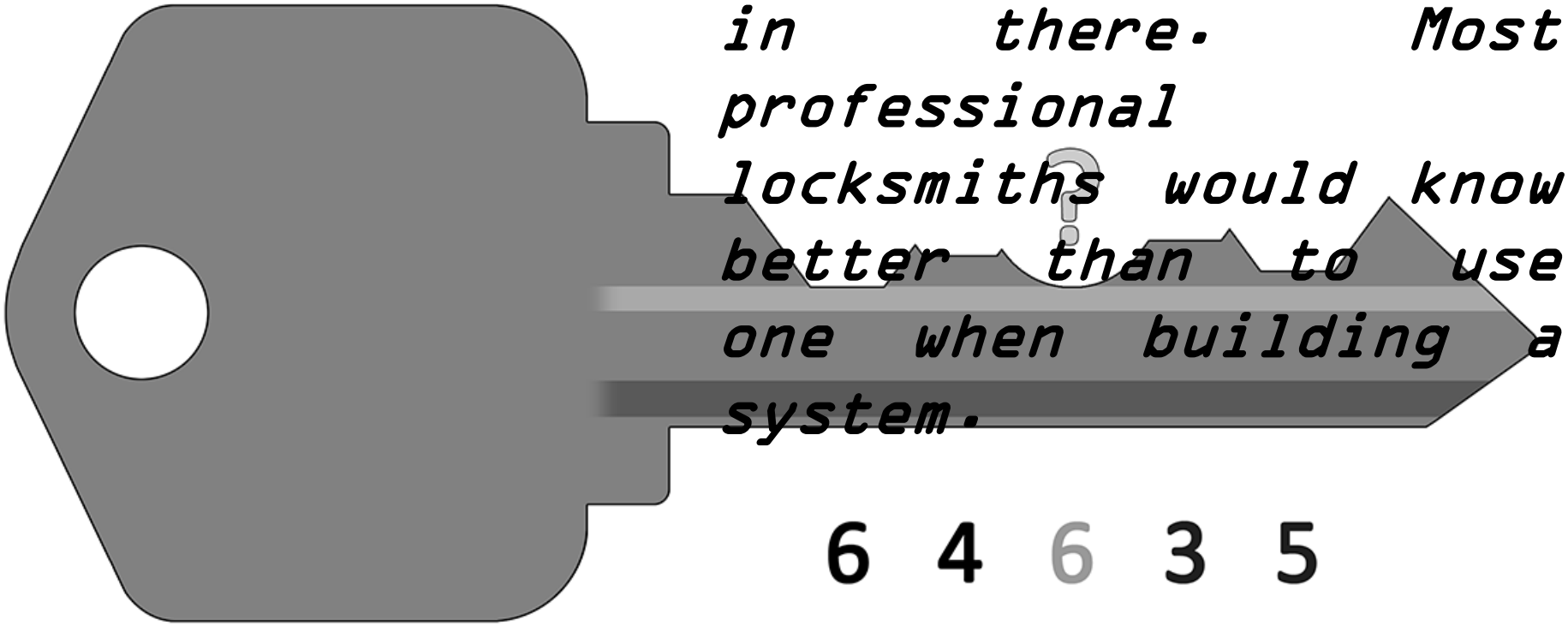
But Otherwise, Position Three



Would We Need to Explore a #b

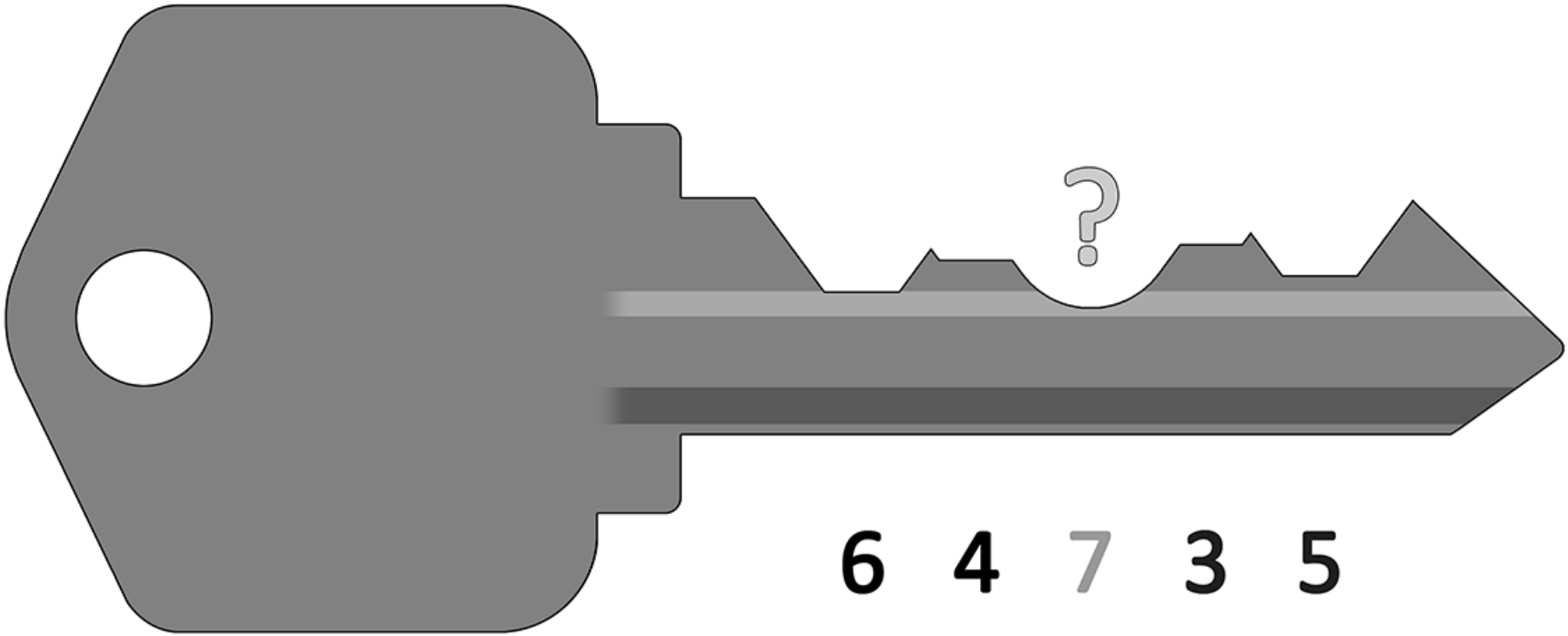


Would We Need to Explore a #6

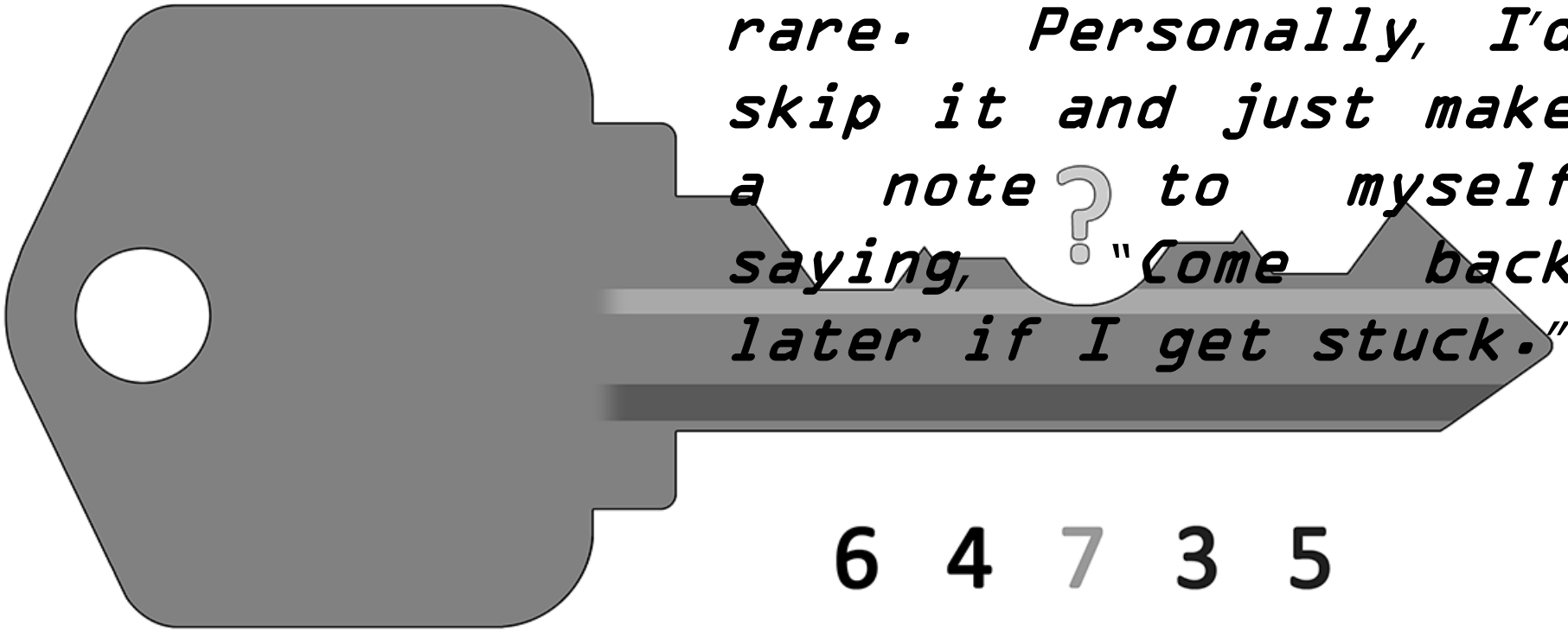


I wouldn't. That would mean there's a single-depth mastering pin in there. Most professional locksmiths would know better than to use one when building a system.

How About a #7 Depth?

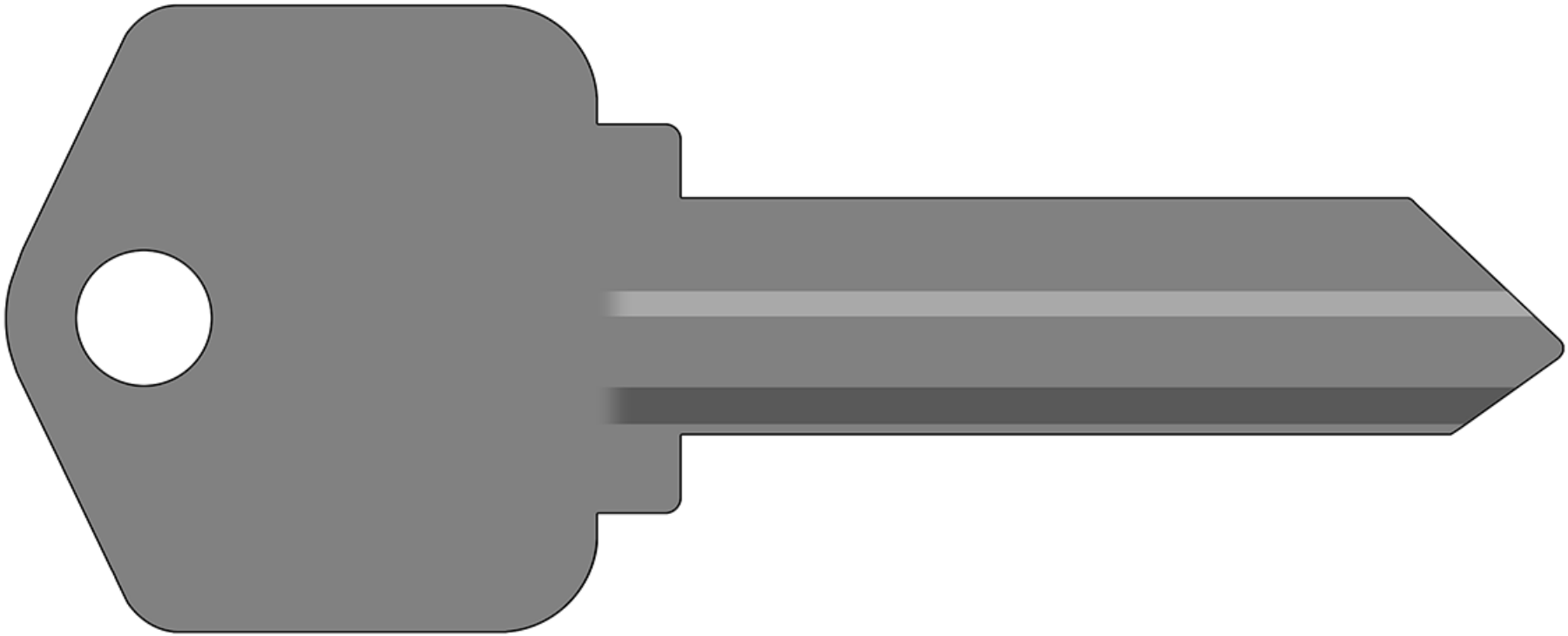


How About a #7 Depth?

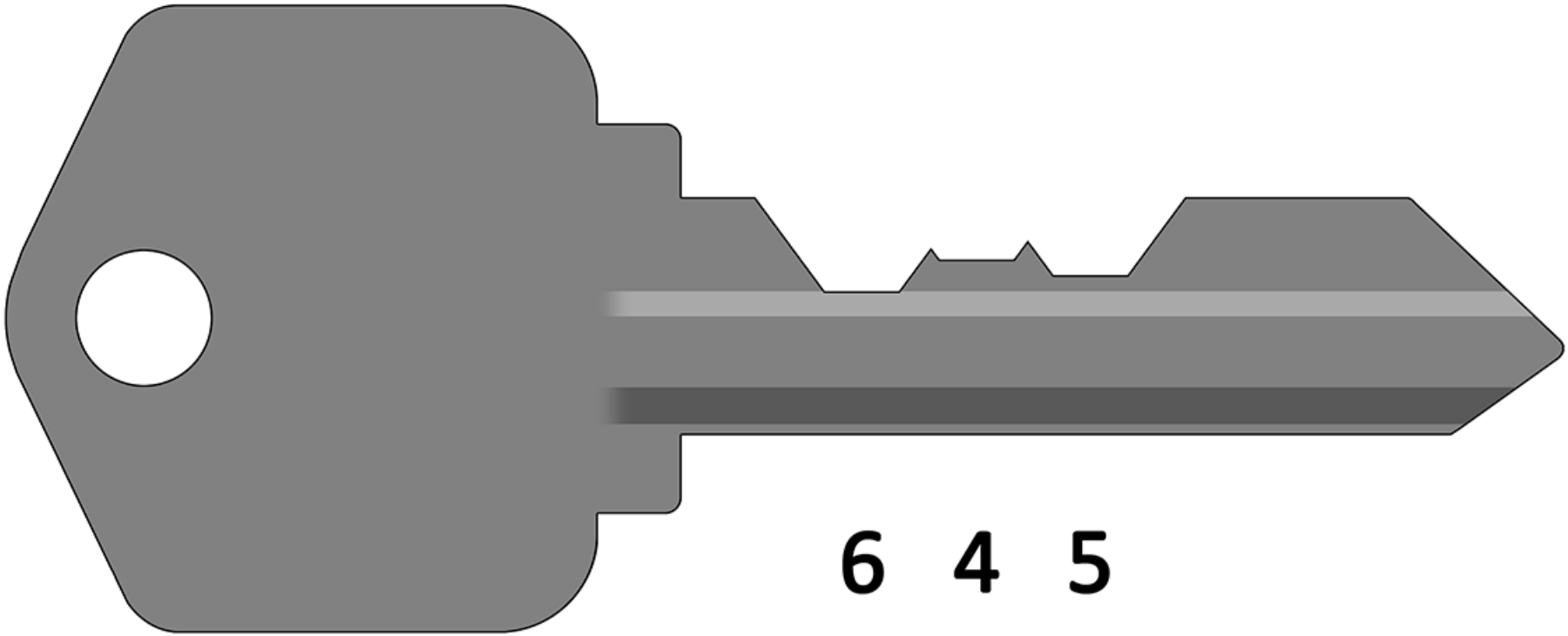


While it's possible to have multi-mastered pin stacks, this is rare. Personally, I'd skip it and just make a note to myself saying, "Come back later if I get stuck."

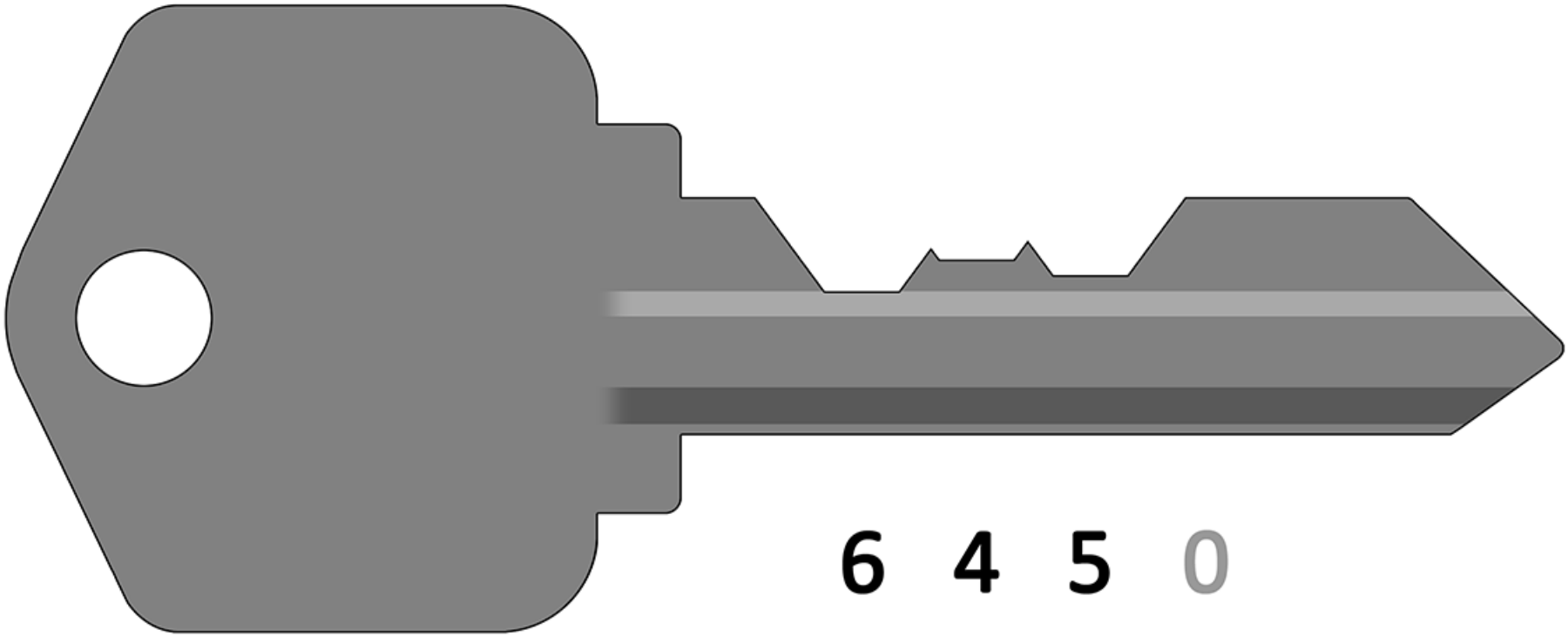
Let's Prepare a Fourth Exploring



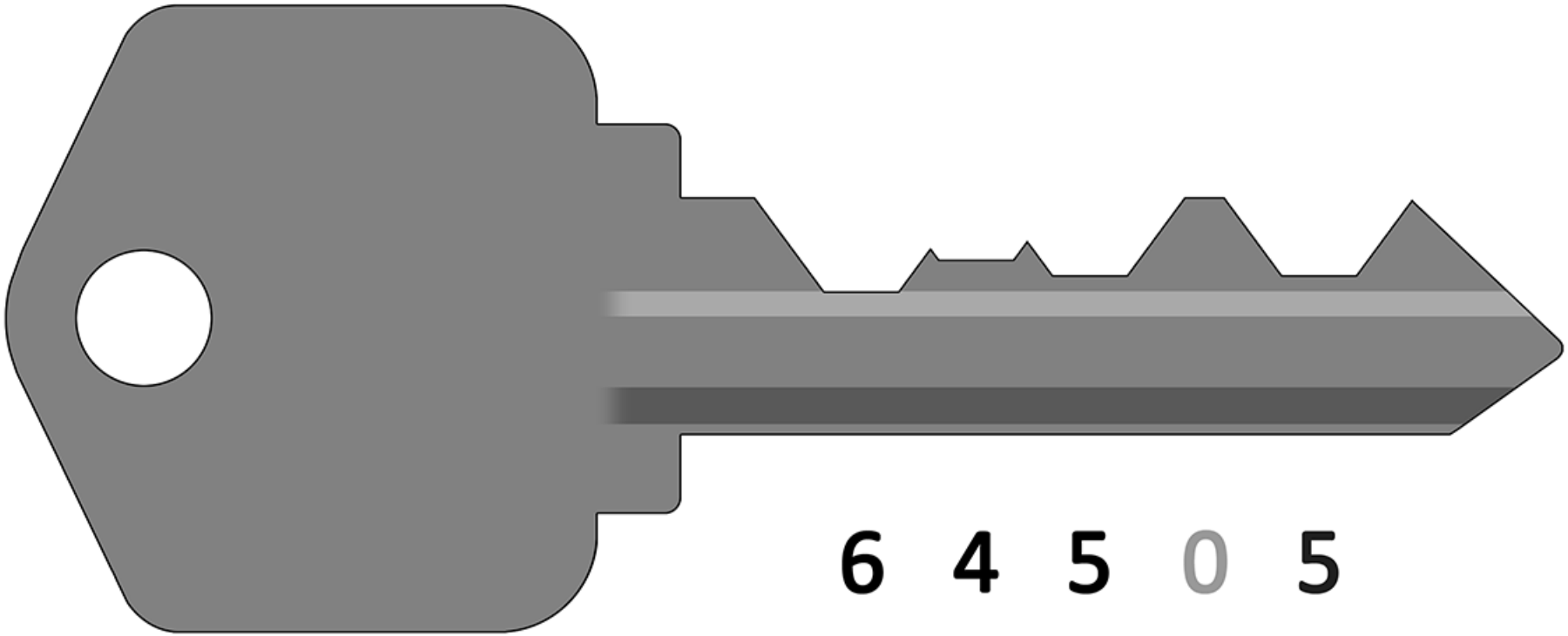
Start Out with Mastering We've



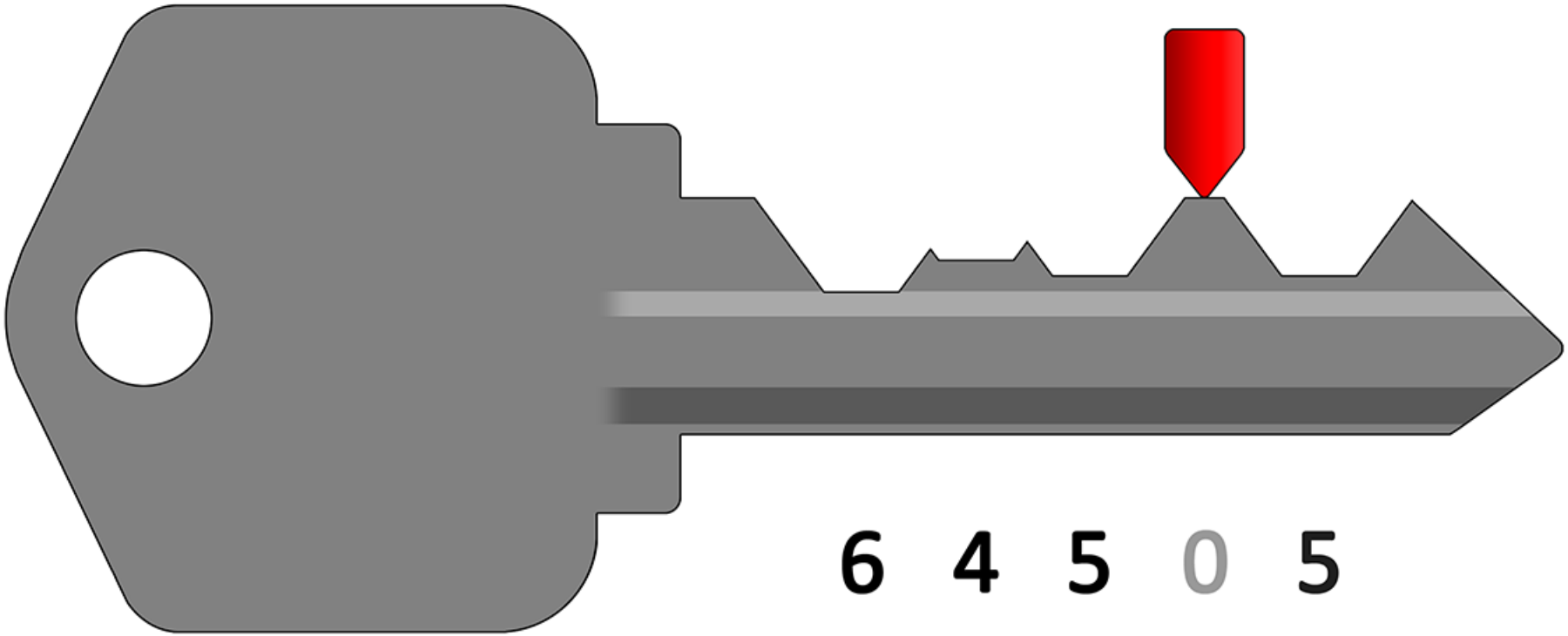
Leave Position Four Blank



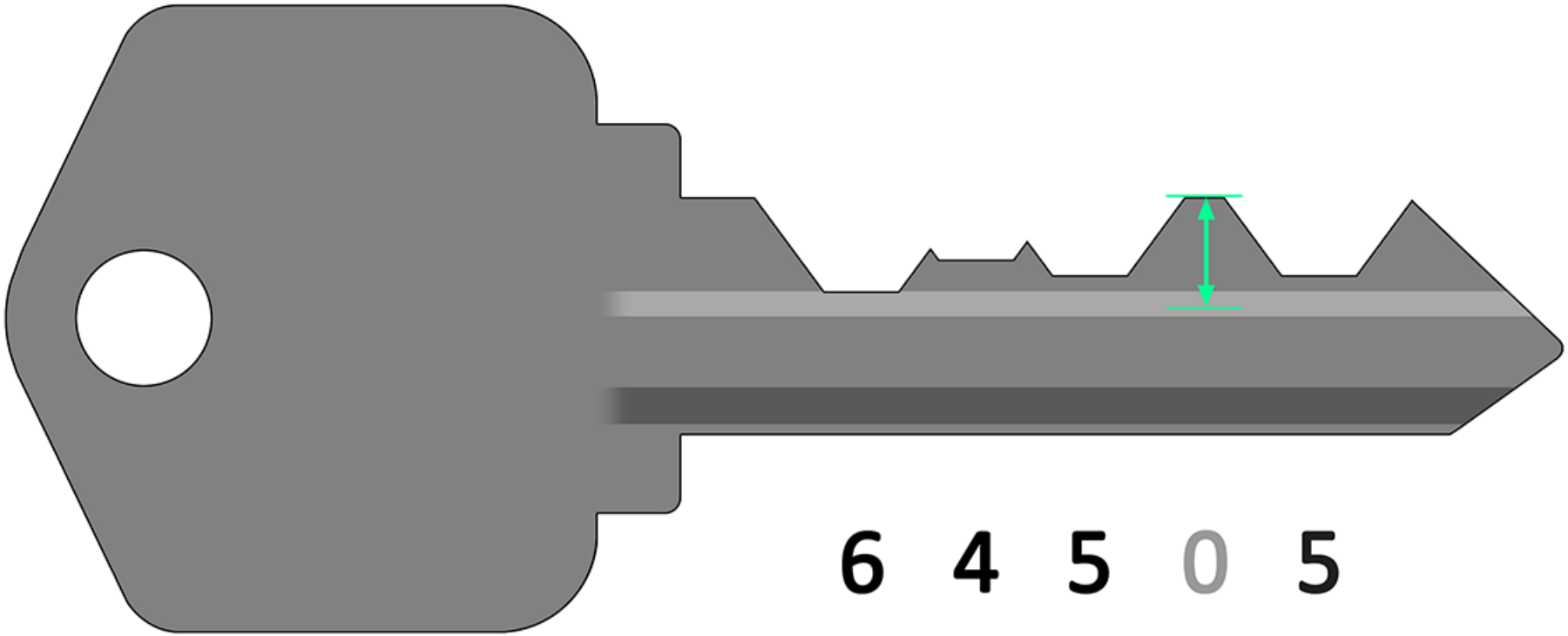
Exploring Key Number Four, Fully-



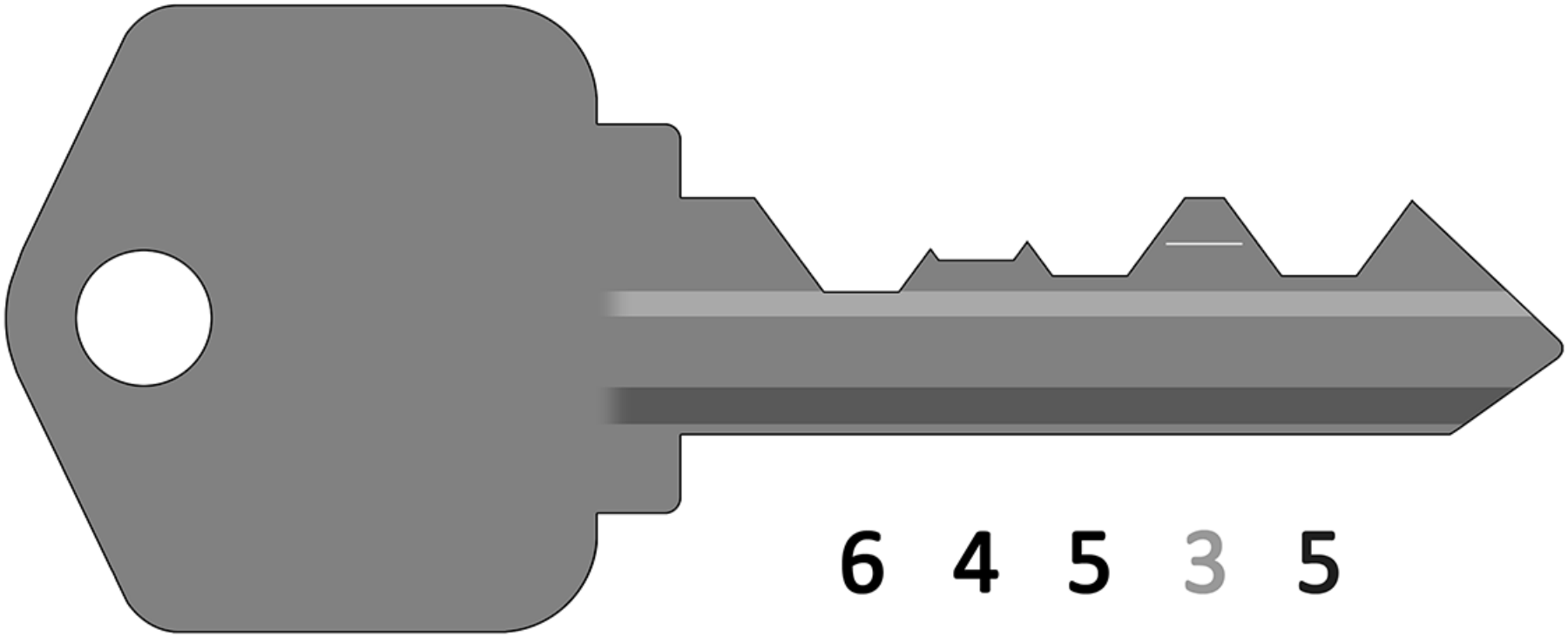
Keep in Mind, This Violates MACS



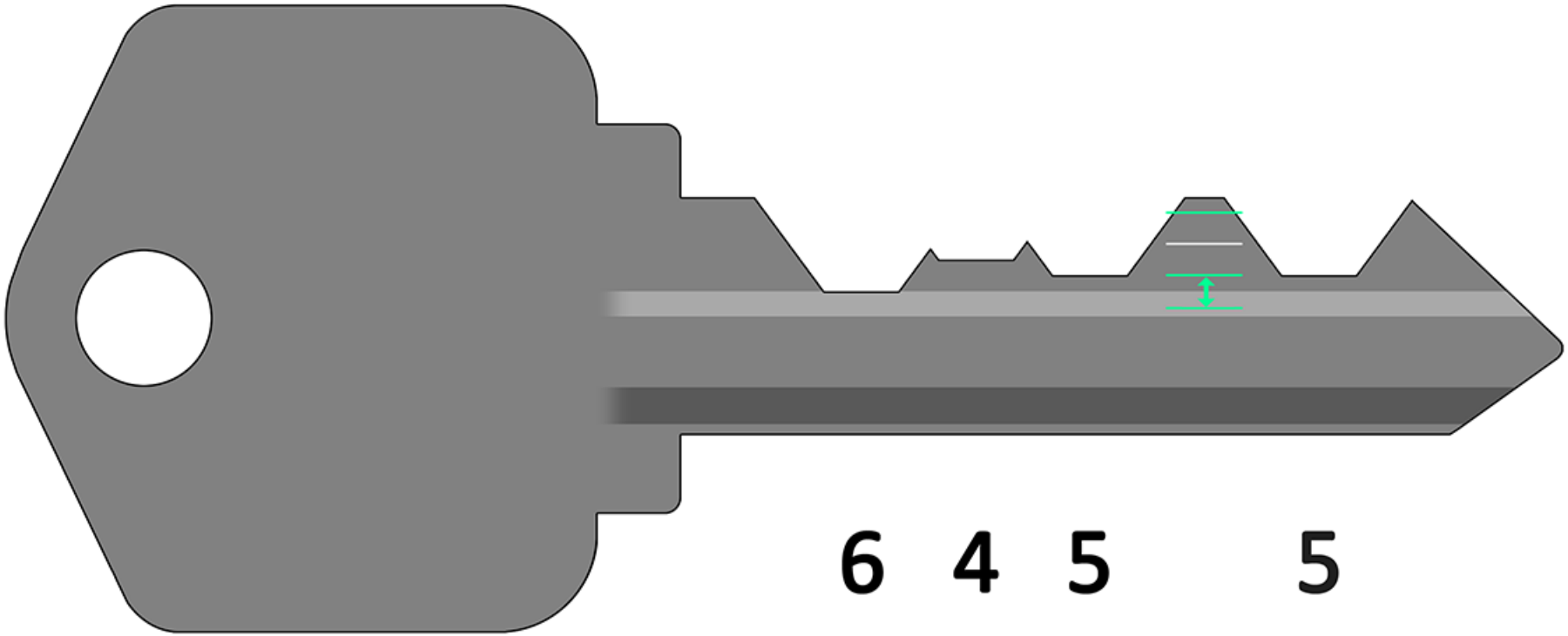
We Could Sweep This Exploring



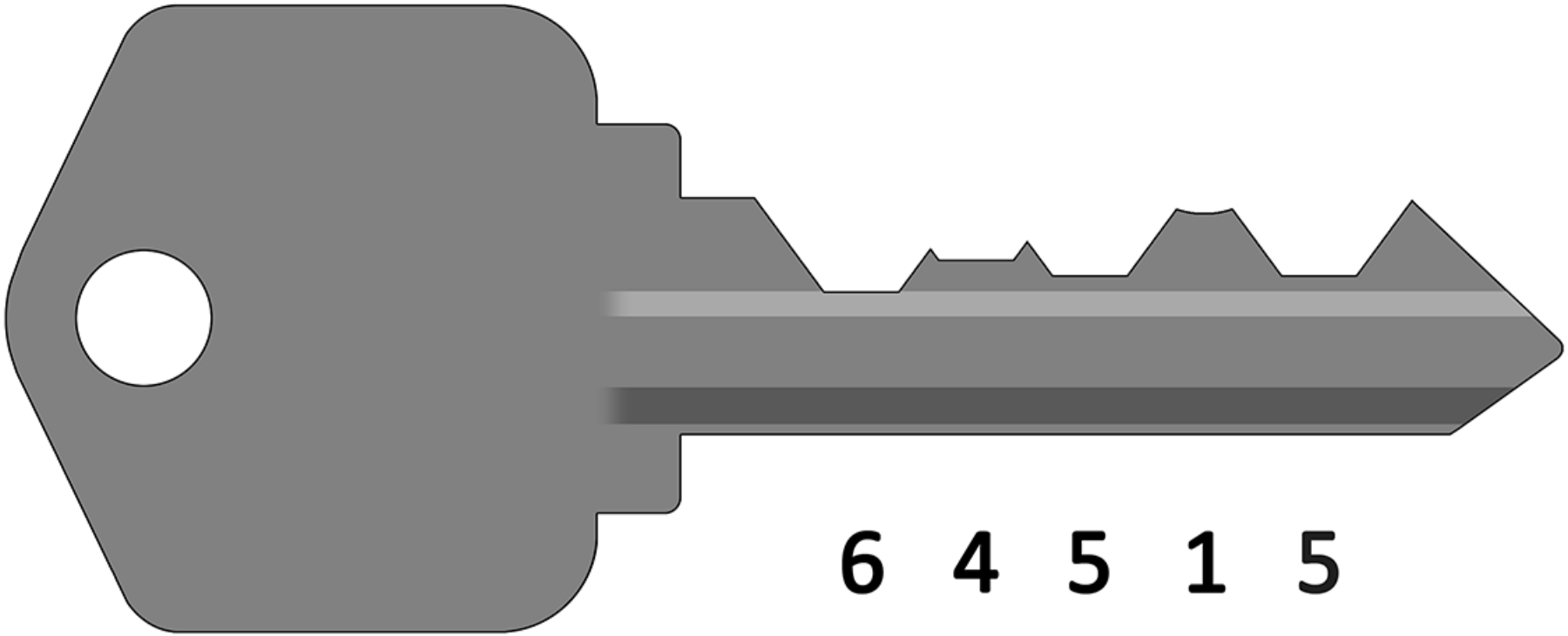
But Remember This is the Change



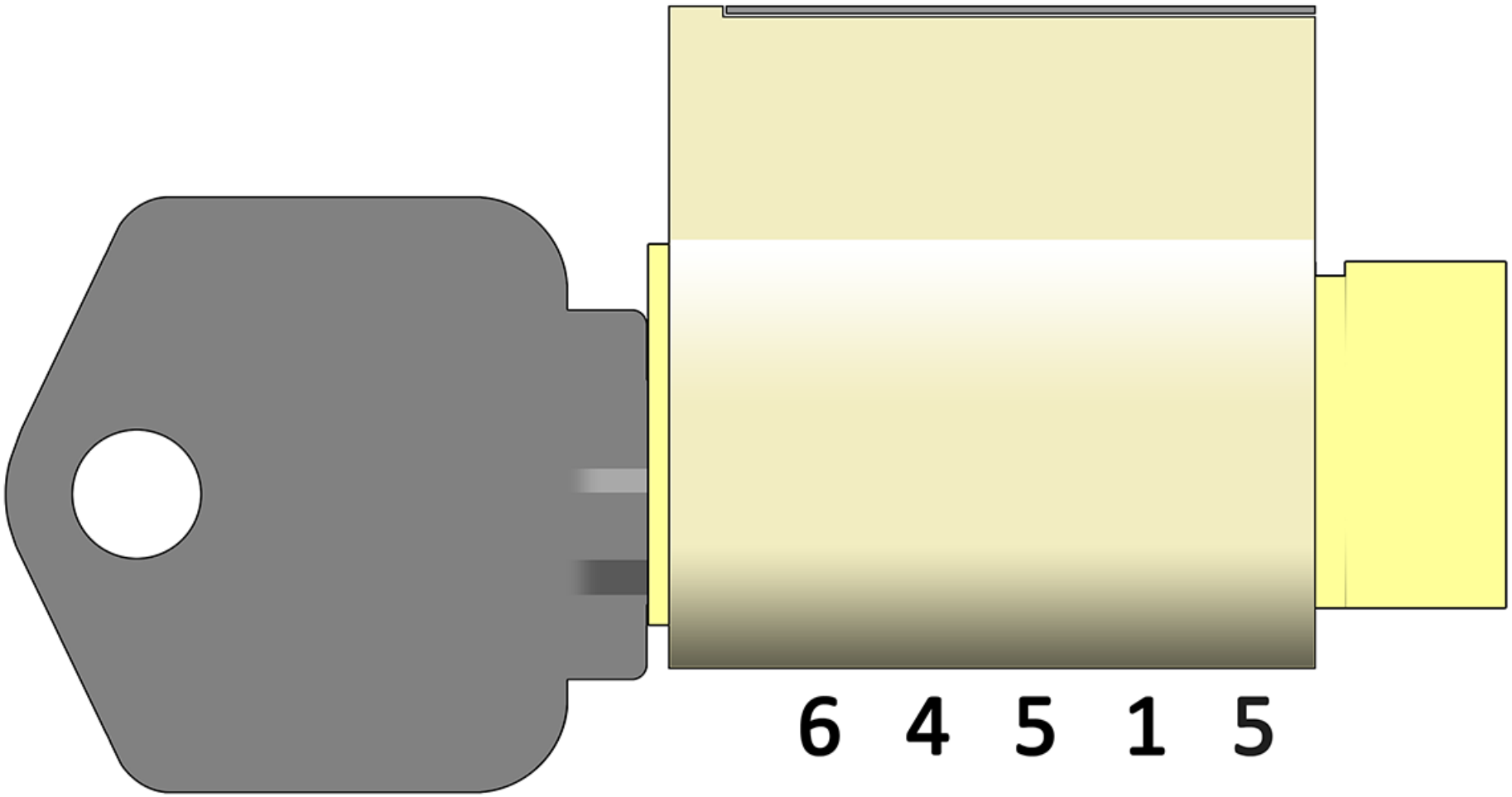
More Efficient: Only Explore



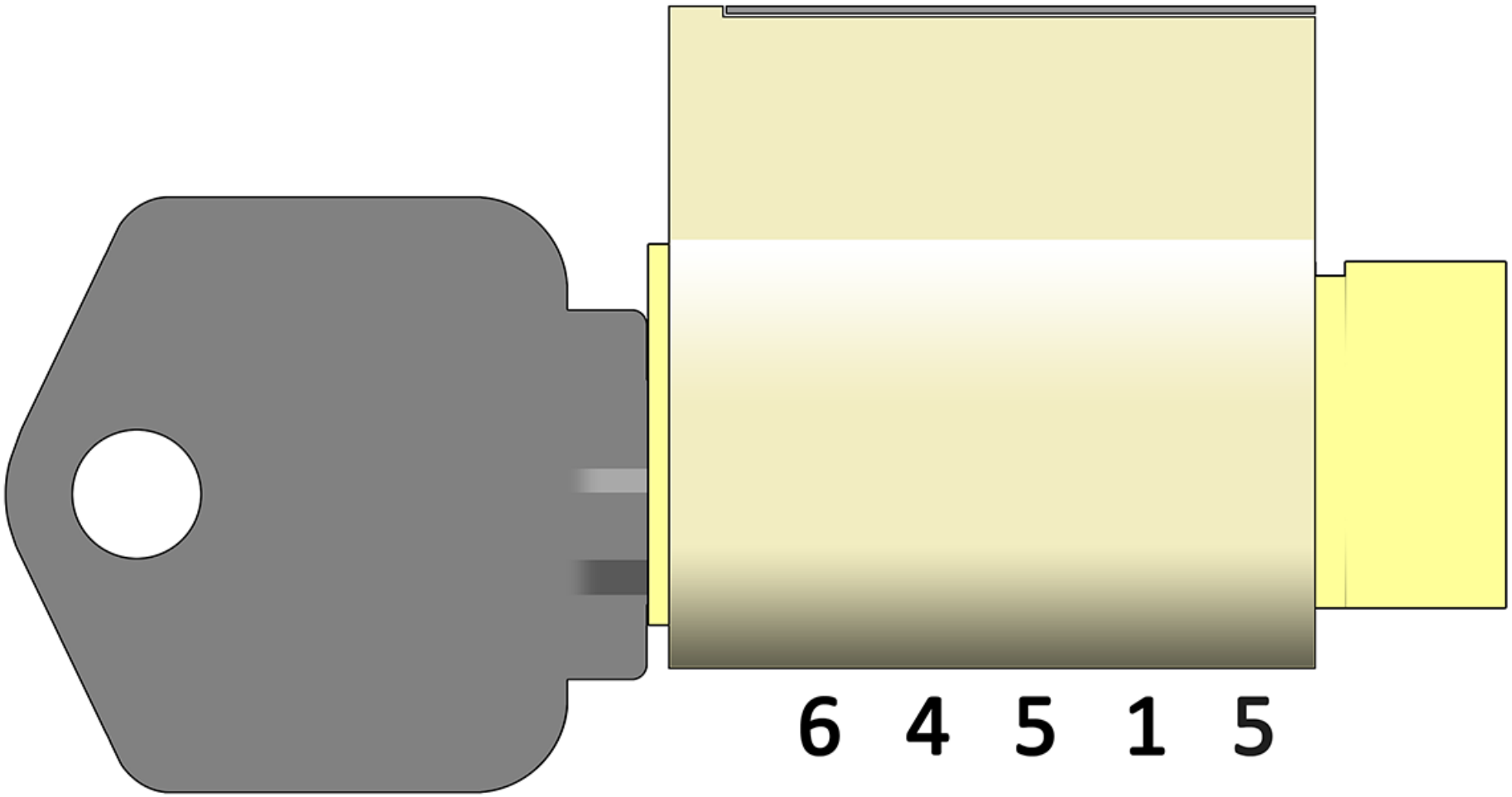
Code-Cut (or Simply File) to the



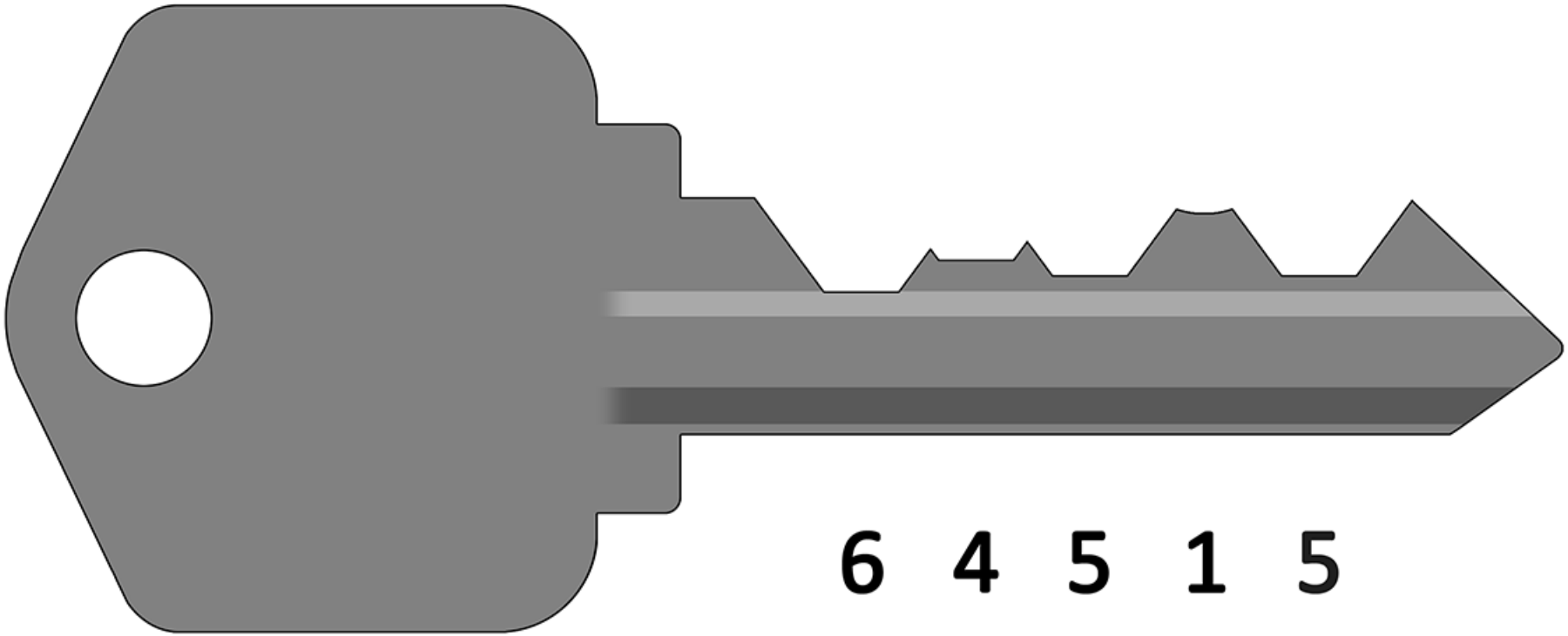
Key Four, First Attempt…



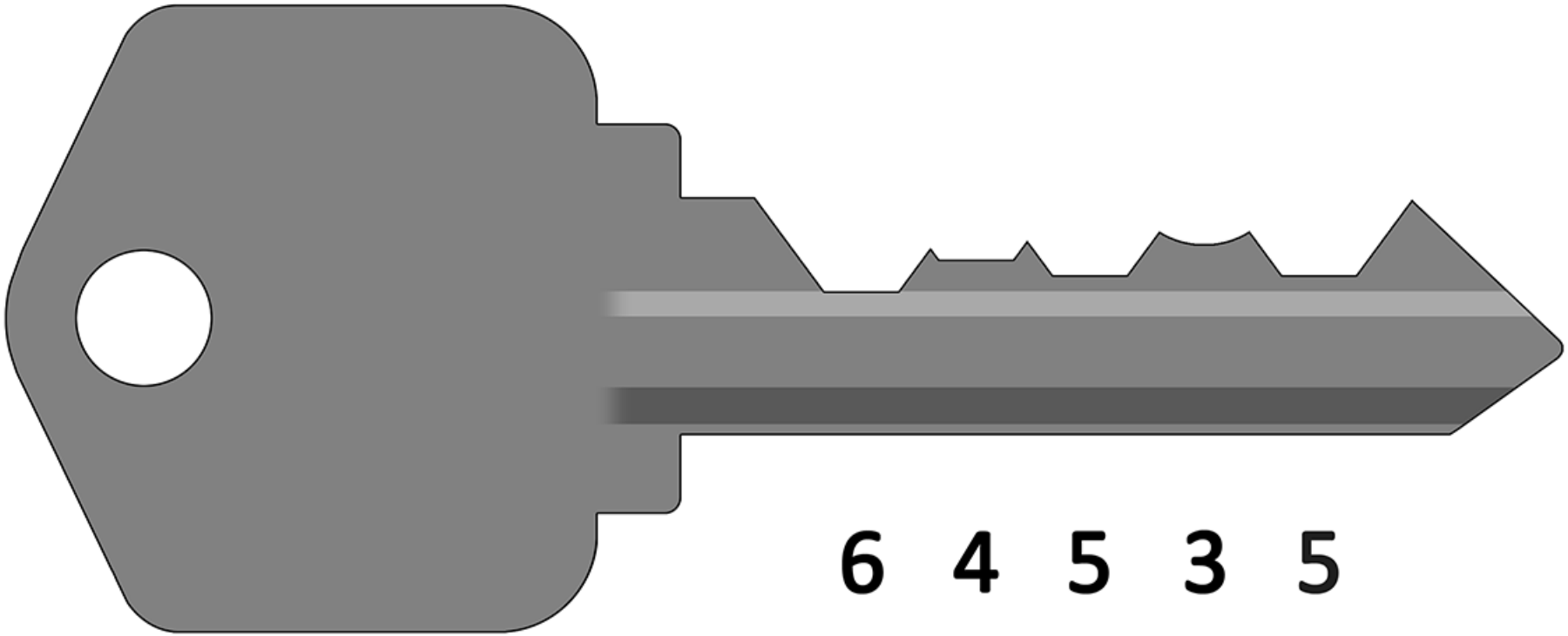
Key Four, First Attempt… No Go.



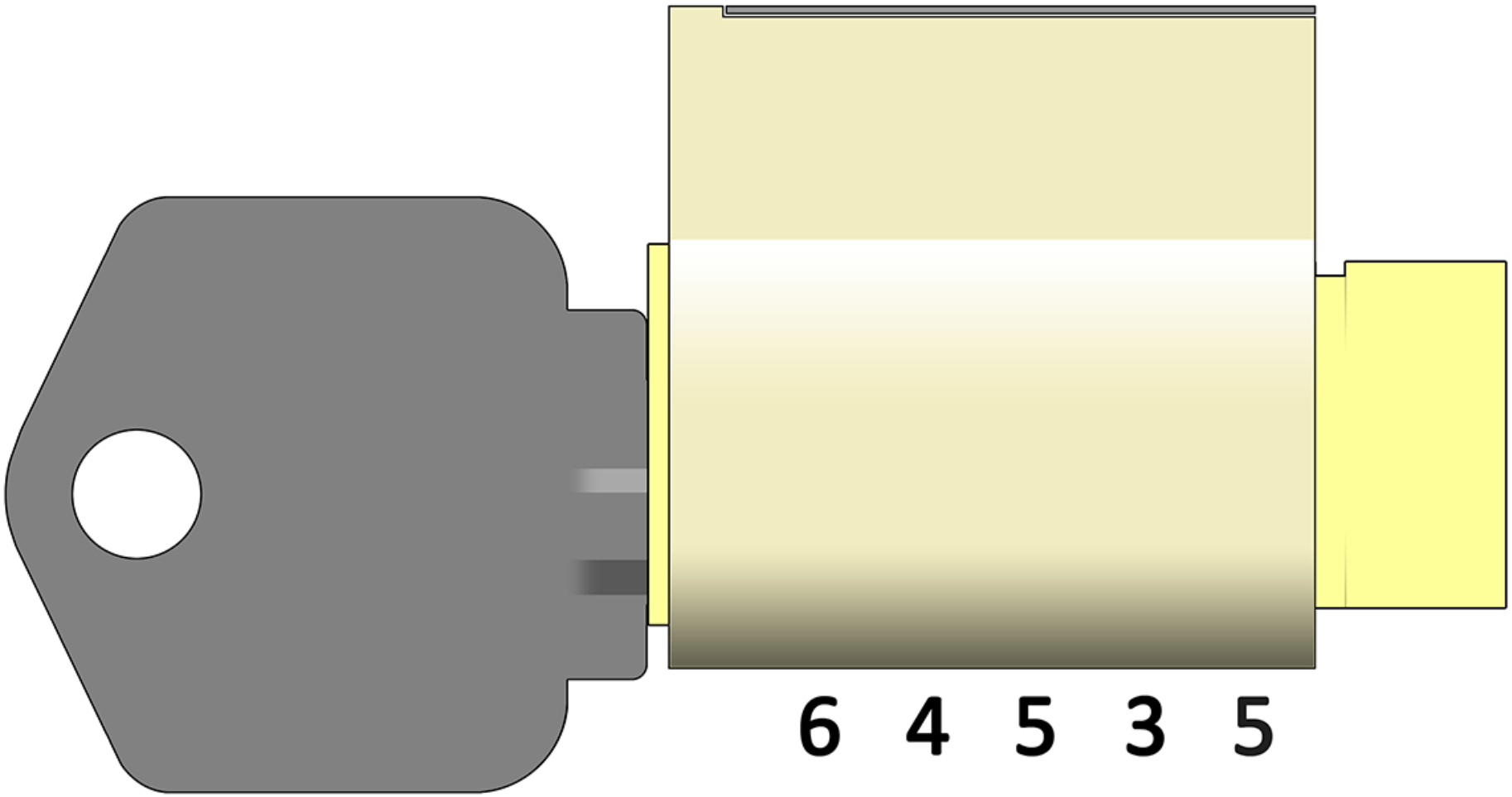
Remove the Key



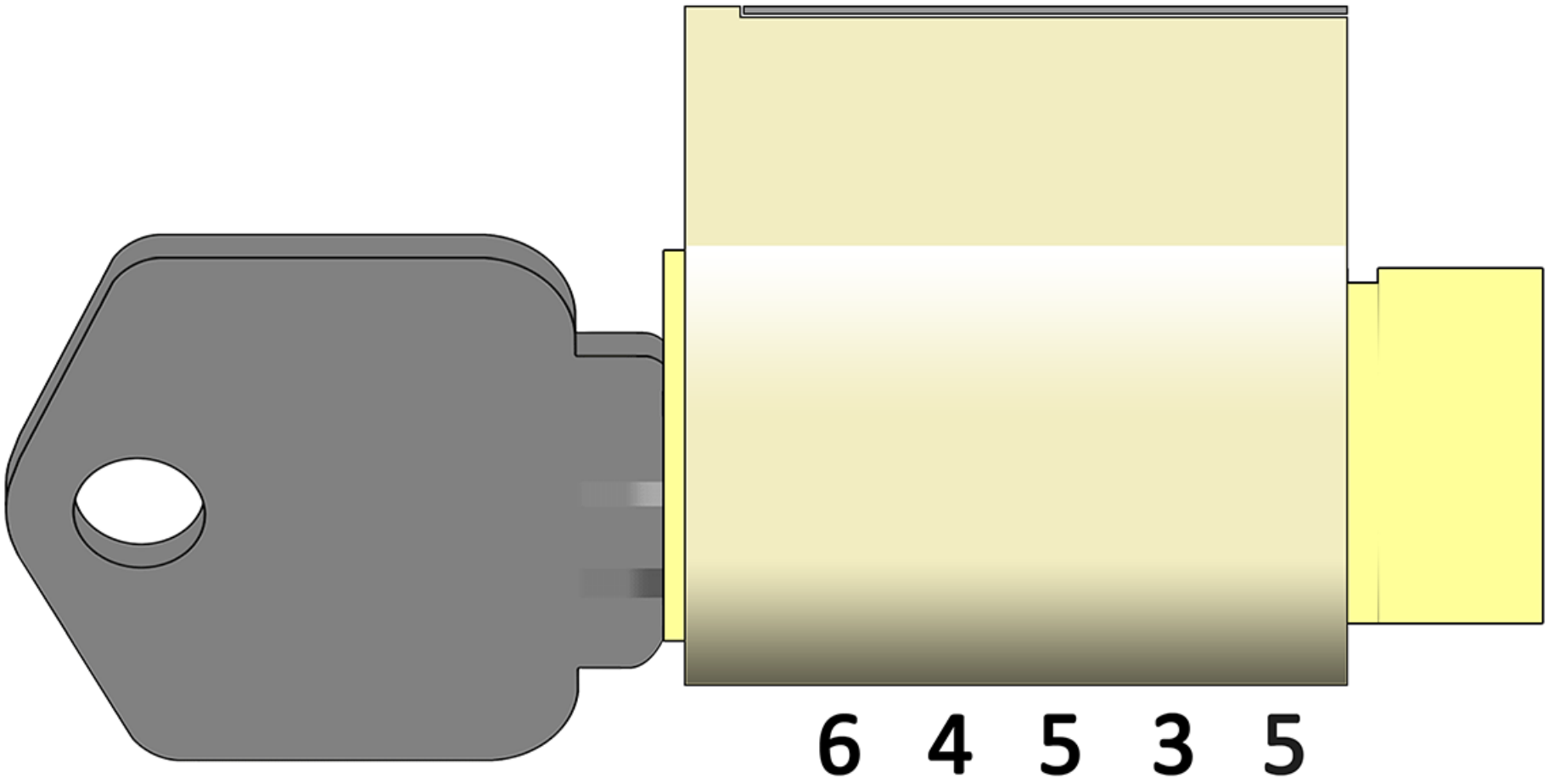
If Desired, File to the #3 Depth,



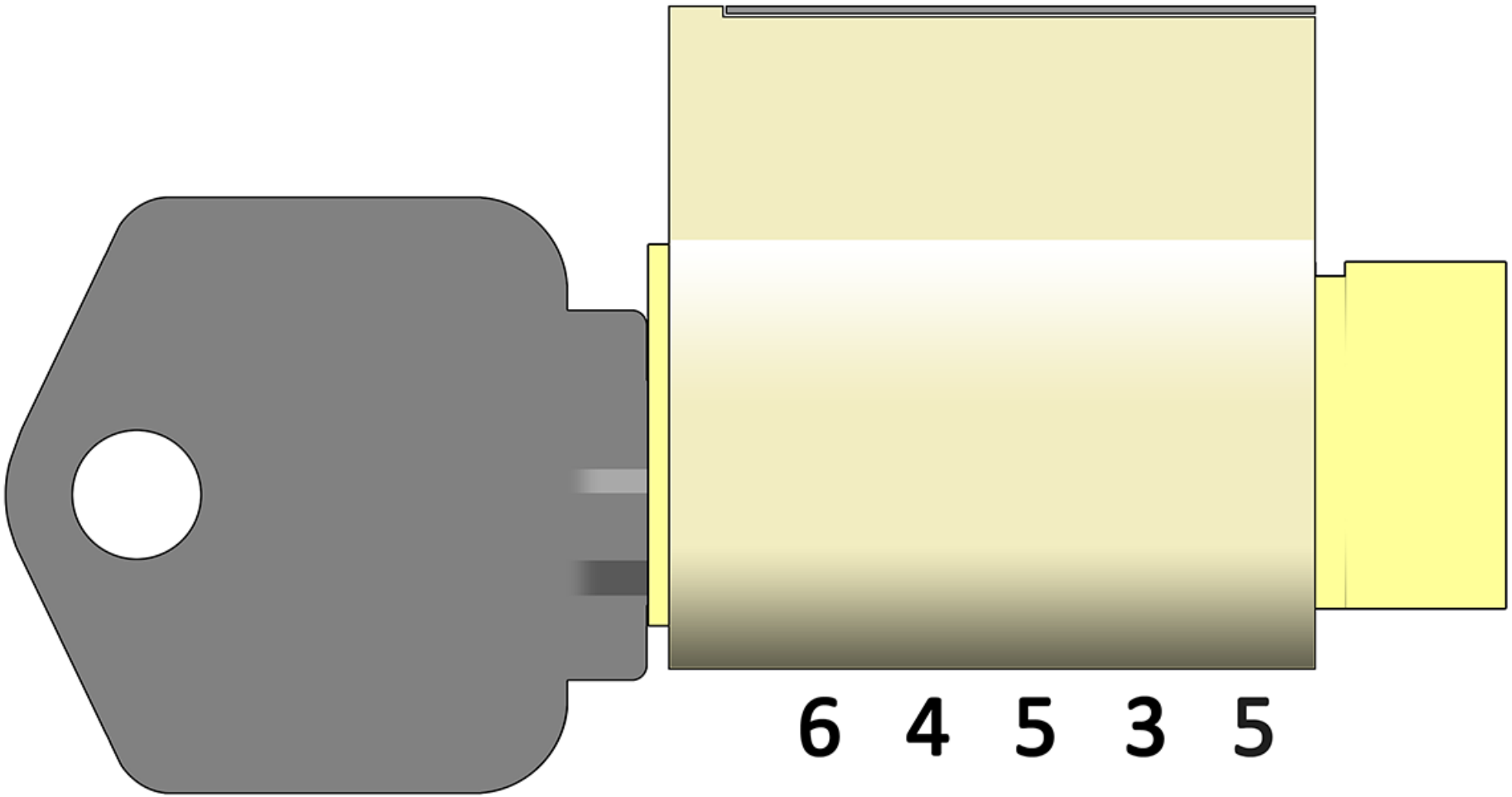
Give the Key a Try…



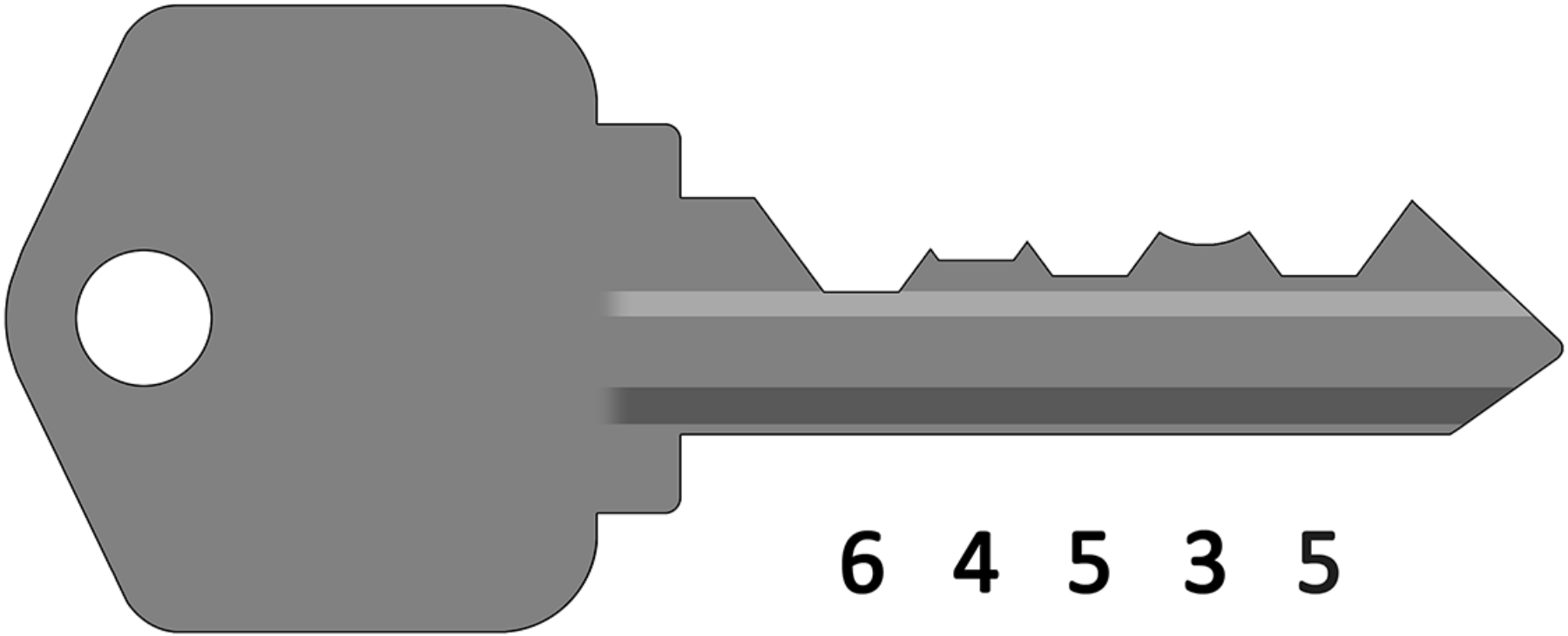
Give the Key a Try… OPEN!



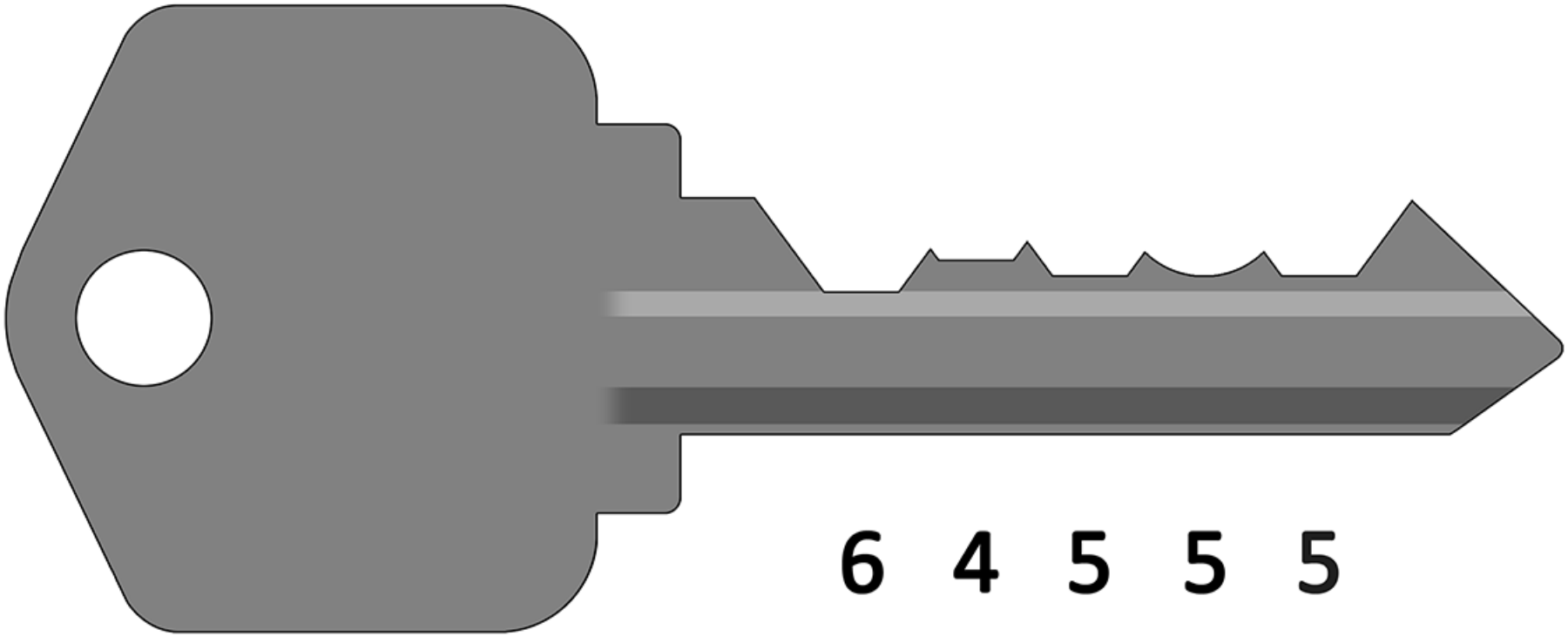
That Was Expected, of Course



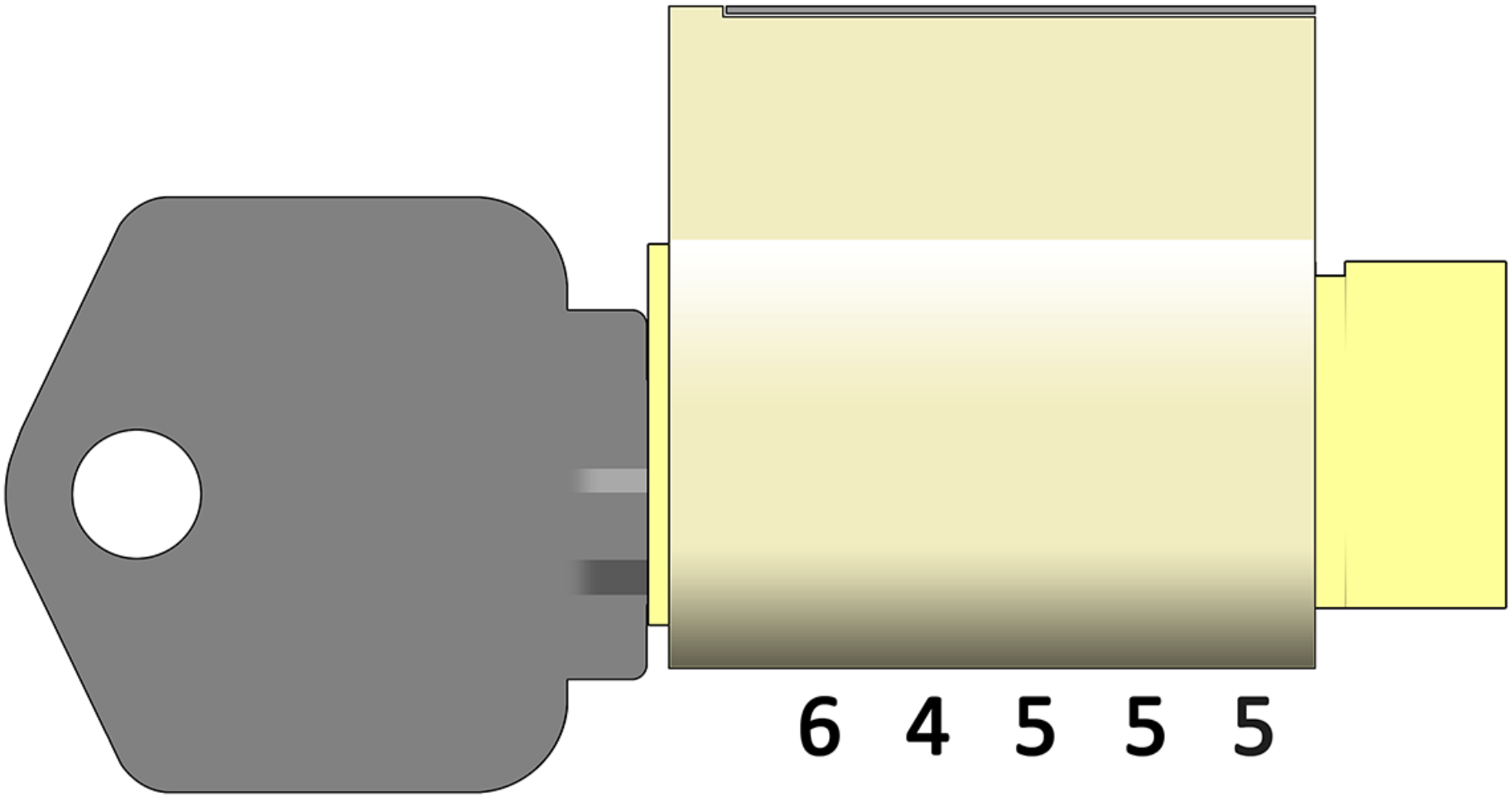
Remove the Key



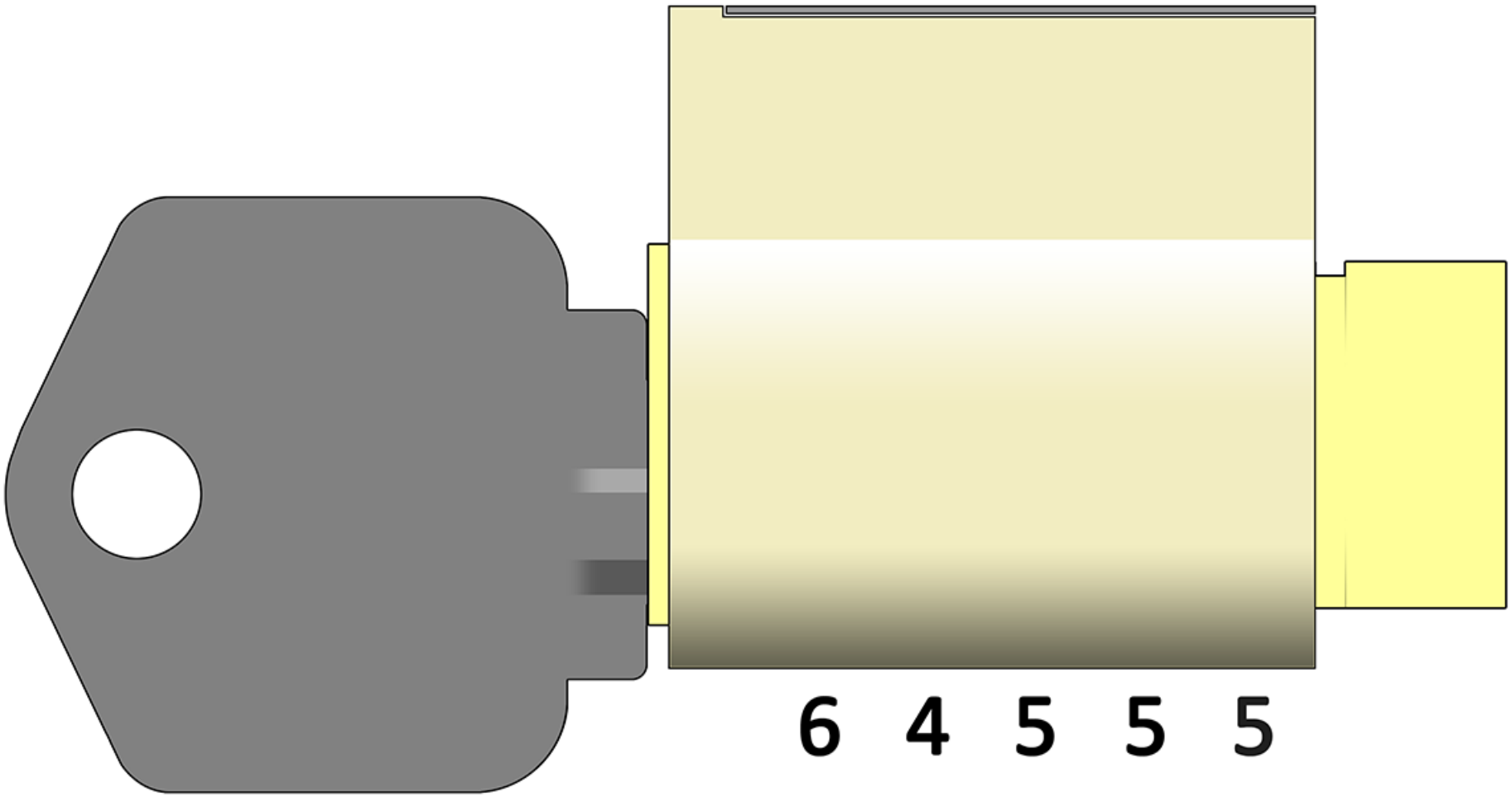
File Down… Skipping a Depth, to



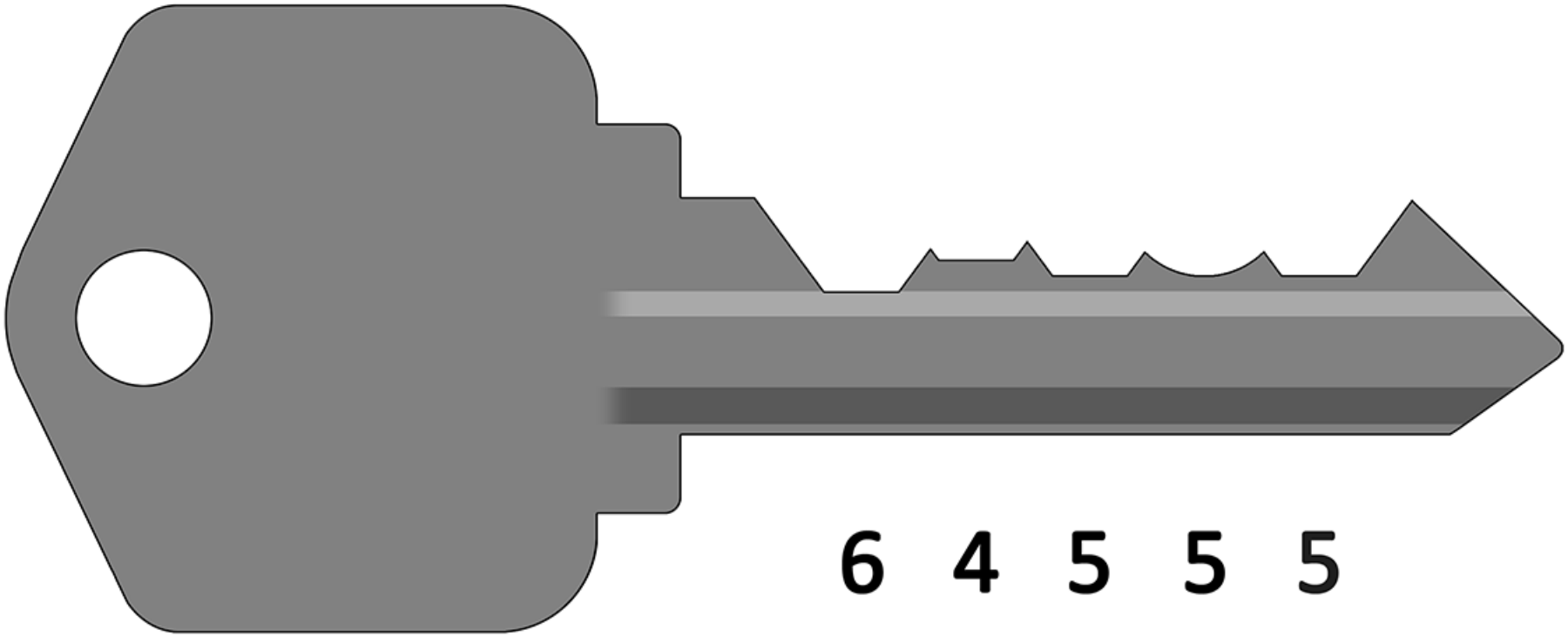
Try the Key…



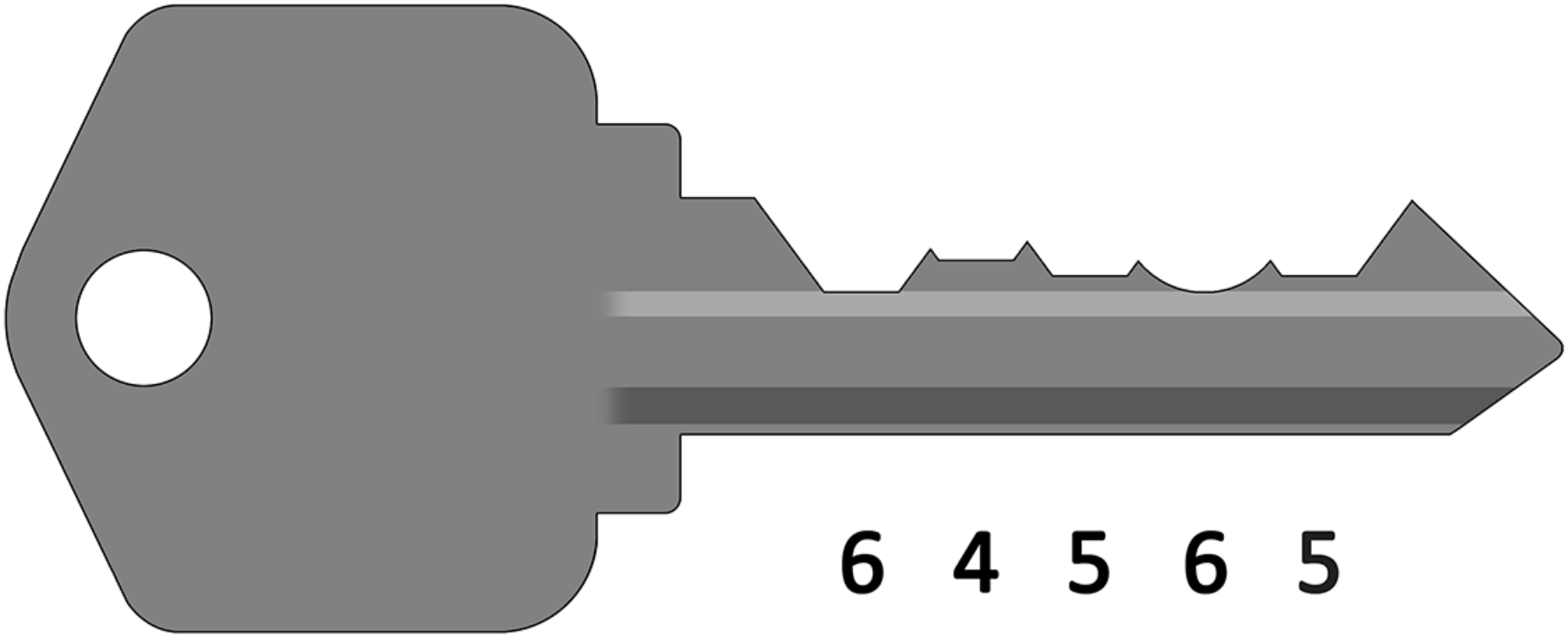
Try the Key… No Luck.



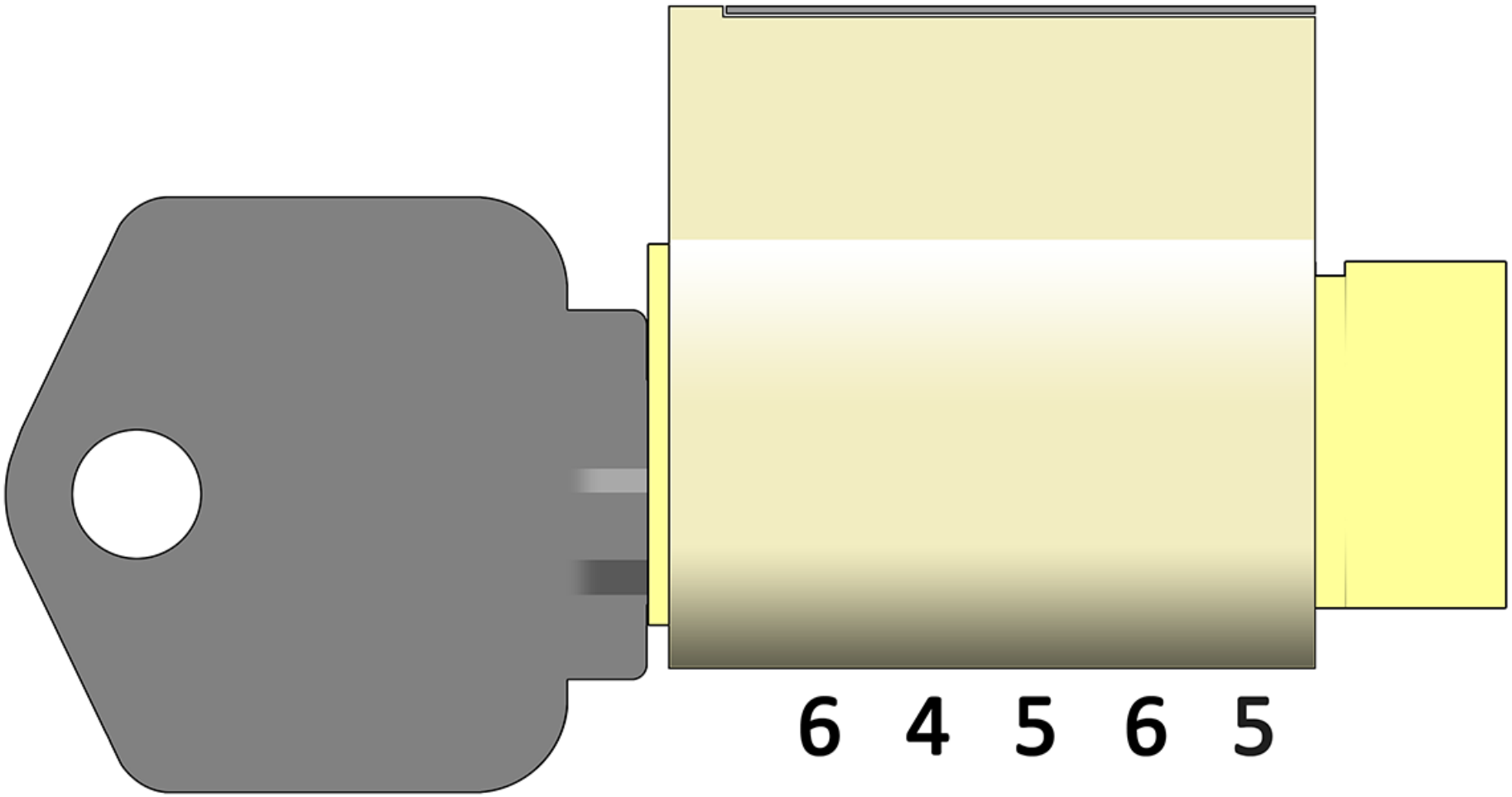
Remove the Key



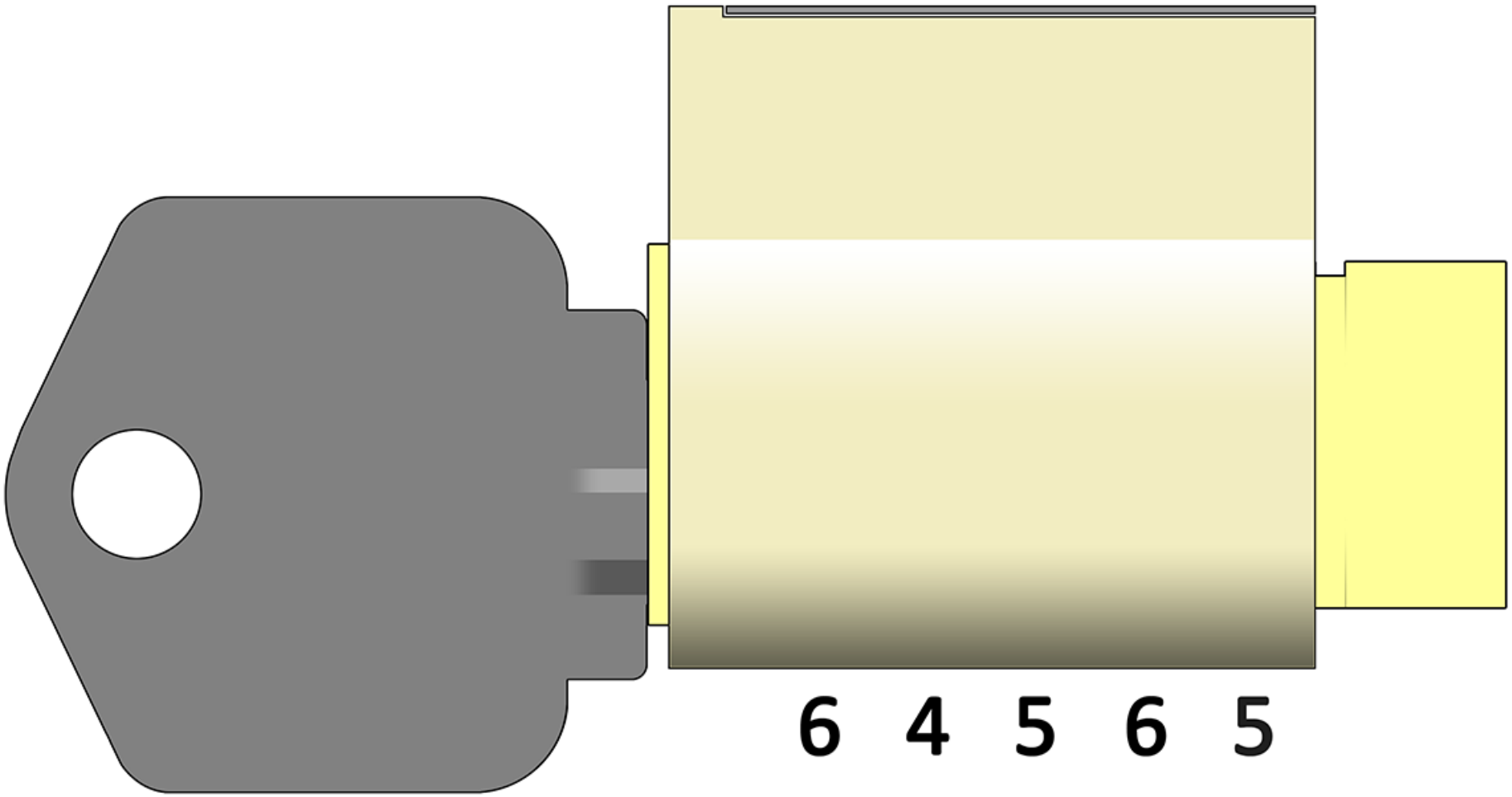
File Down by Another Depth



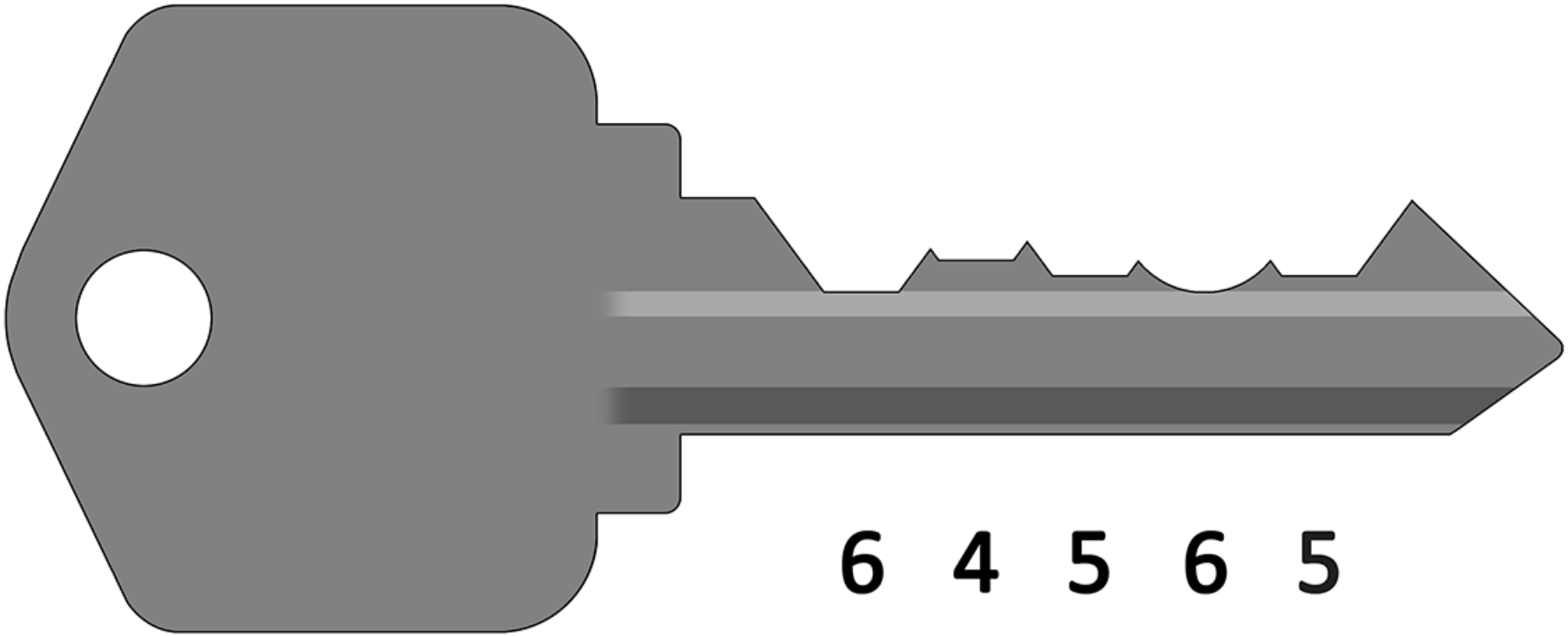
Try the Key…



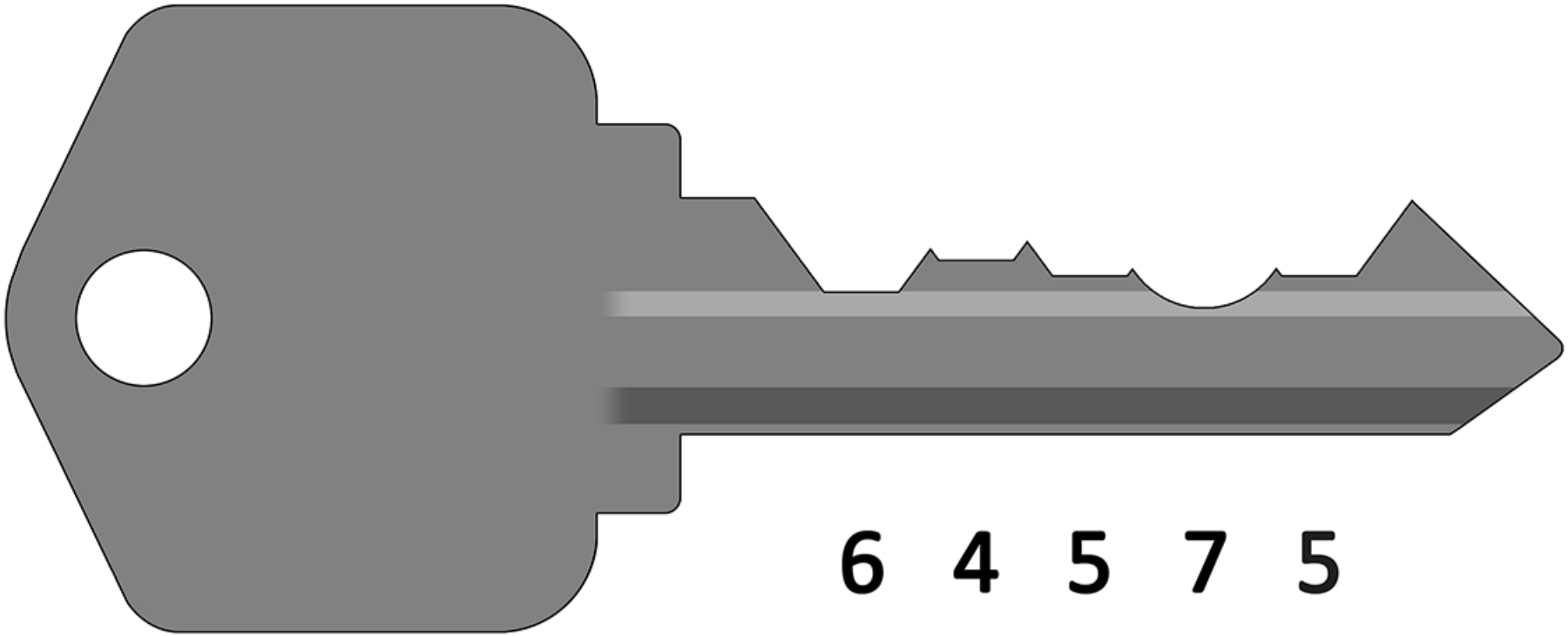
Try the Key… No Joy.



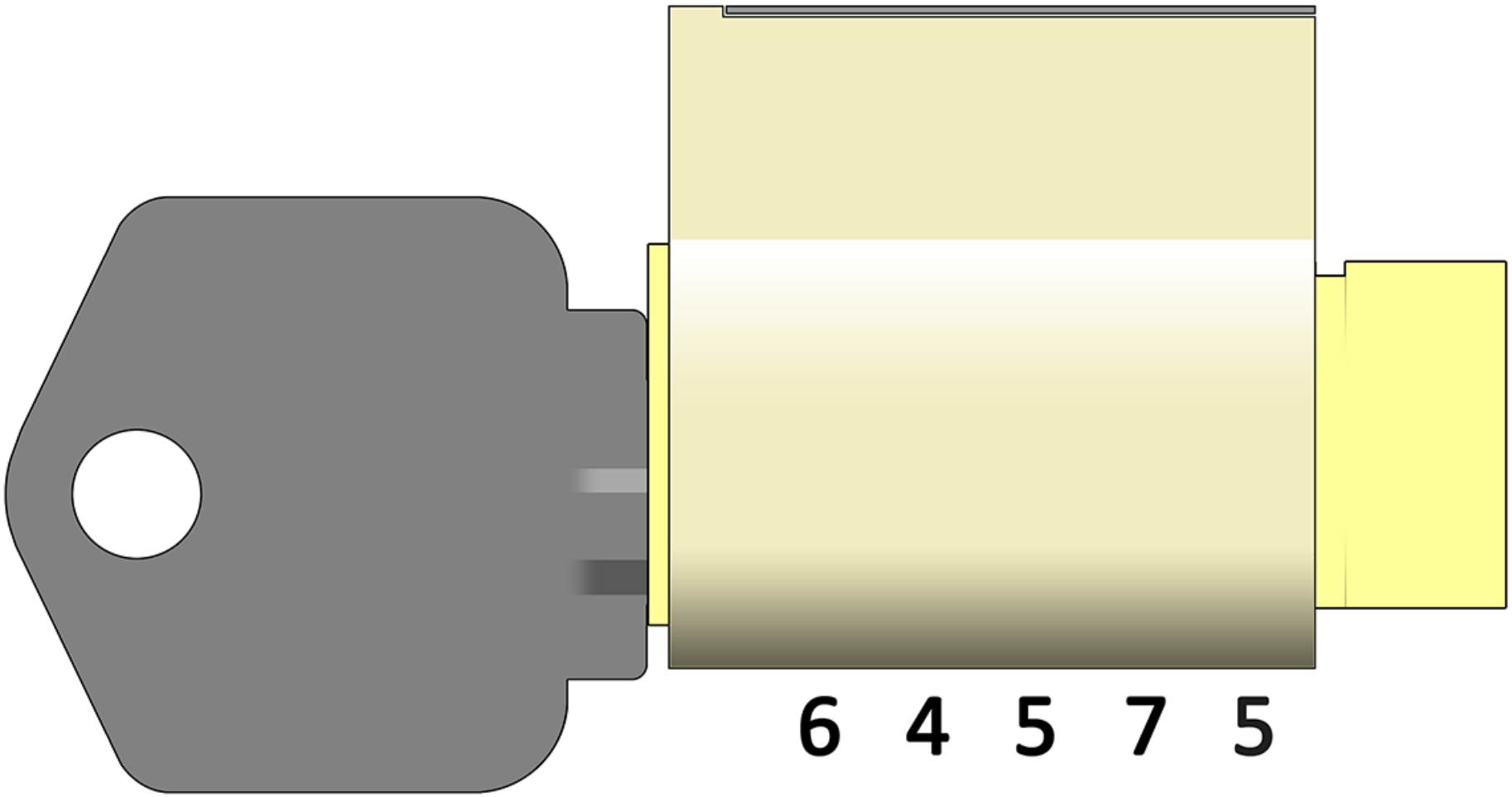
Remove the Key



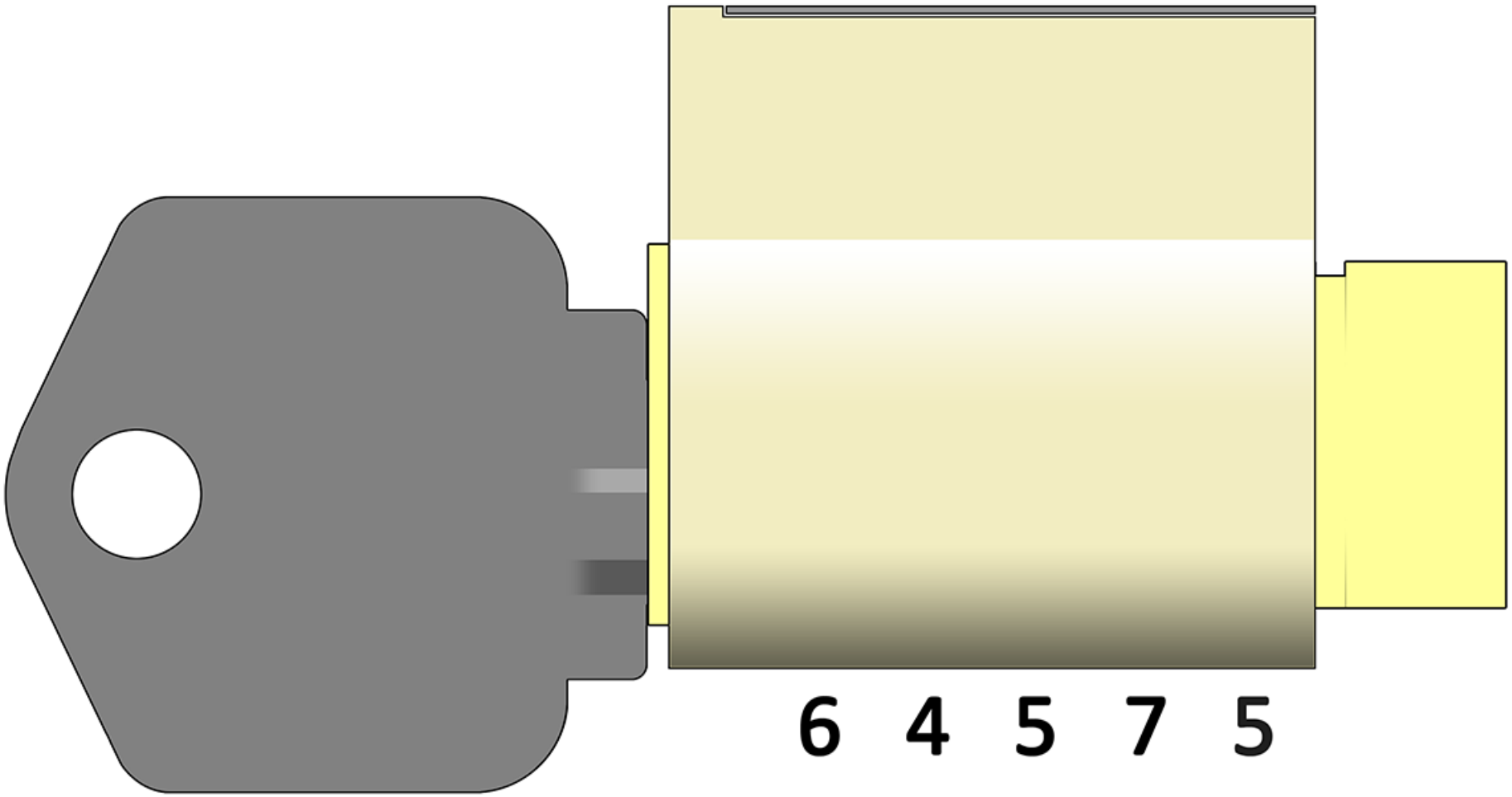
File Down to the Last Depth



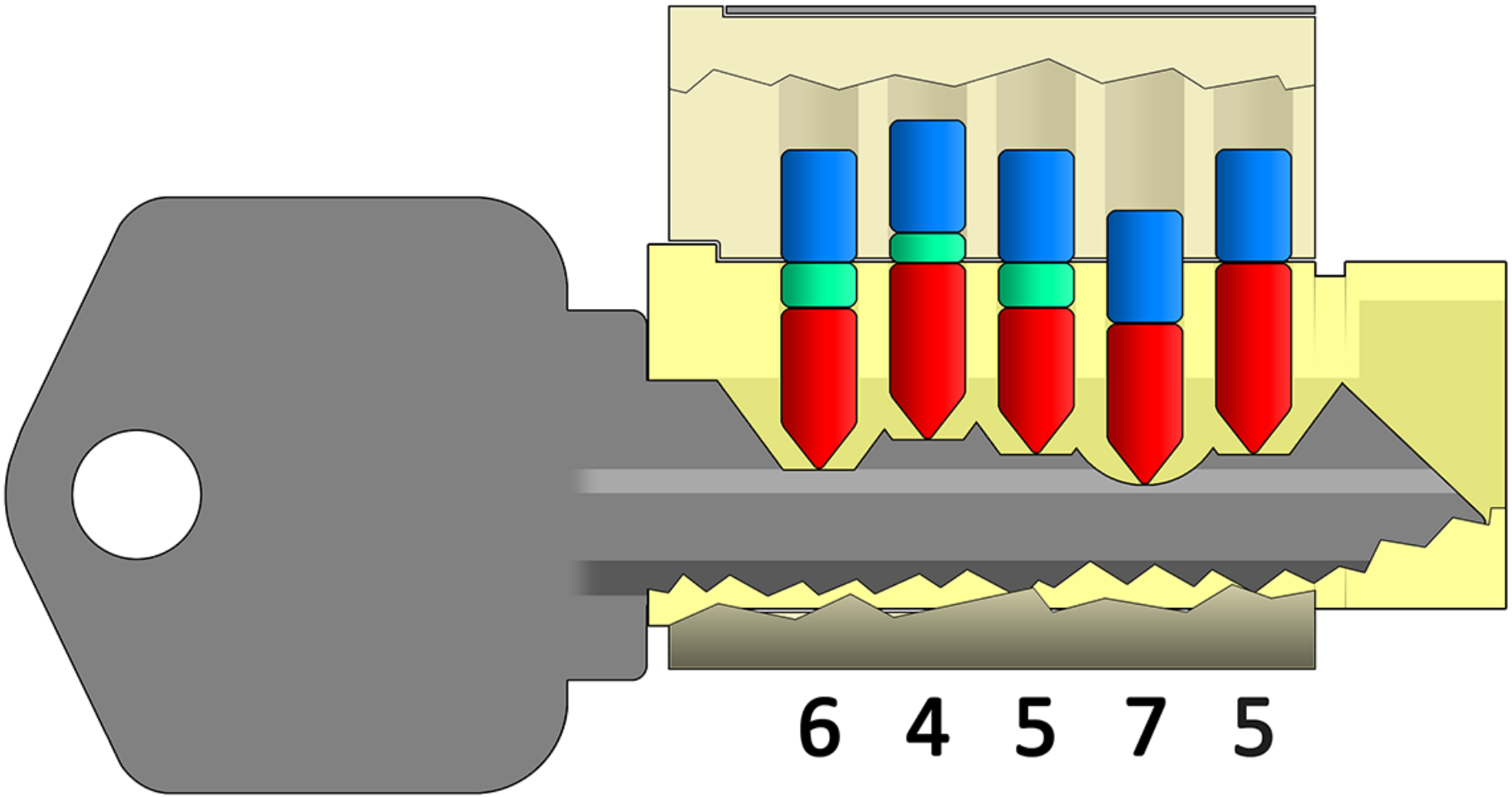
Try the Key…



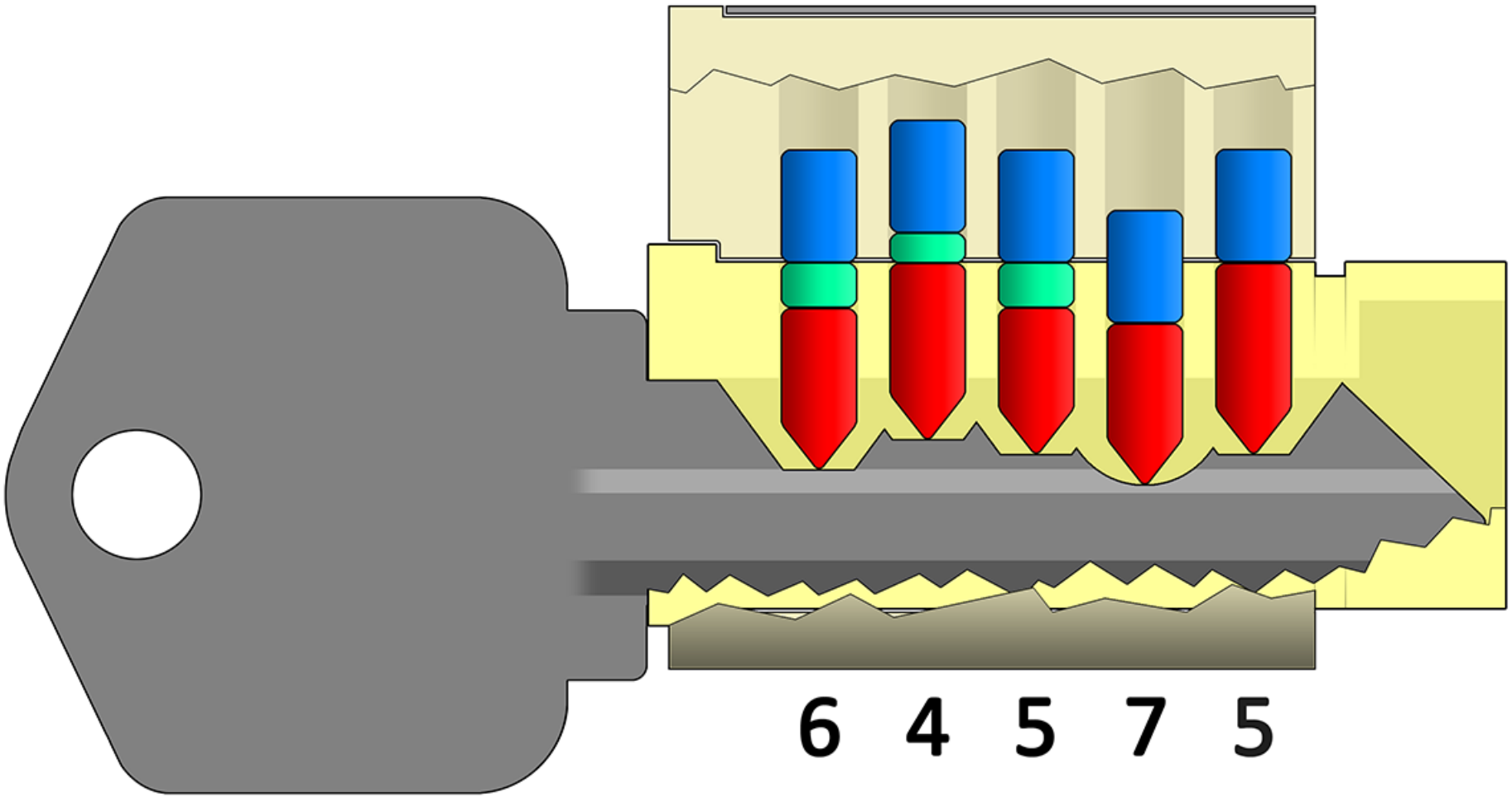
Try the Key… Nope.



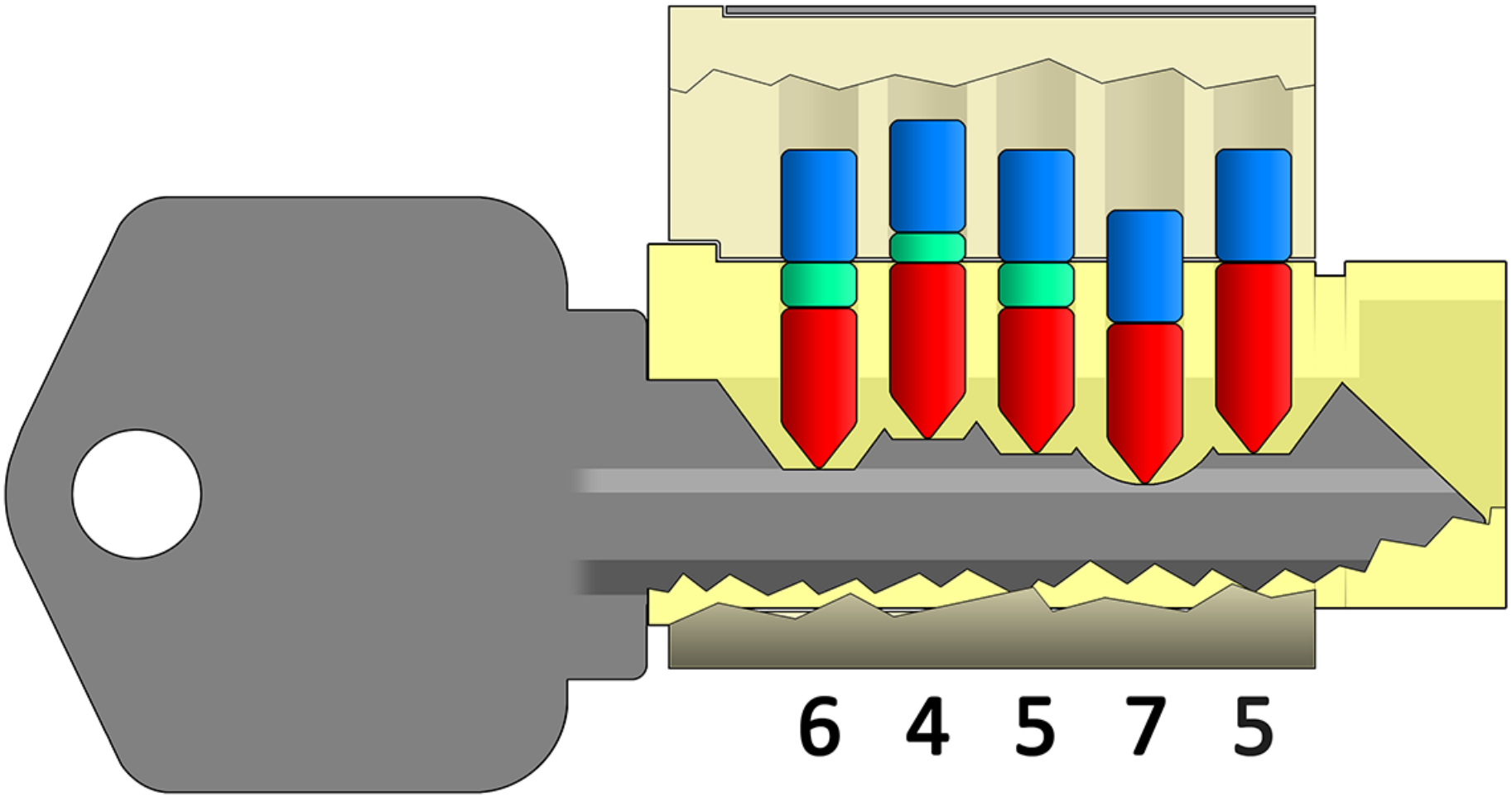
So, WTF ?



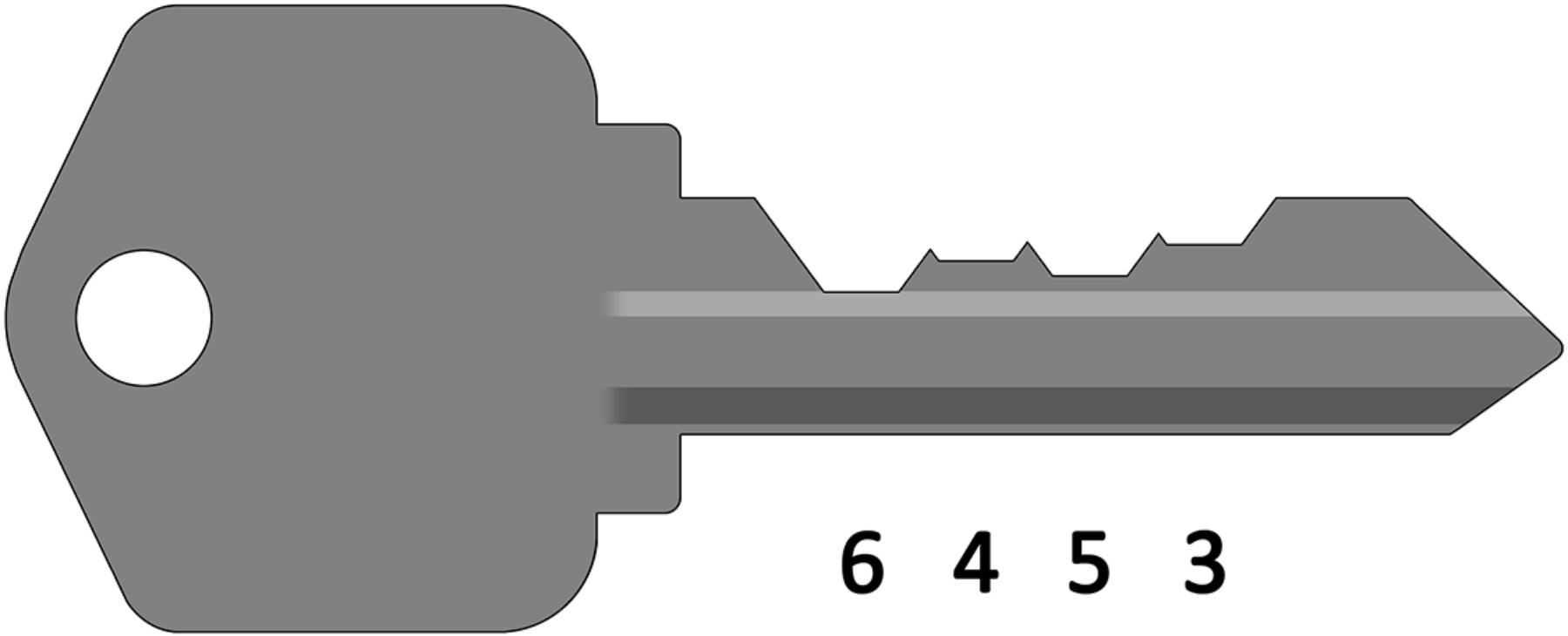
Maybe You Question Yourself



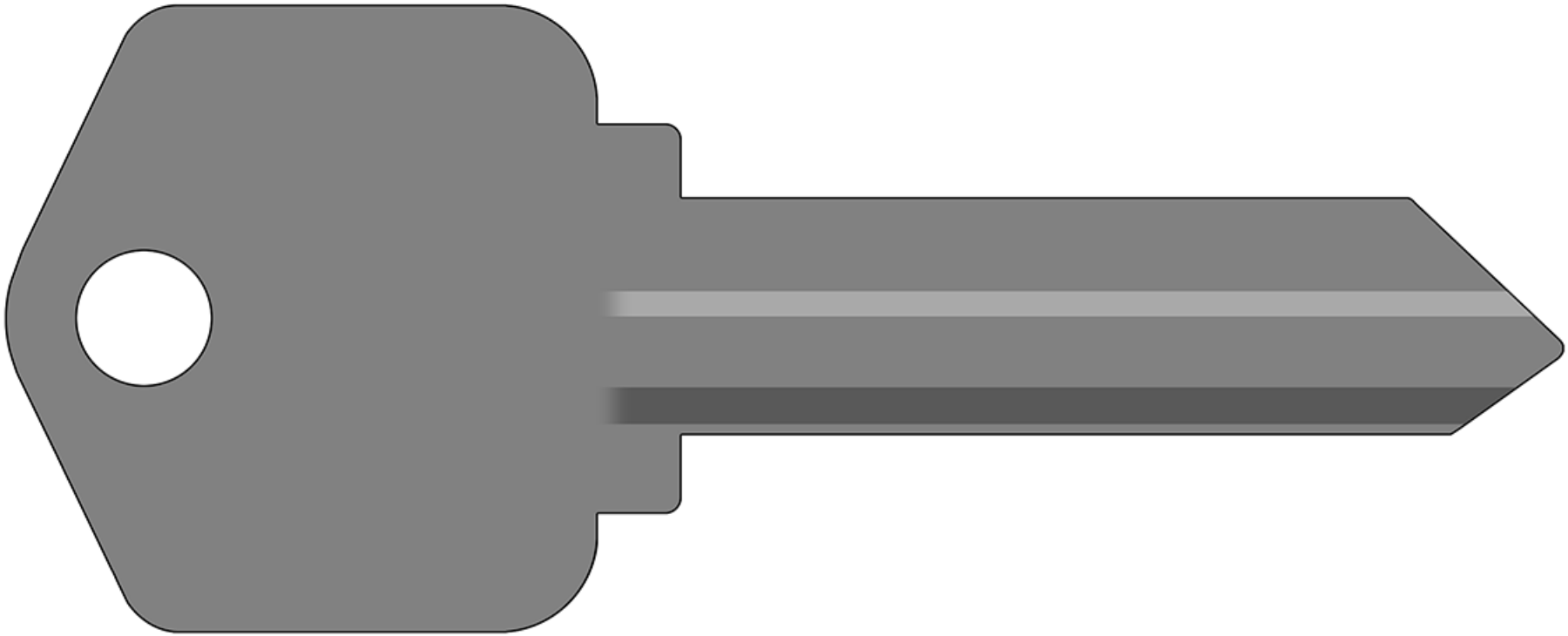
In This Case… Position Four is



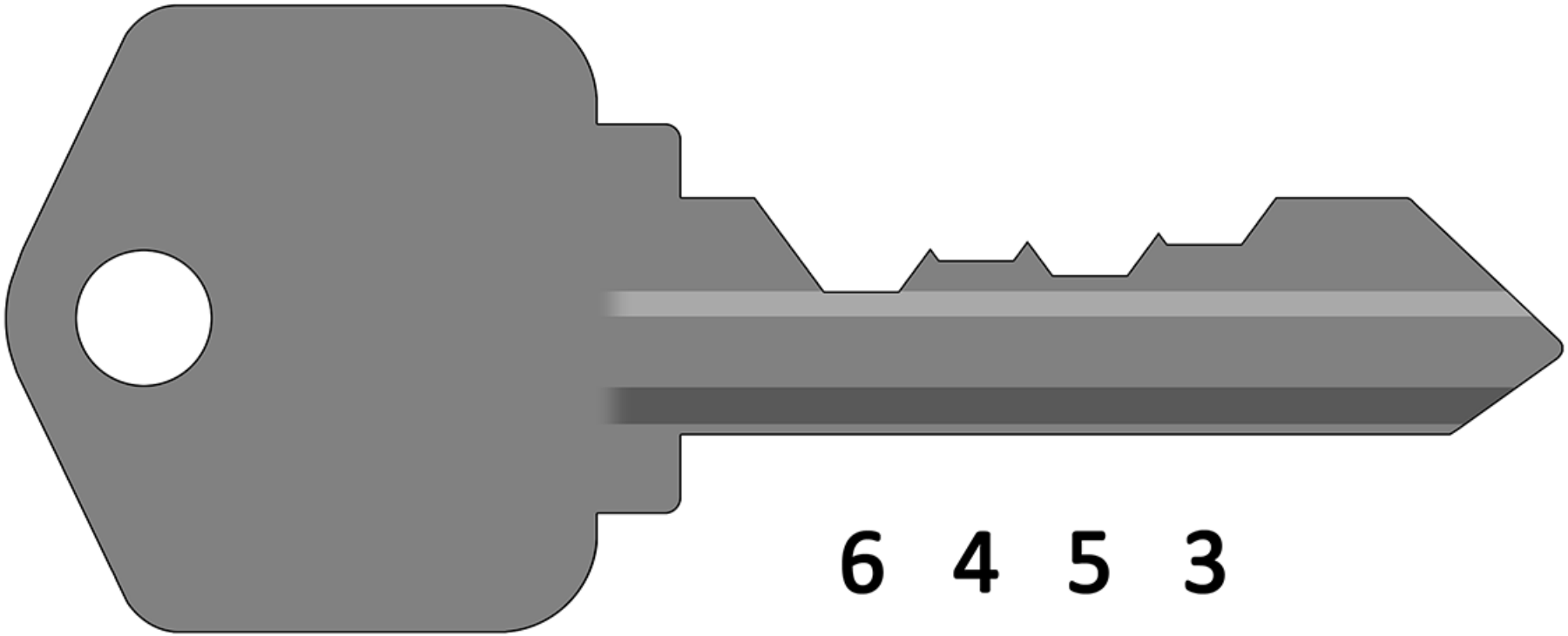
The Master Key We've Decoded Thus –



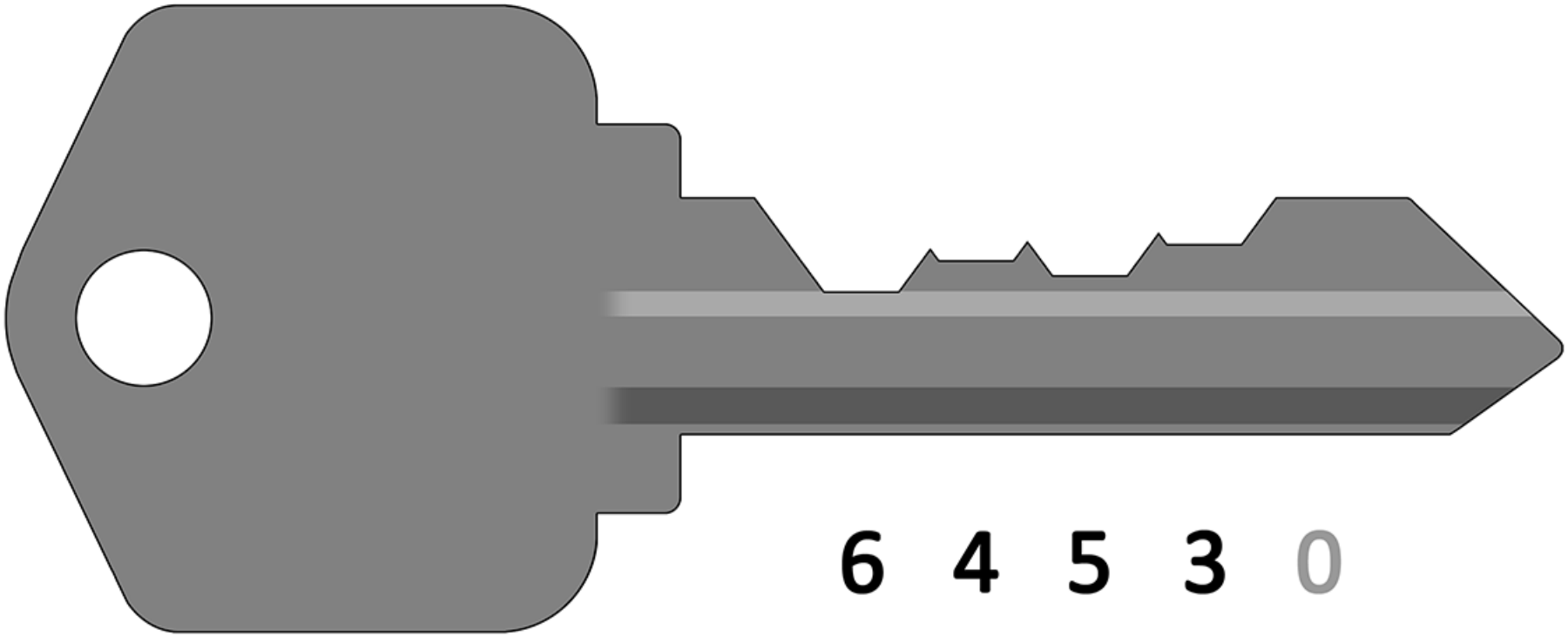
Let's Prepare a Fifth (and



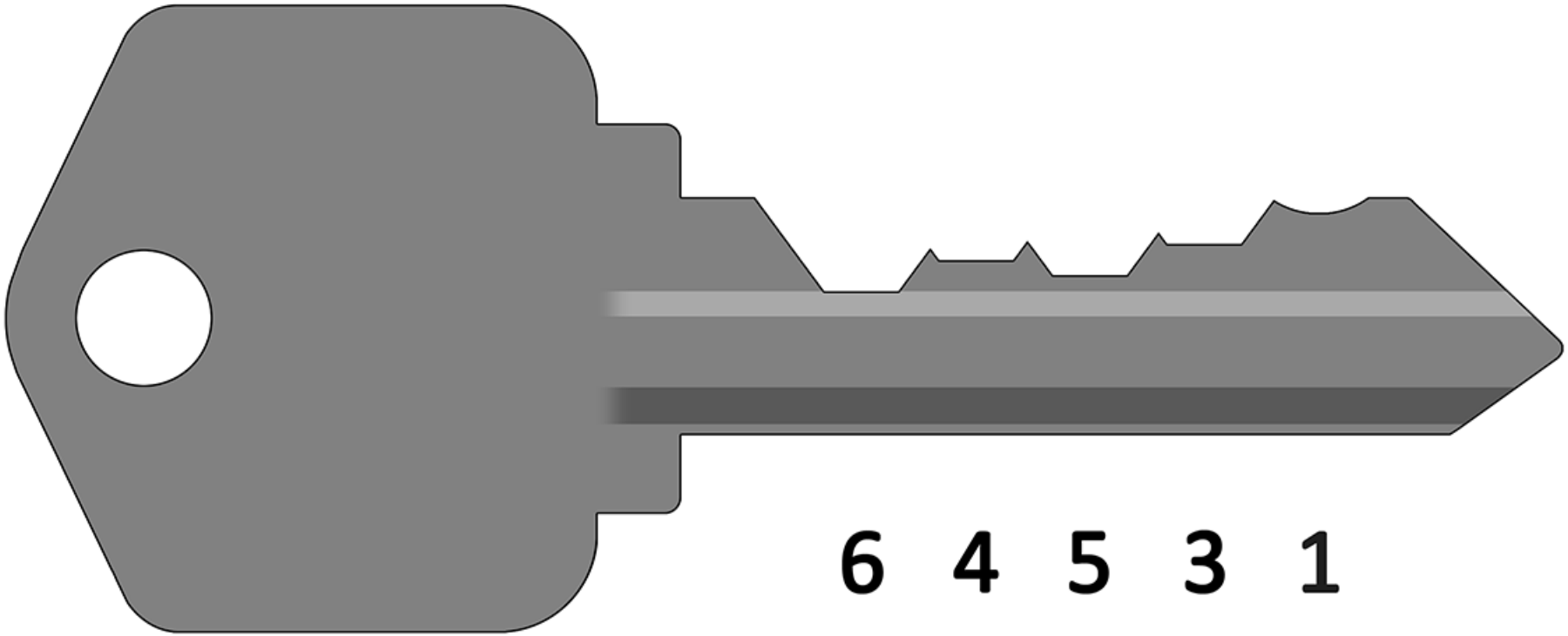
Code-Cut the Mastering We've



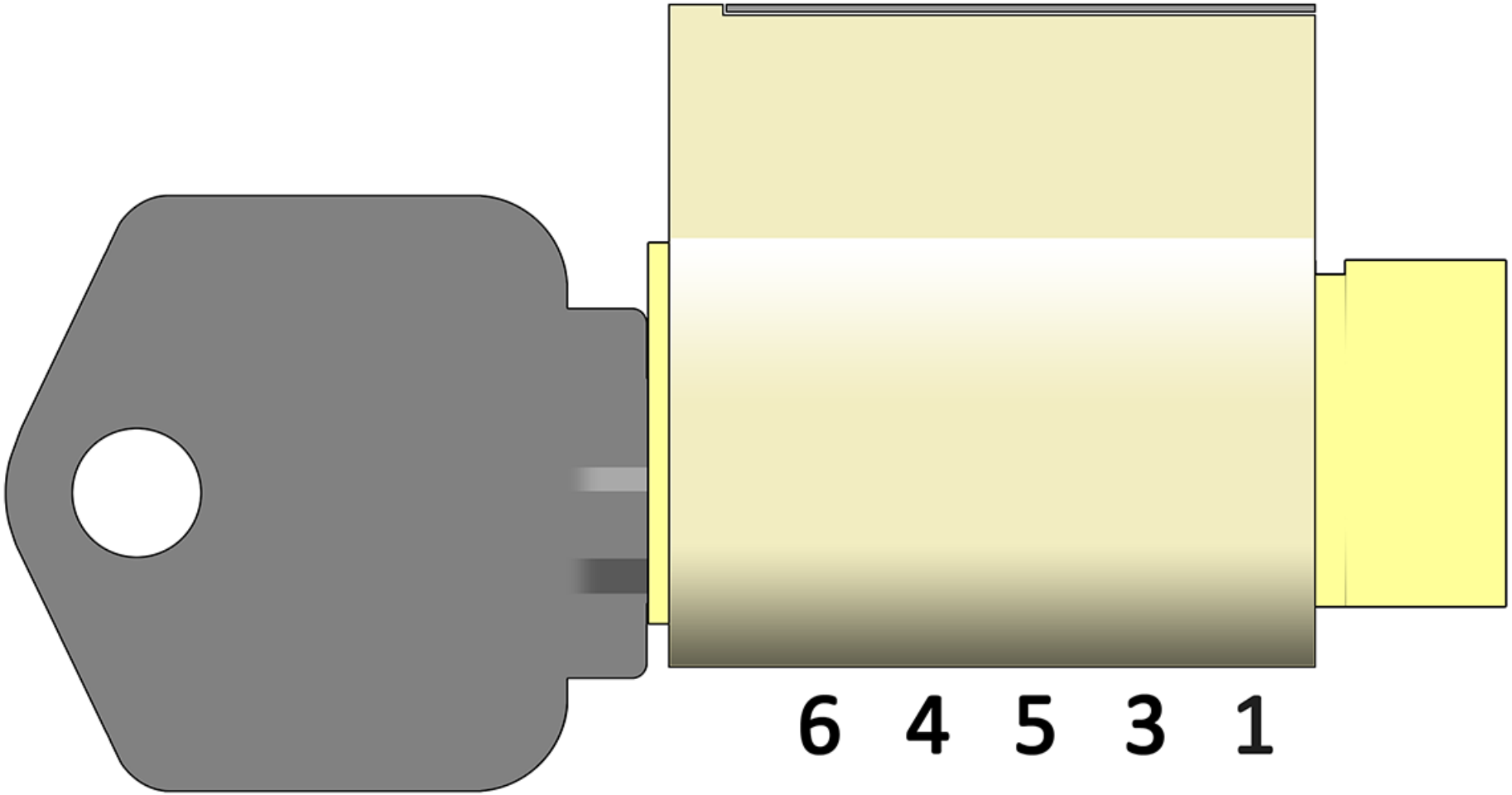
Leaving the Fifth Position Free



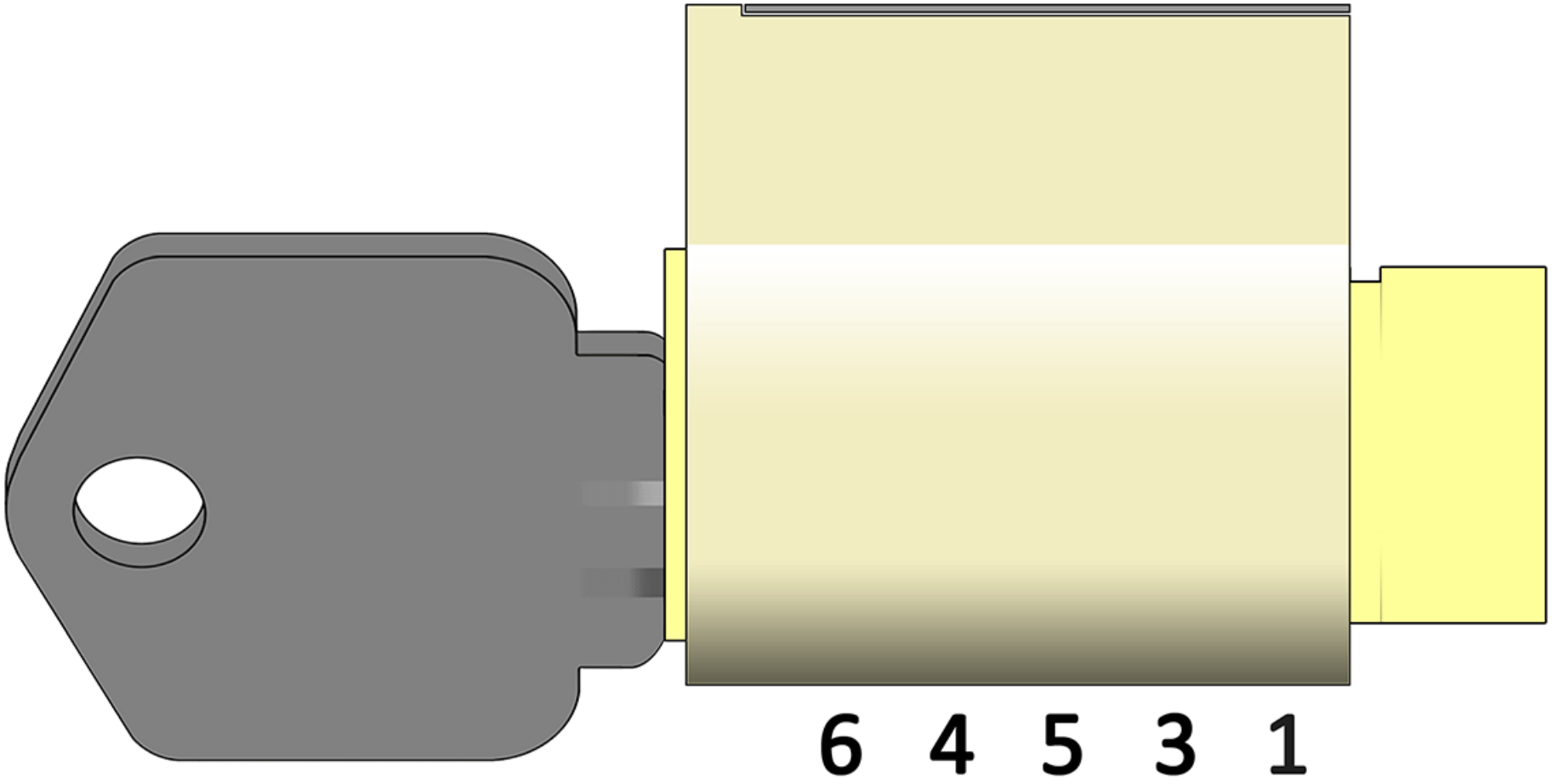
Attempt Either at the Blank



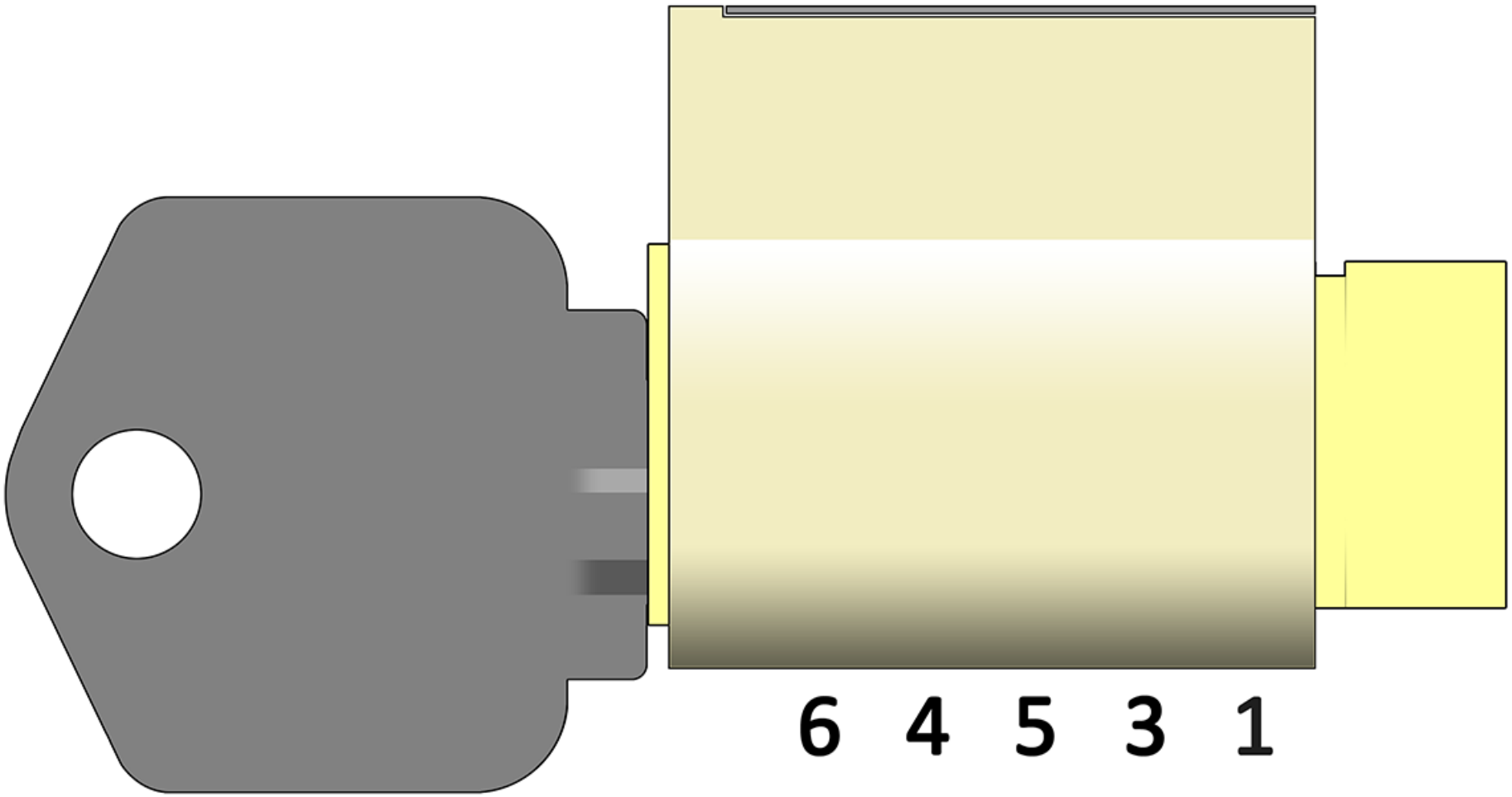
Try the Key…



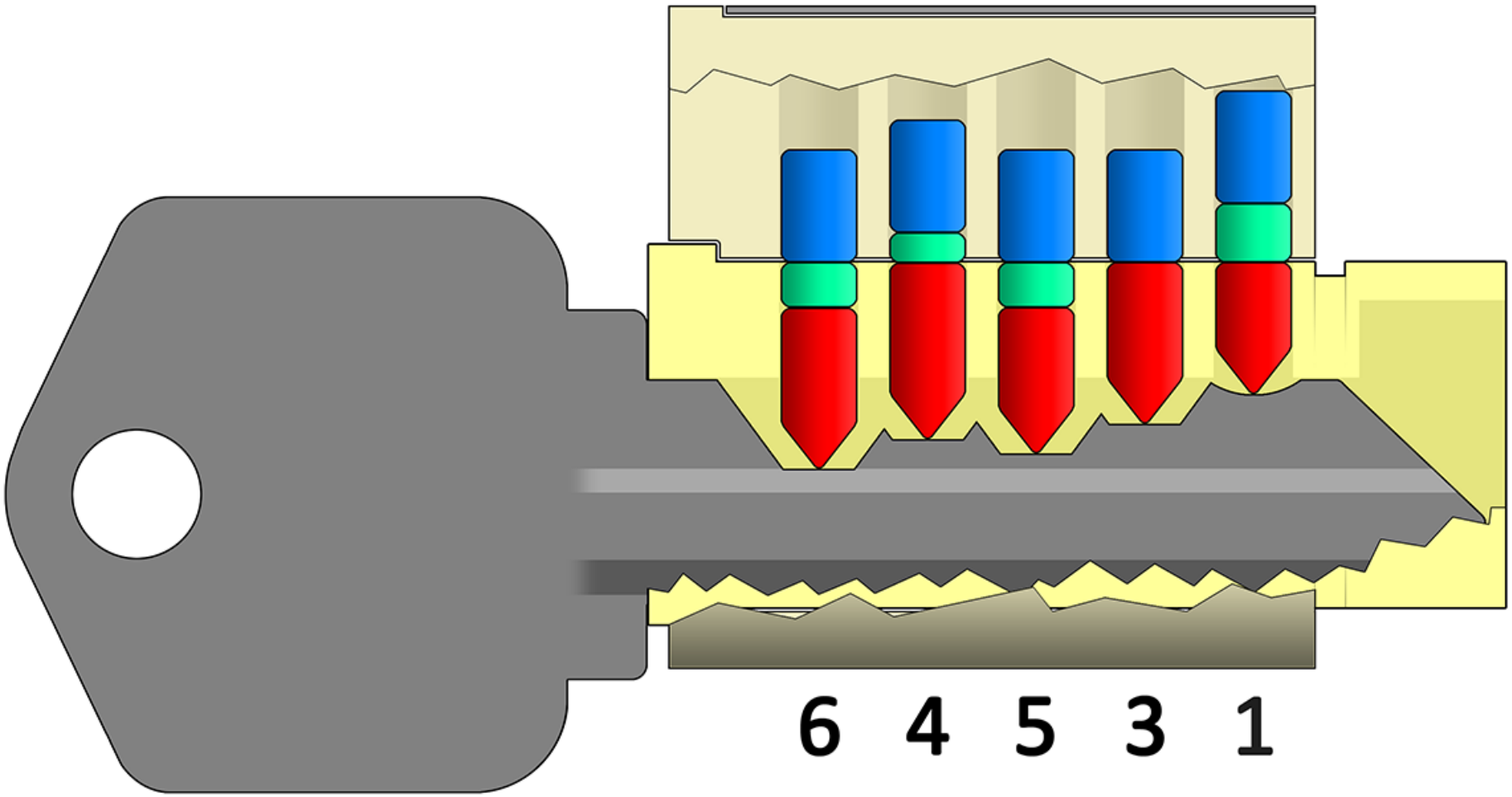
Try the Key… OPEN!



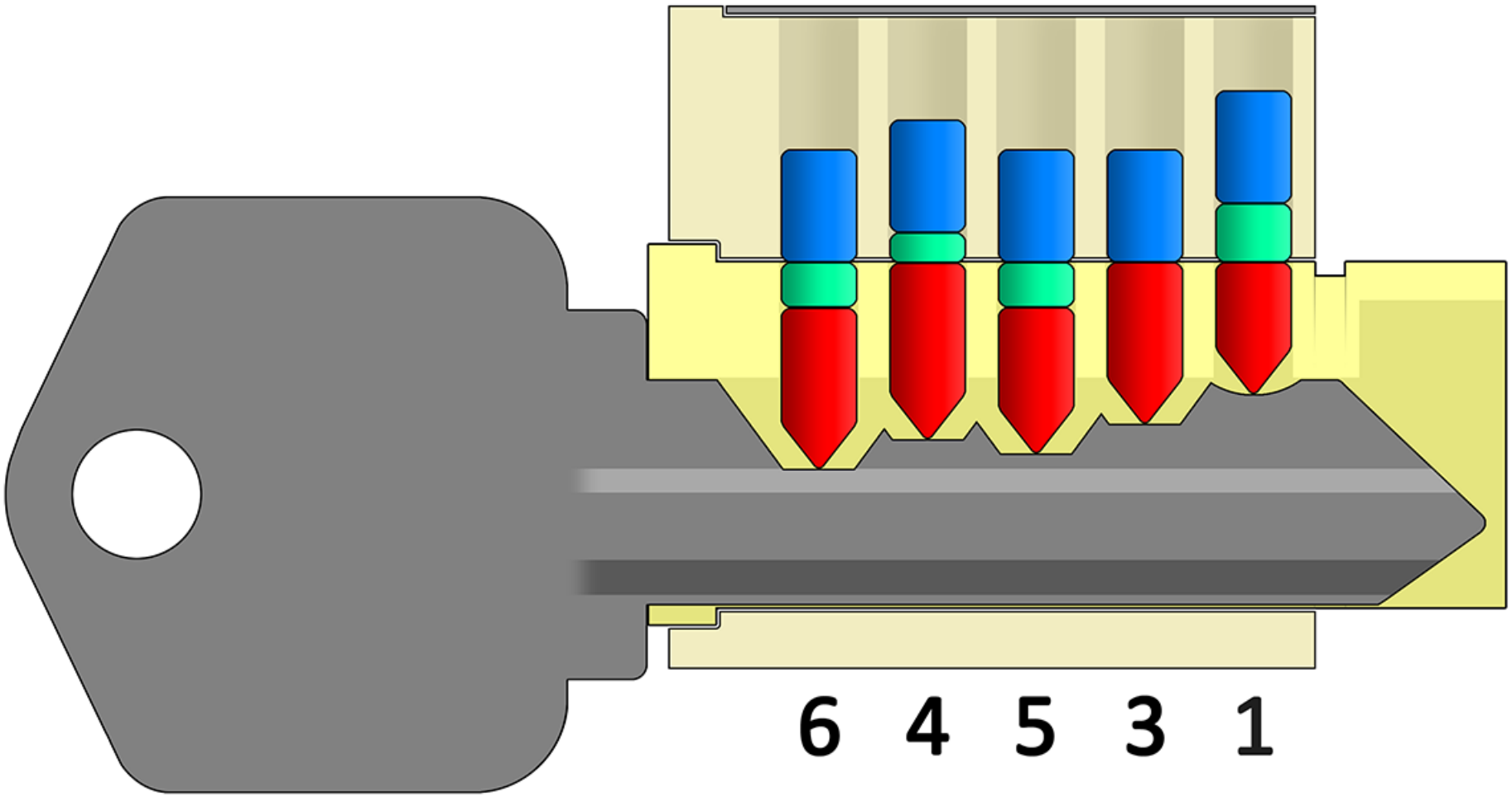
That's a Heaping Bowl of



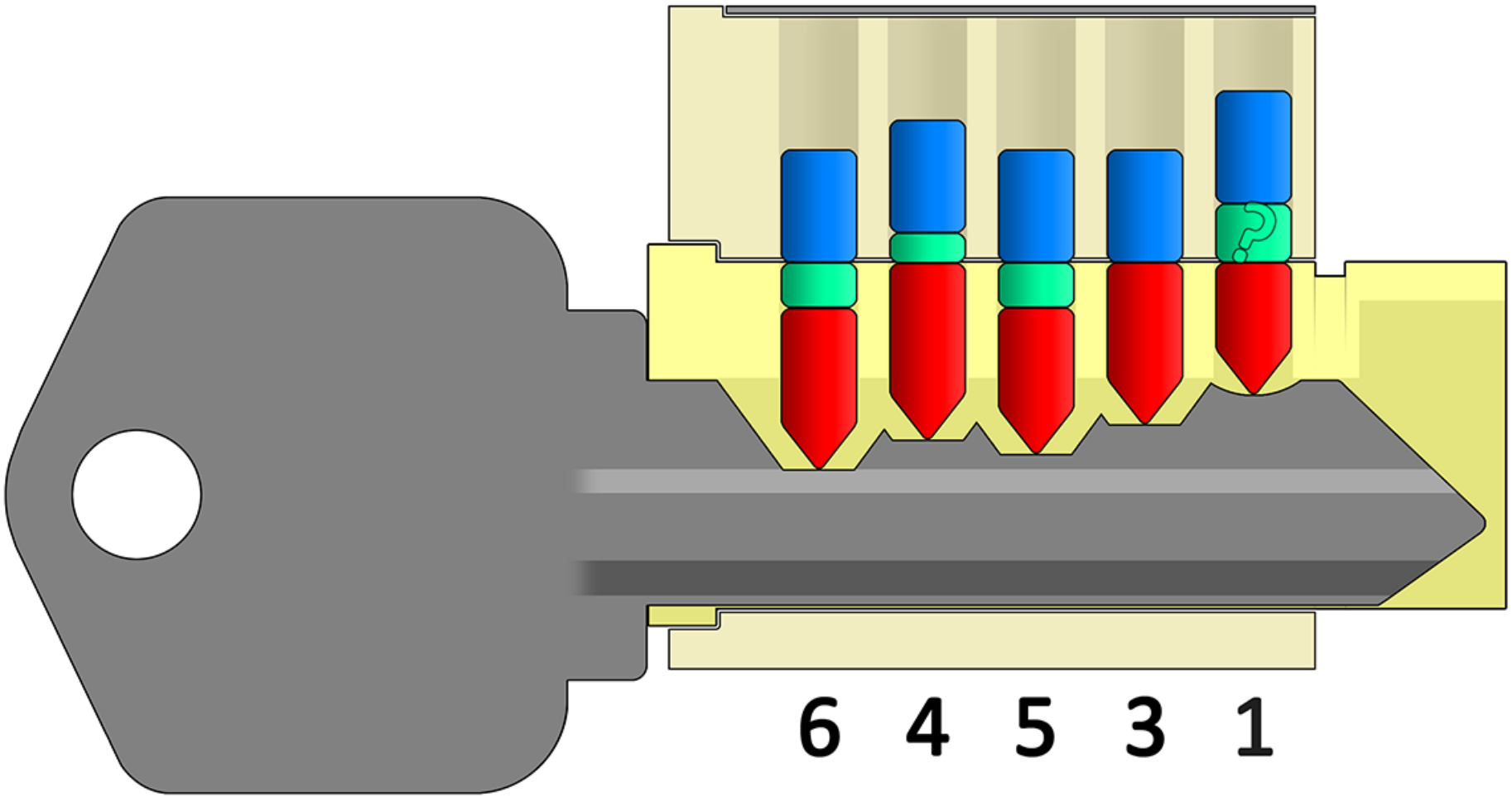
There's a Very Real Chance We



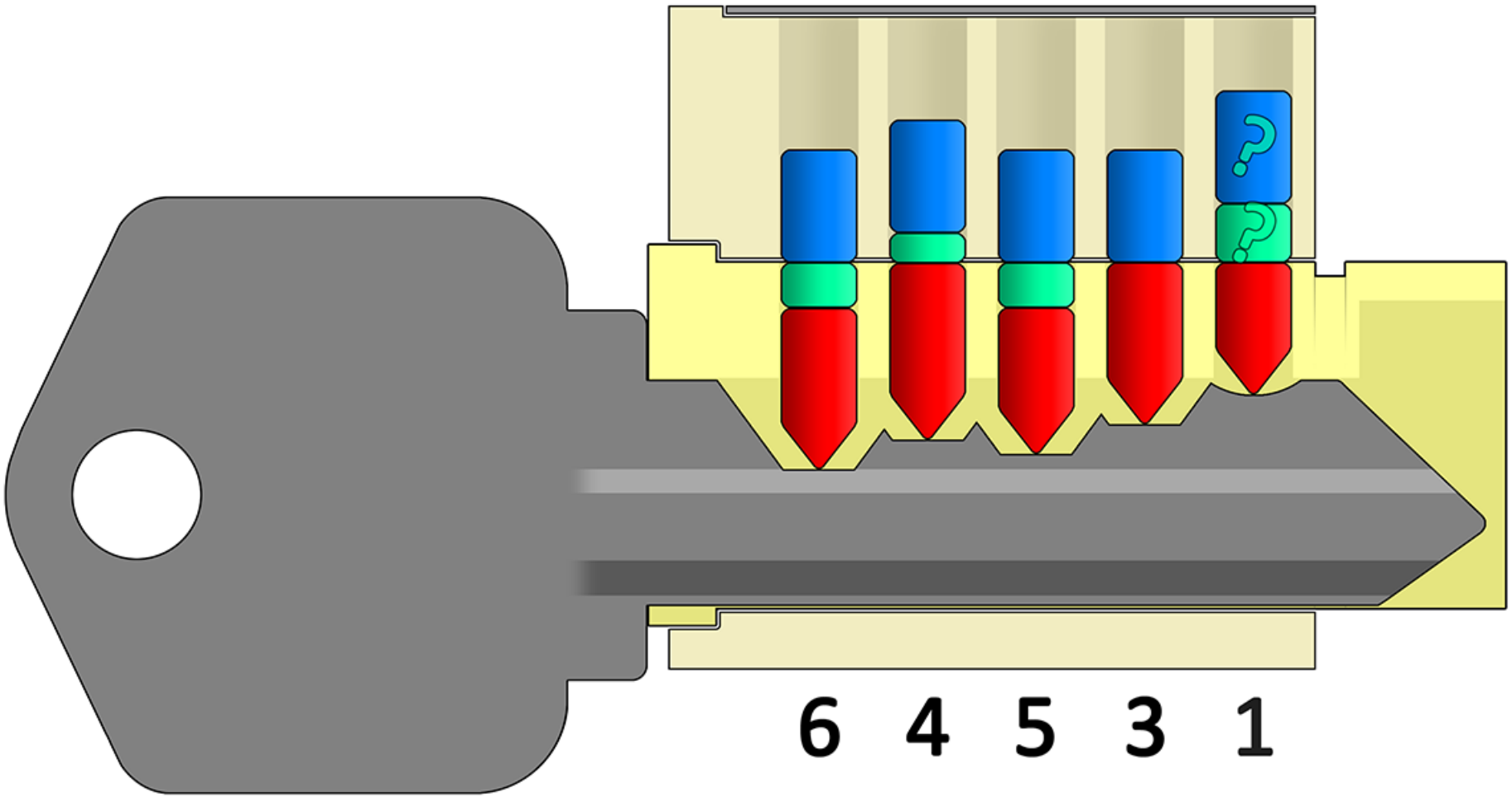
The Mastering Might be Fully



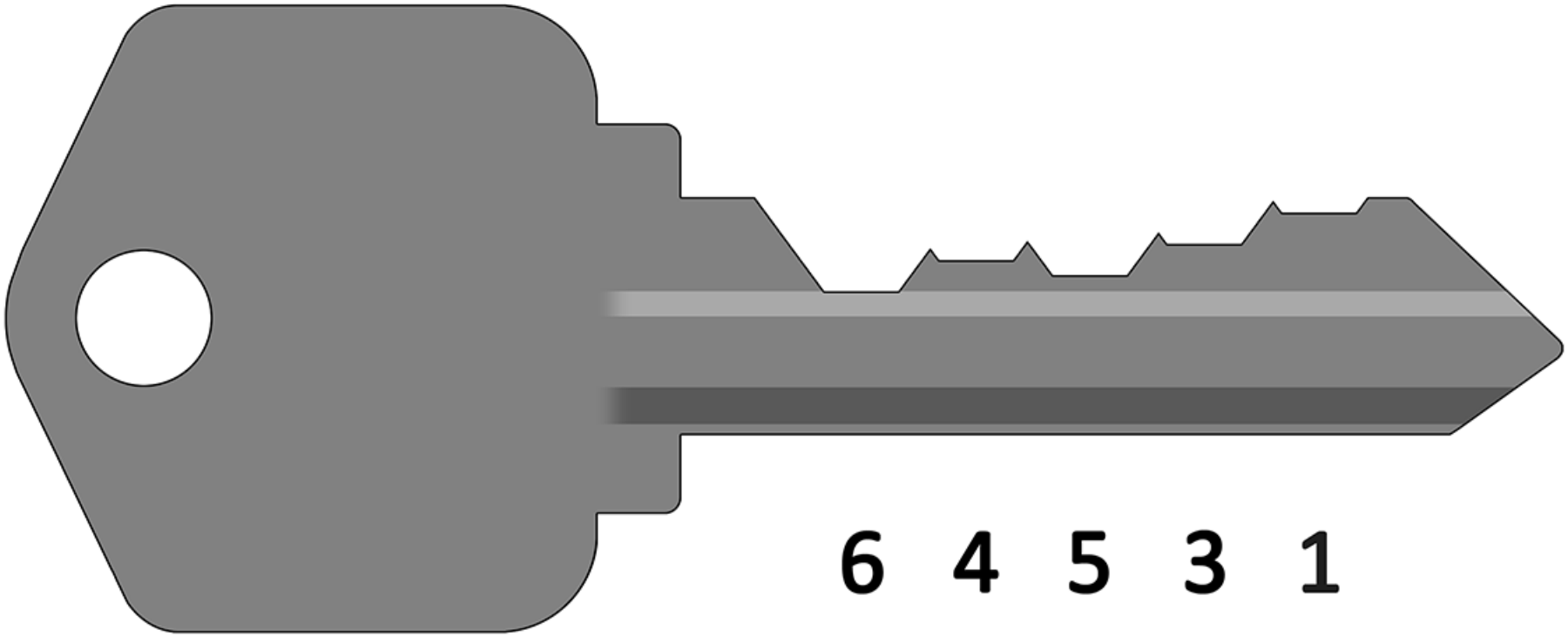
True, There *Could* be Another Cut ..



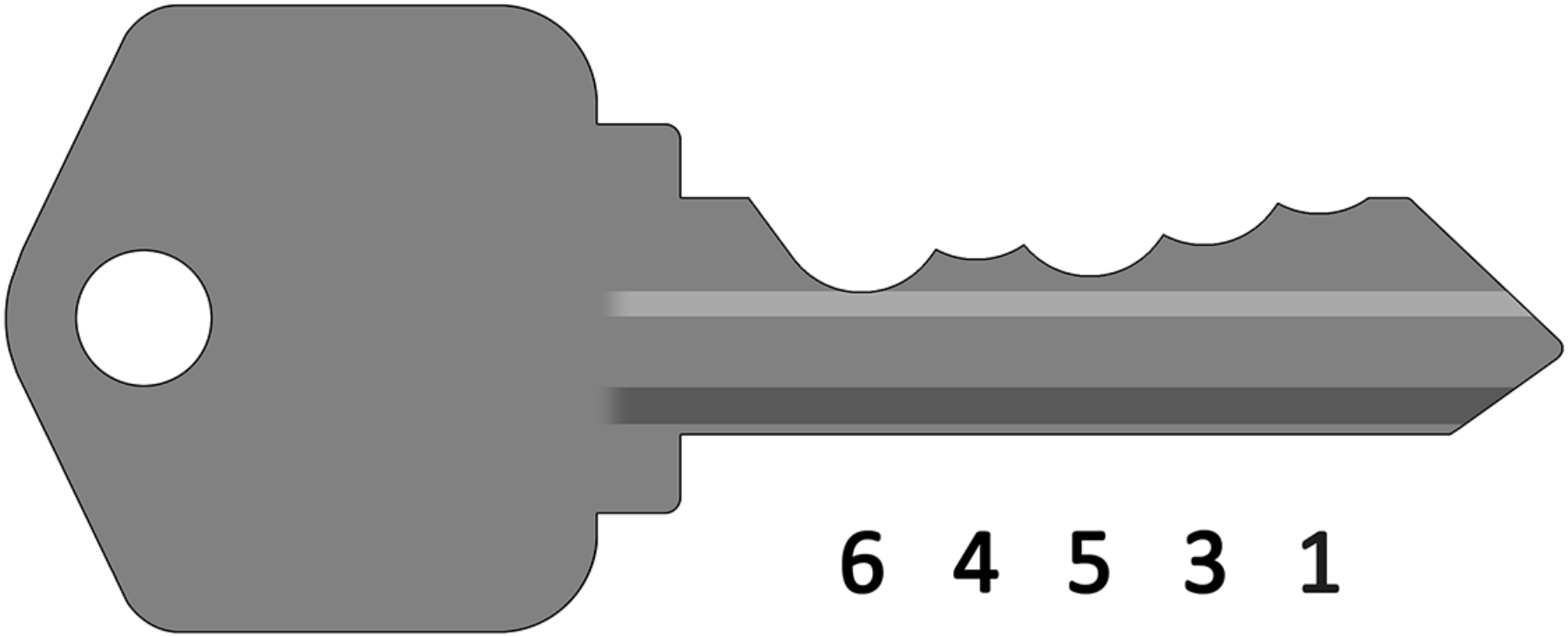
There Could Even be Other Cuts



But Personally, I'd Just Start

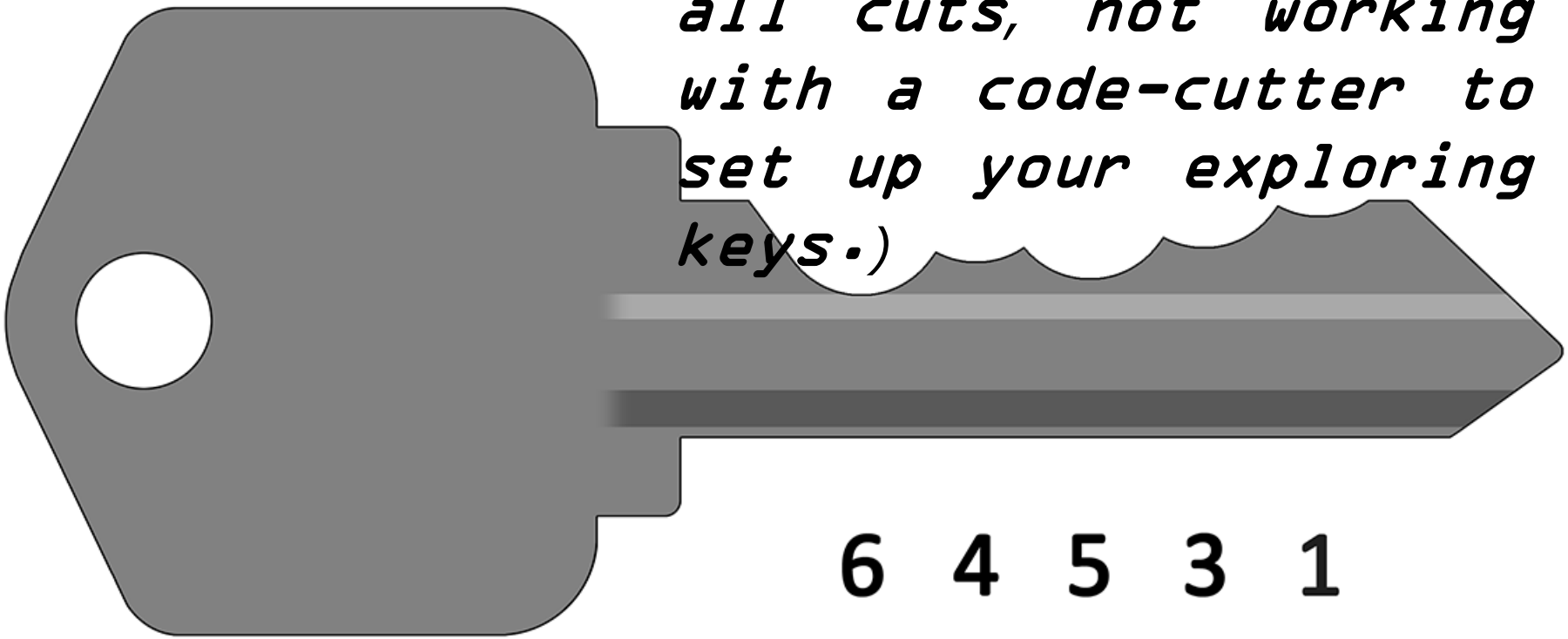


Of Course, *Your* Key Will Likely

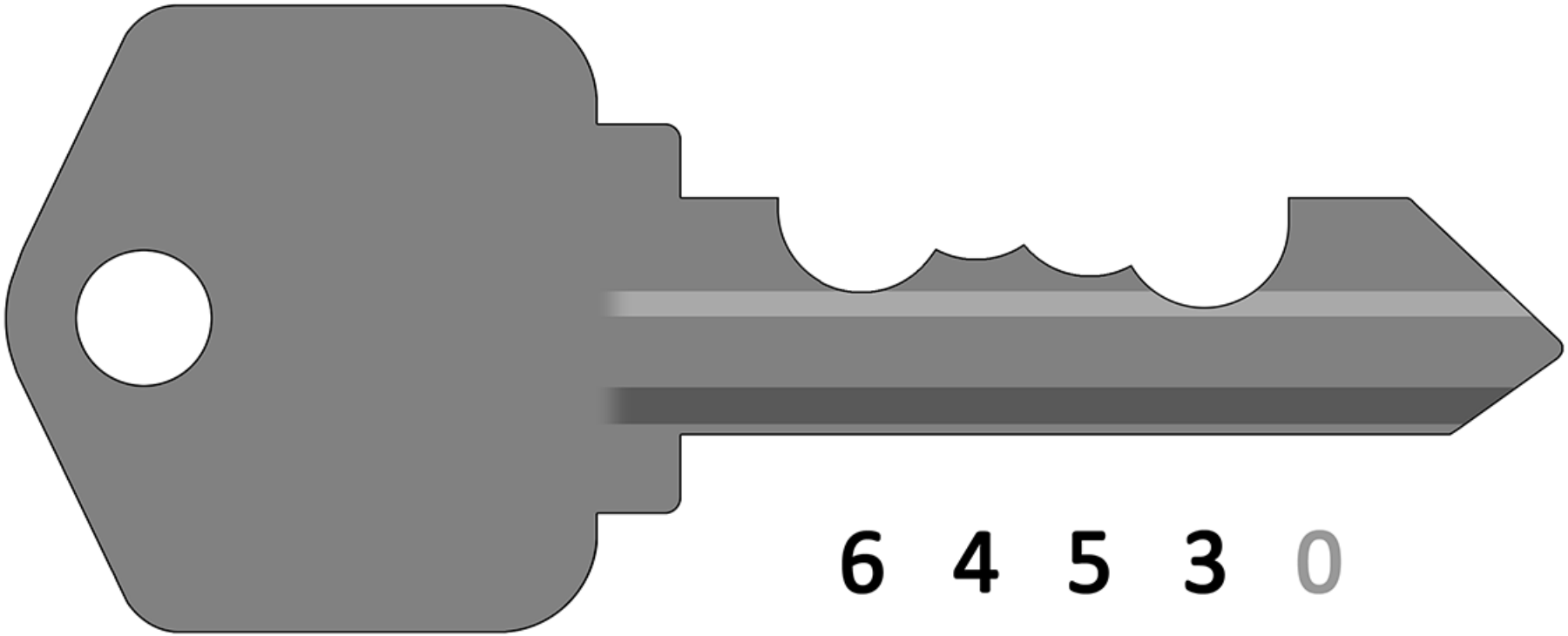


Of Course, *Your* Key Will Likely

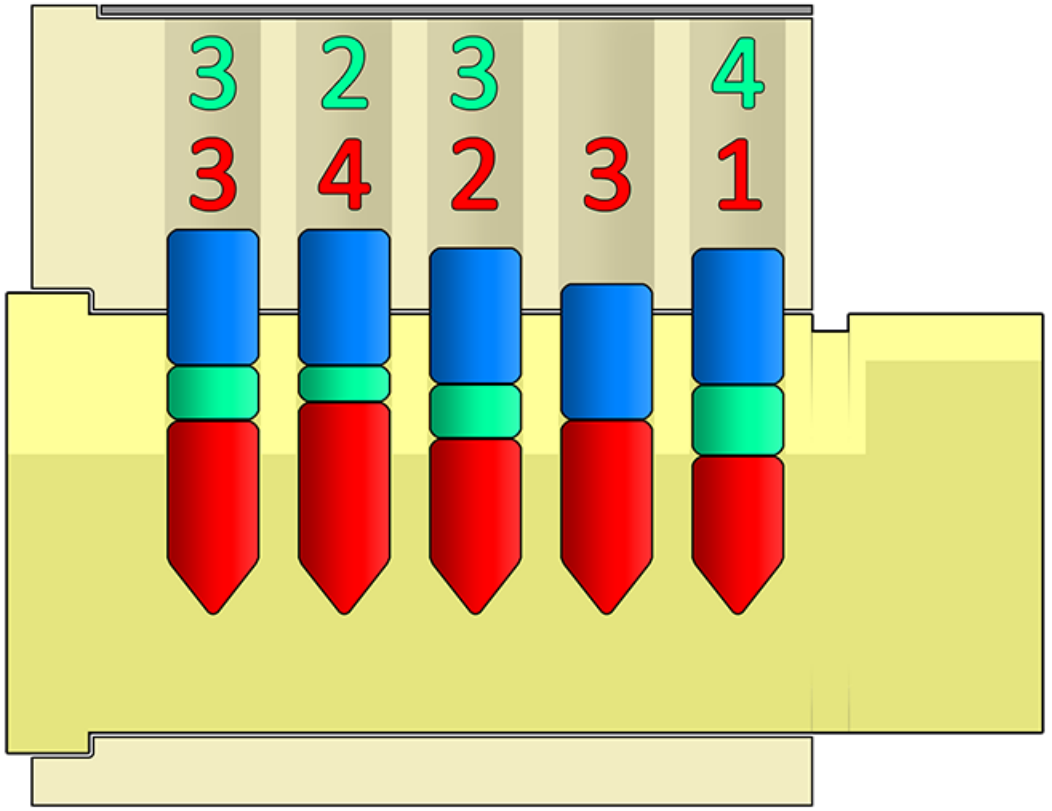
(Since most likely you will be hand-filing all cuts, not working with a code-cutter to set up your exploring keys.)



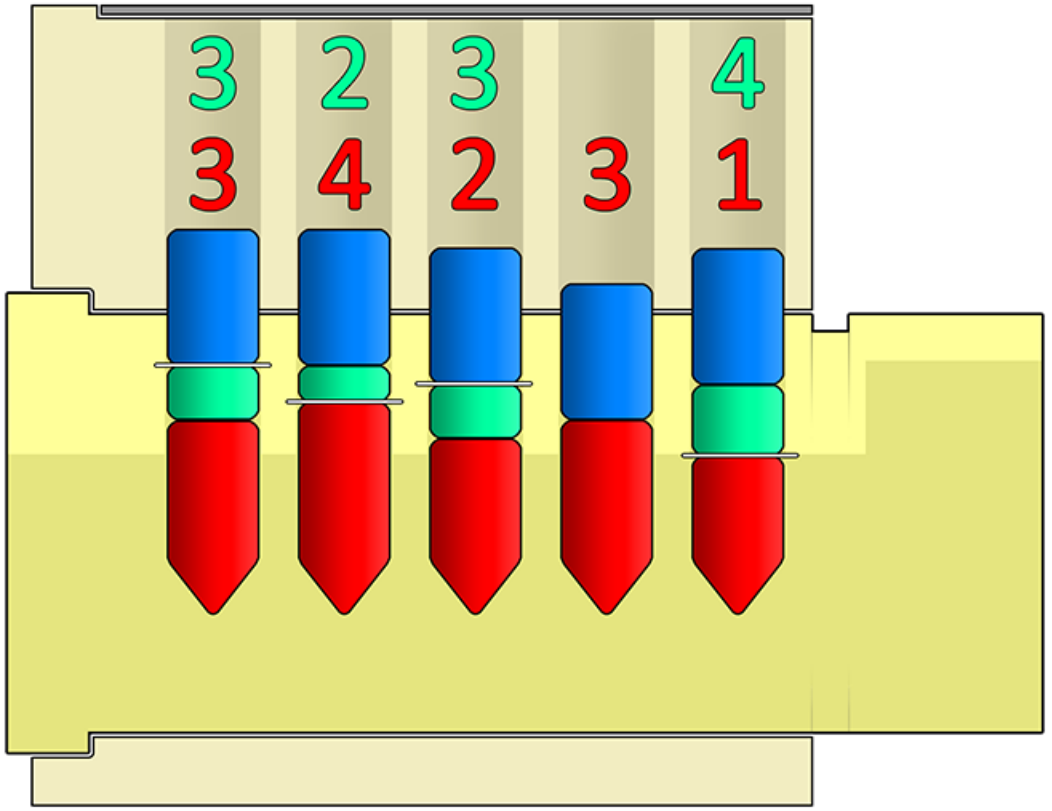
Speaking of Hand-Filed Keys…



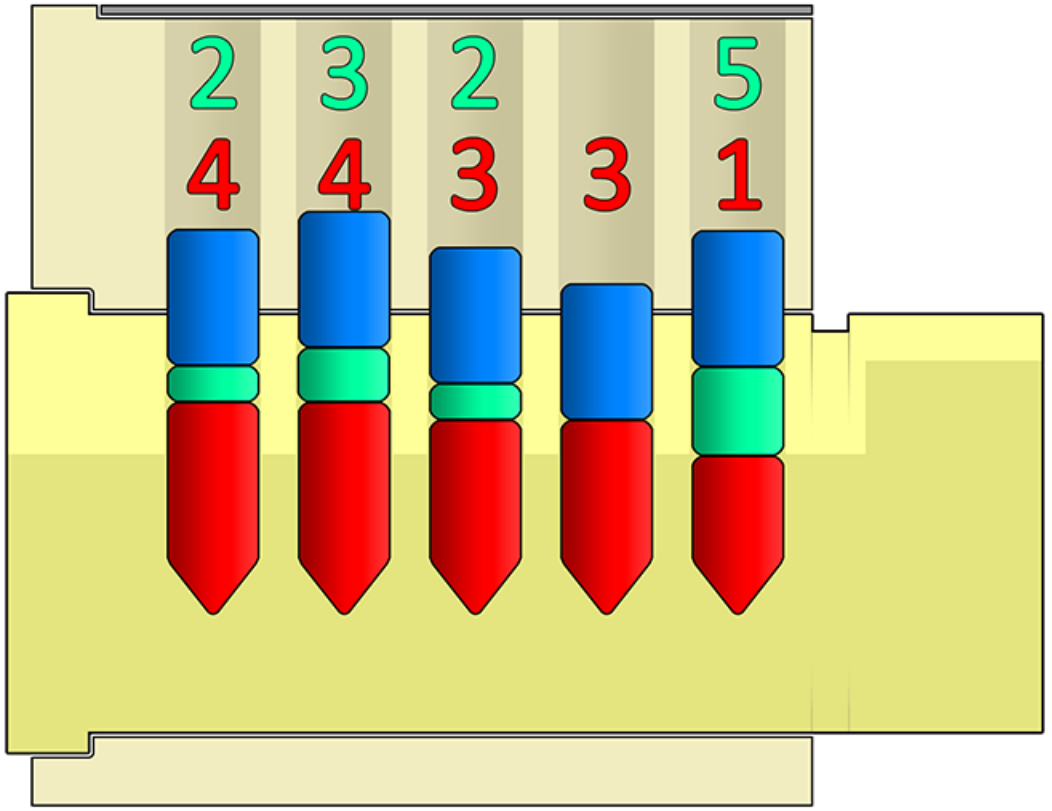
The Internals of our Original



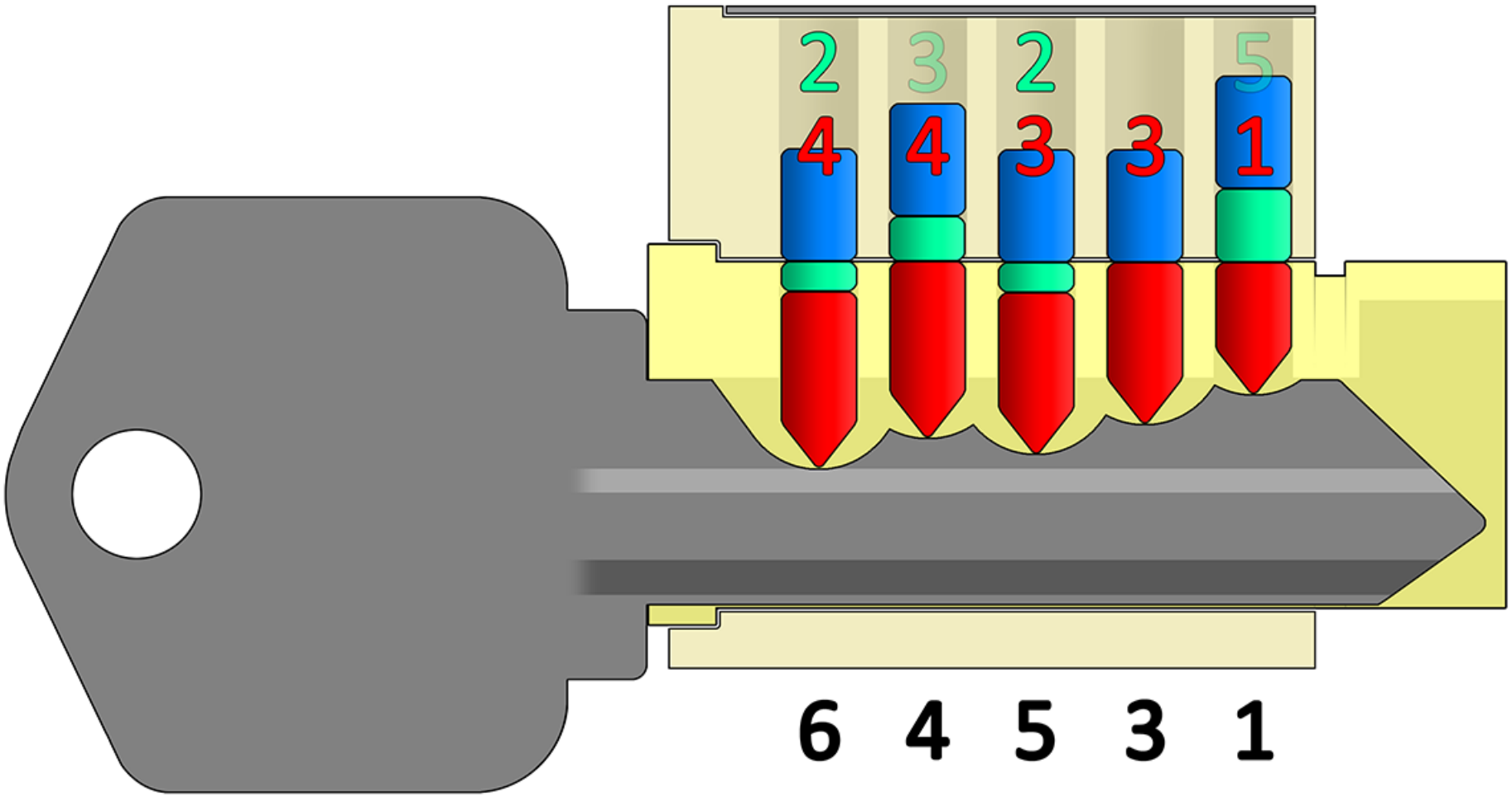
These Marks Represent the



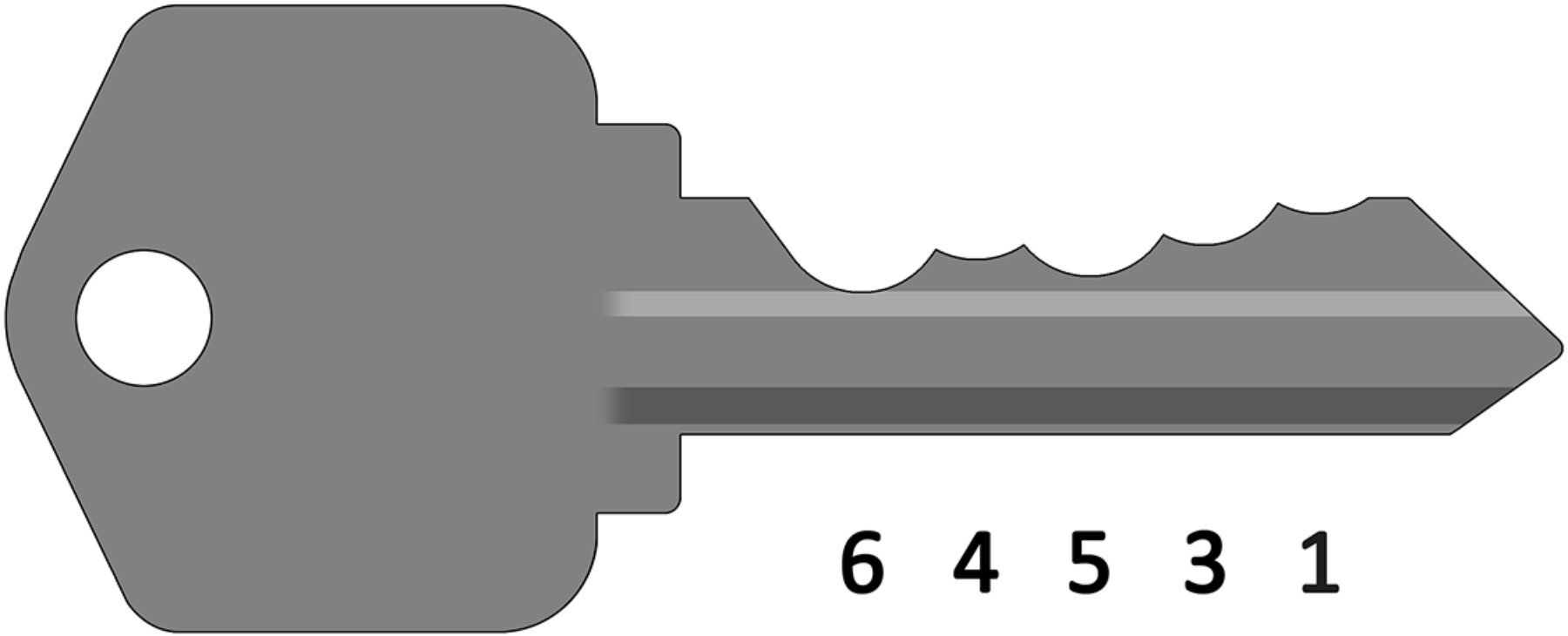
Here's a Hypothetical Alternate



Our Decoded Master Key Would



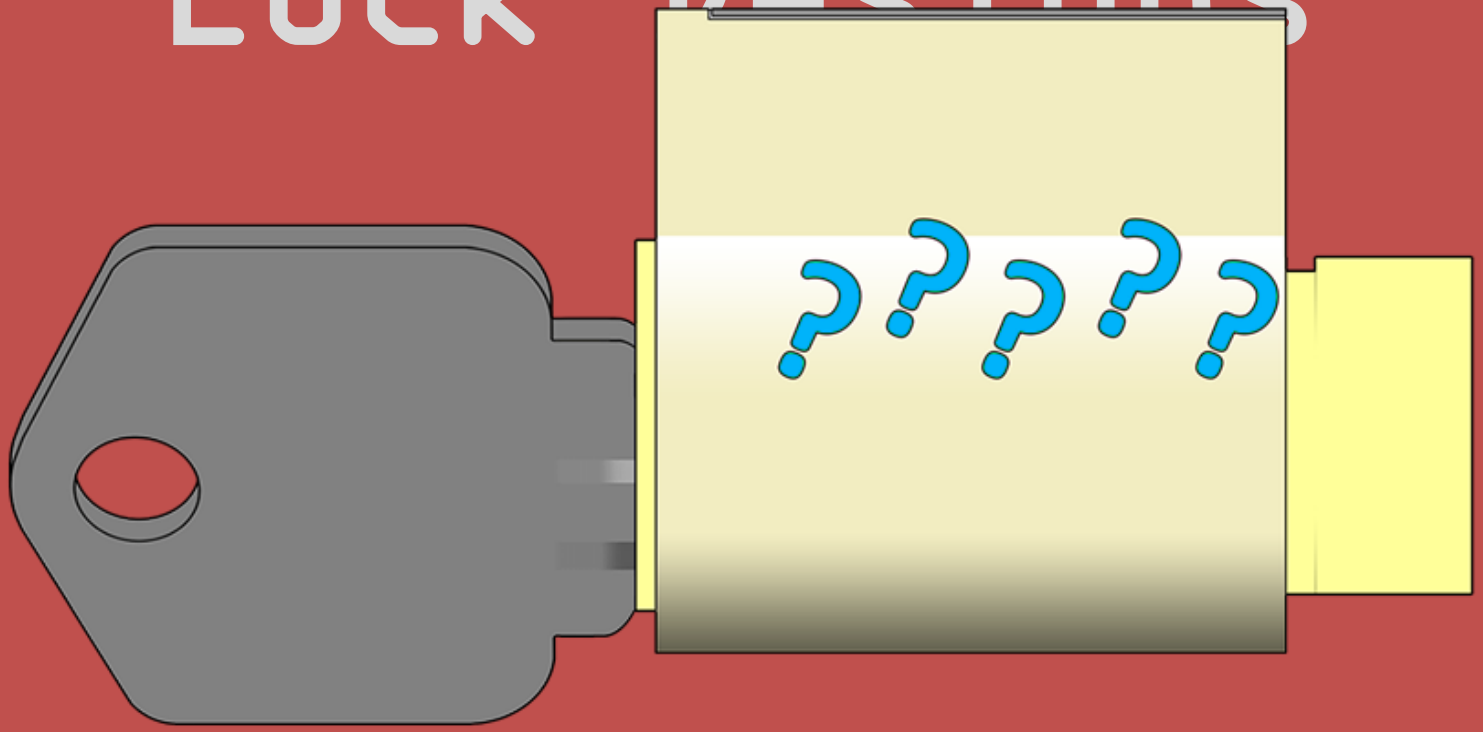
A Winnar is You!



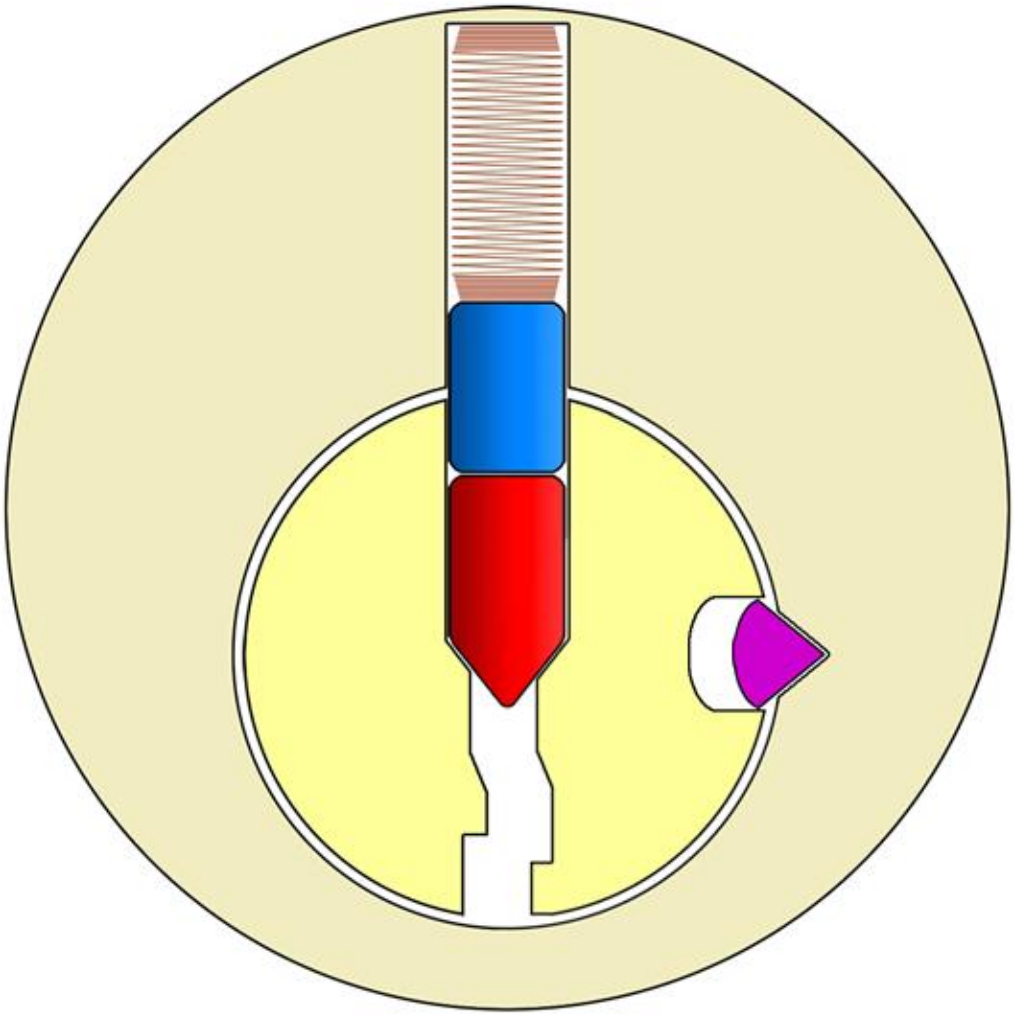
Mitigating Against This Attack?

- Restricted Keyway / Restricted Blanks
- Secondary Monitoring Systems
- Audit Trails / Access Control Scheduling
- Use Entirely Separate Zone Arrangements
- Move Away From Tumbler System

Other Badass Lock Designs

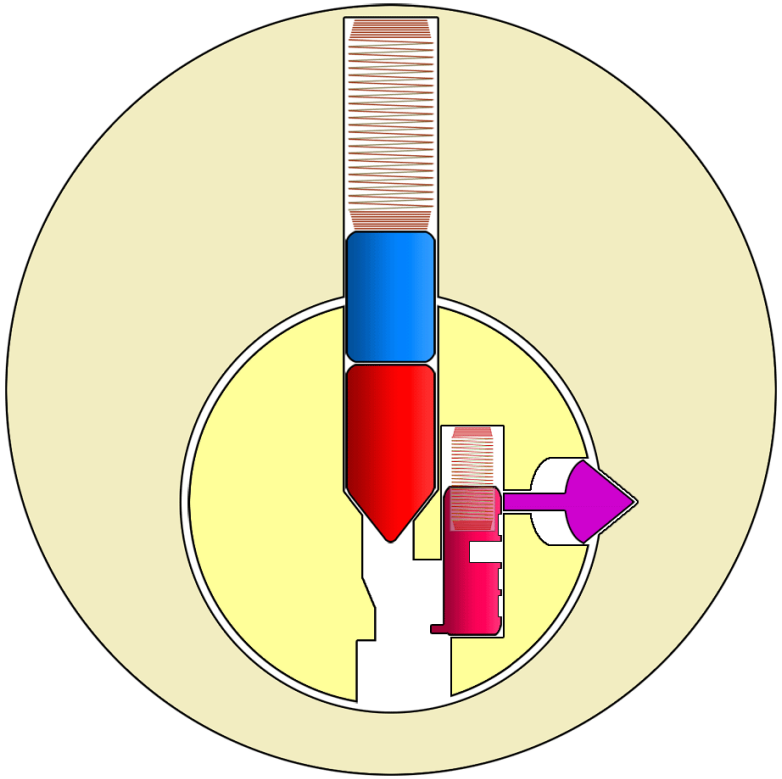


High Security Locks - Side Bar



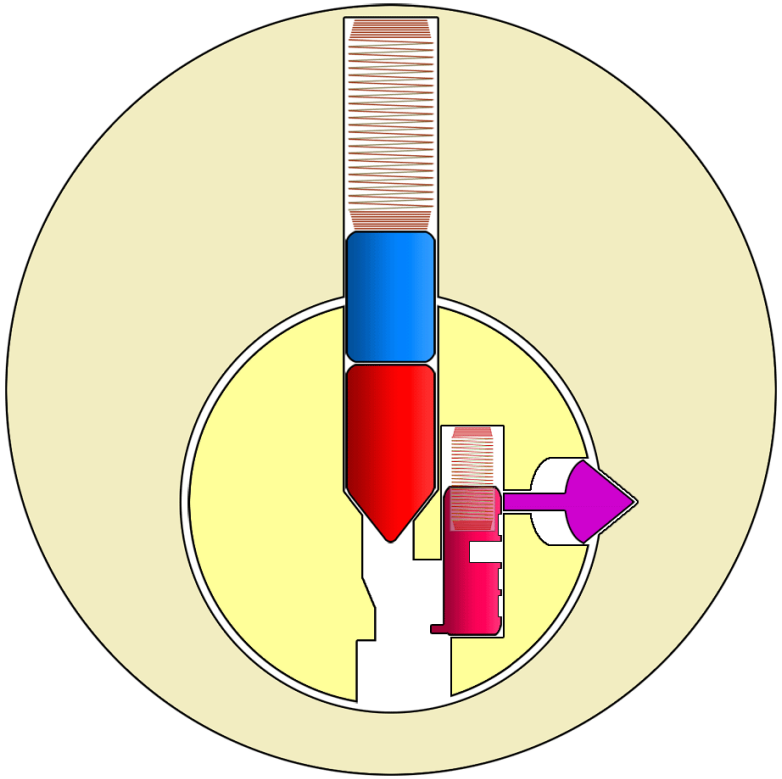
High Security Locks - Pin-Based

Side Bar

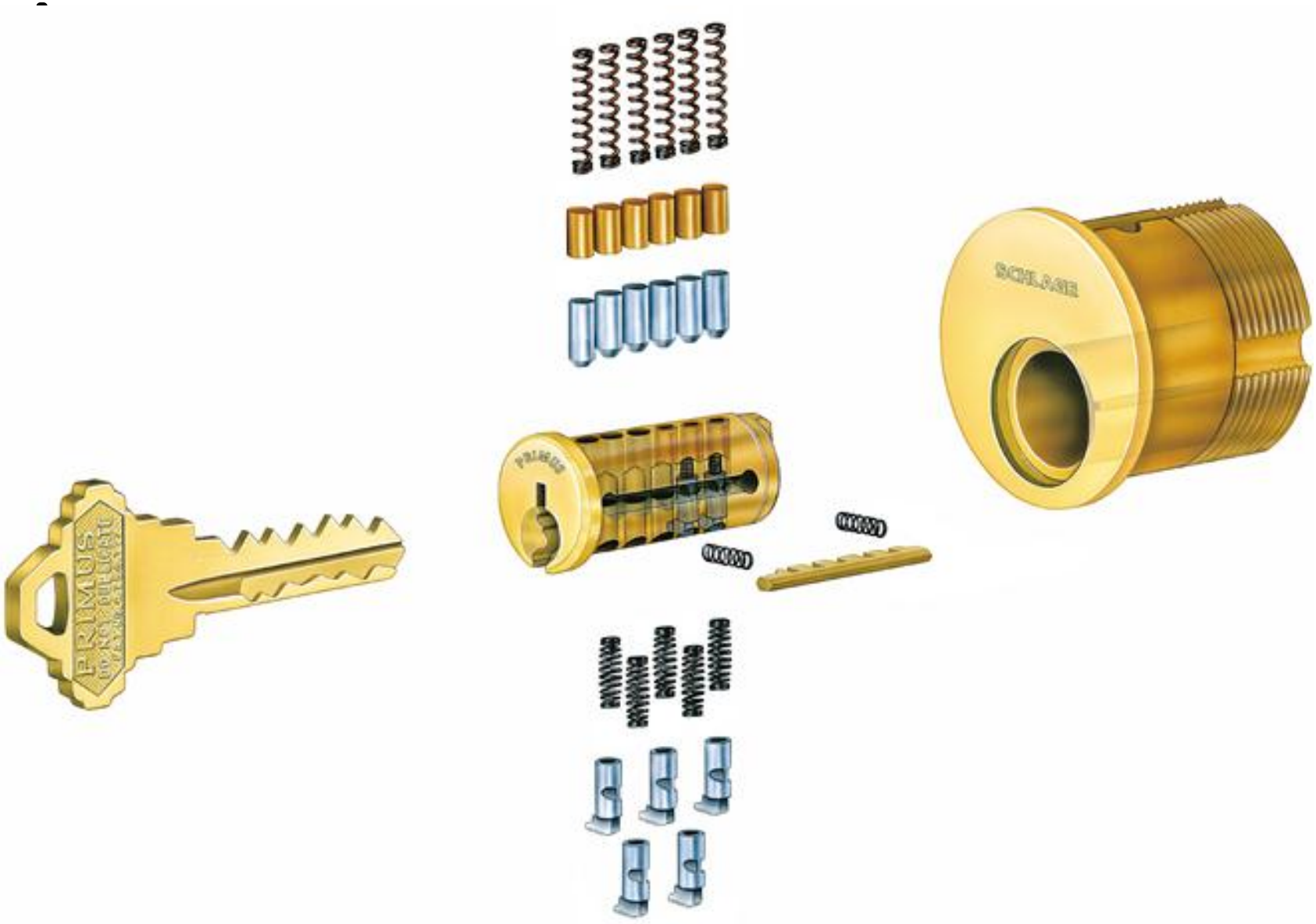


High Security Locks - Pin-Based

Side Bar

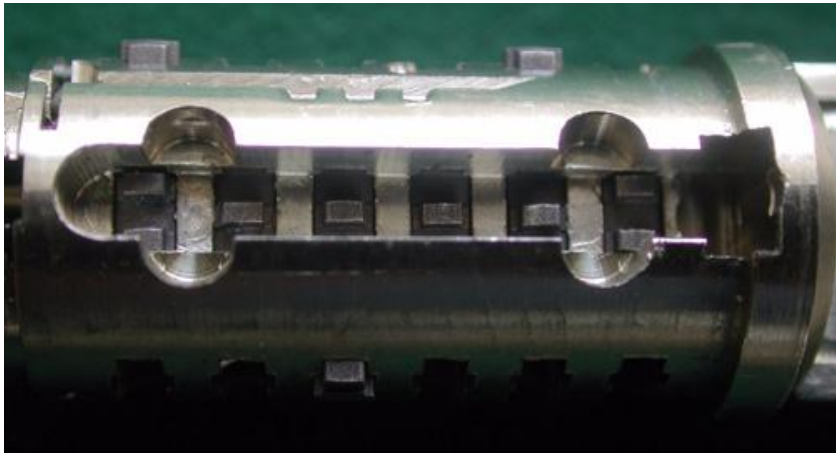


Pin-Based Side Bar - Schlage Pr

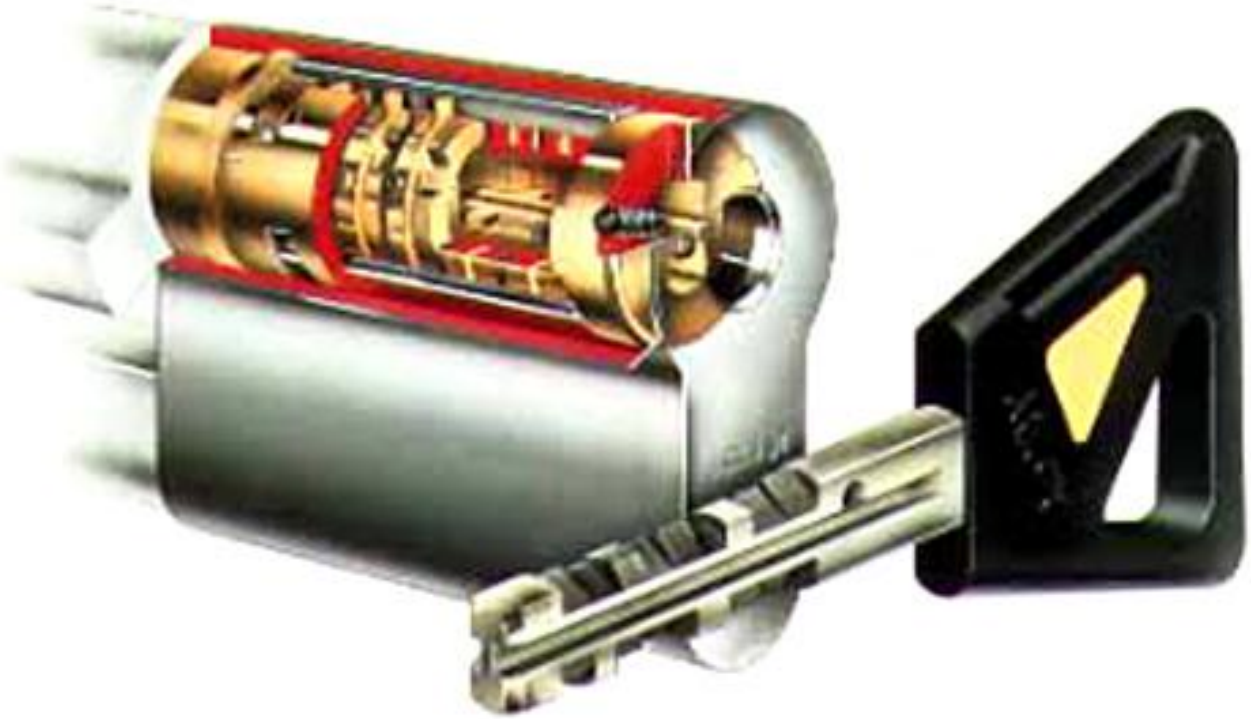


High Security Locks - Side Bar

Only Design

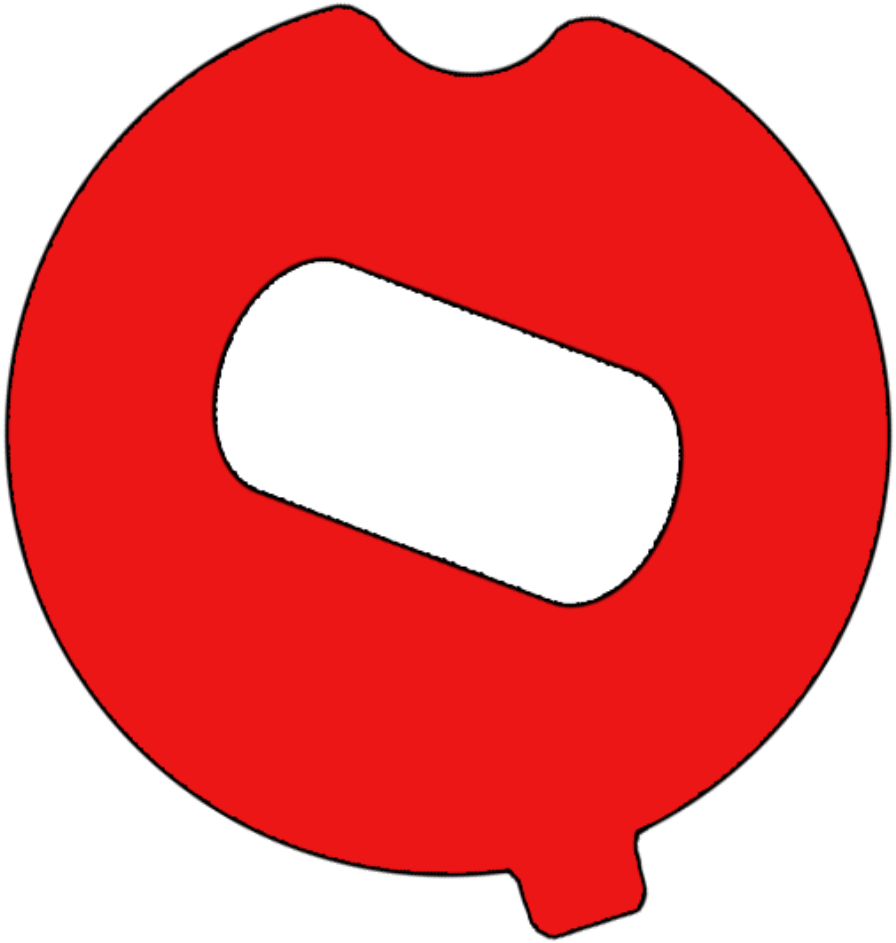


Rotating Discs



Rotating Discs

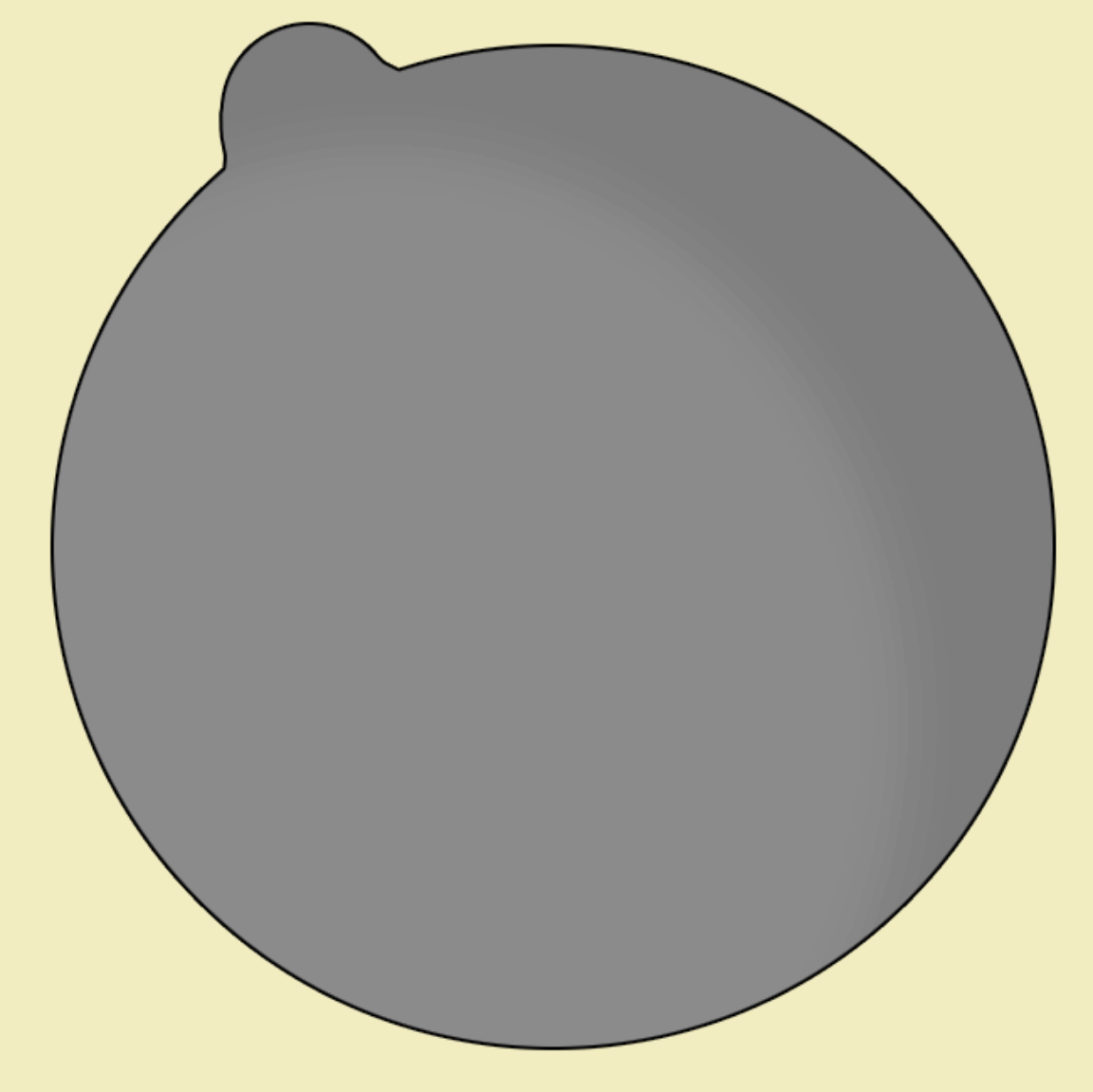
Rotating Discs



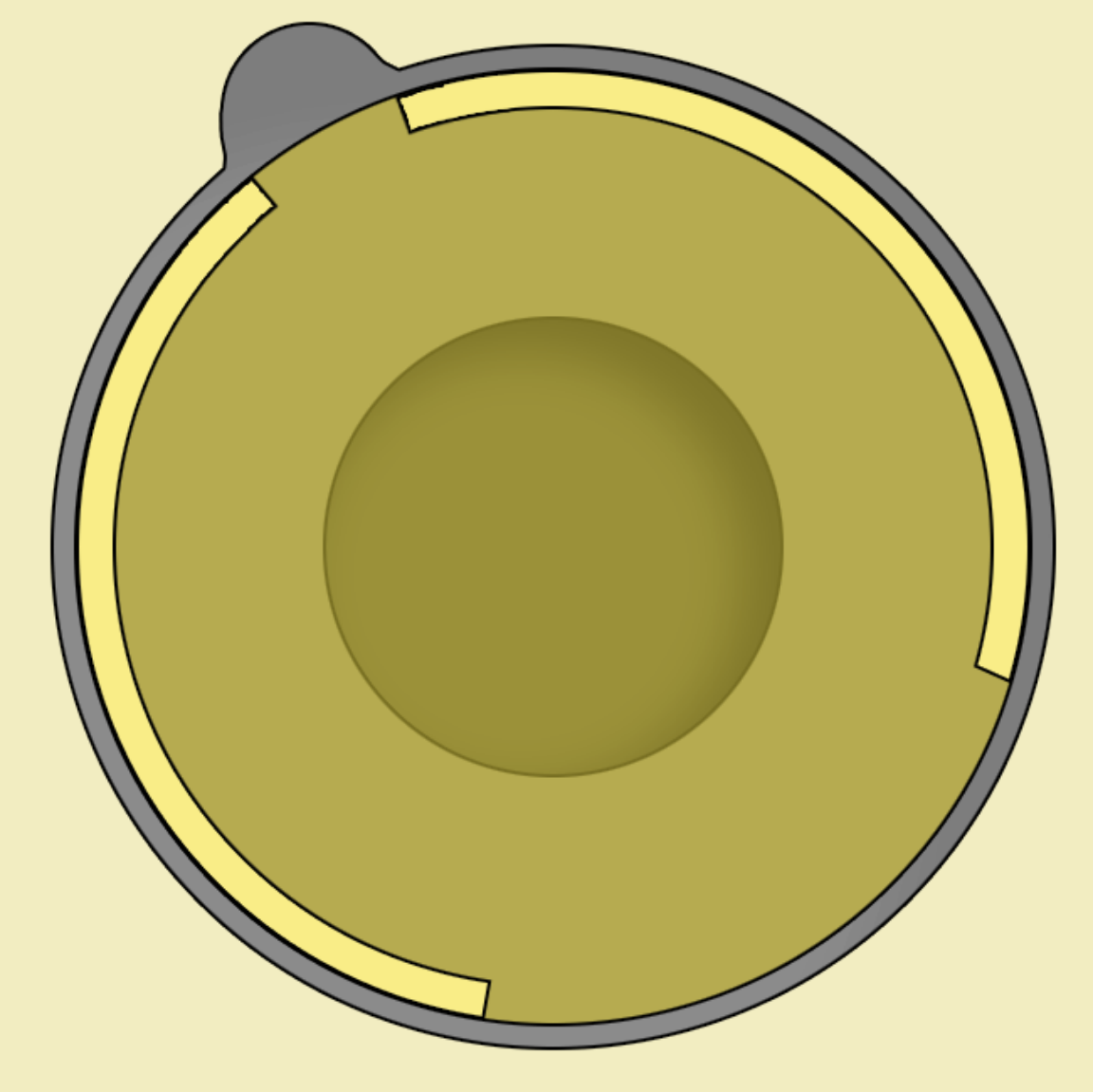
Rotating Discs

Rotating Discs

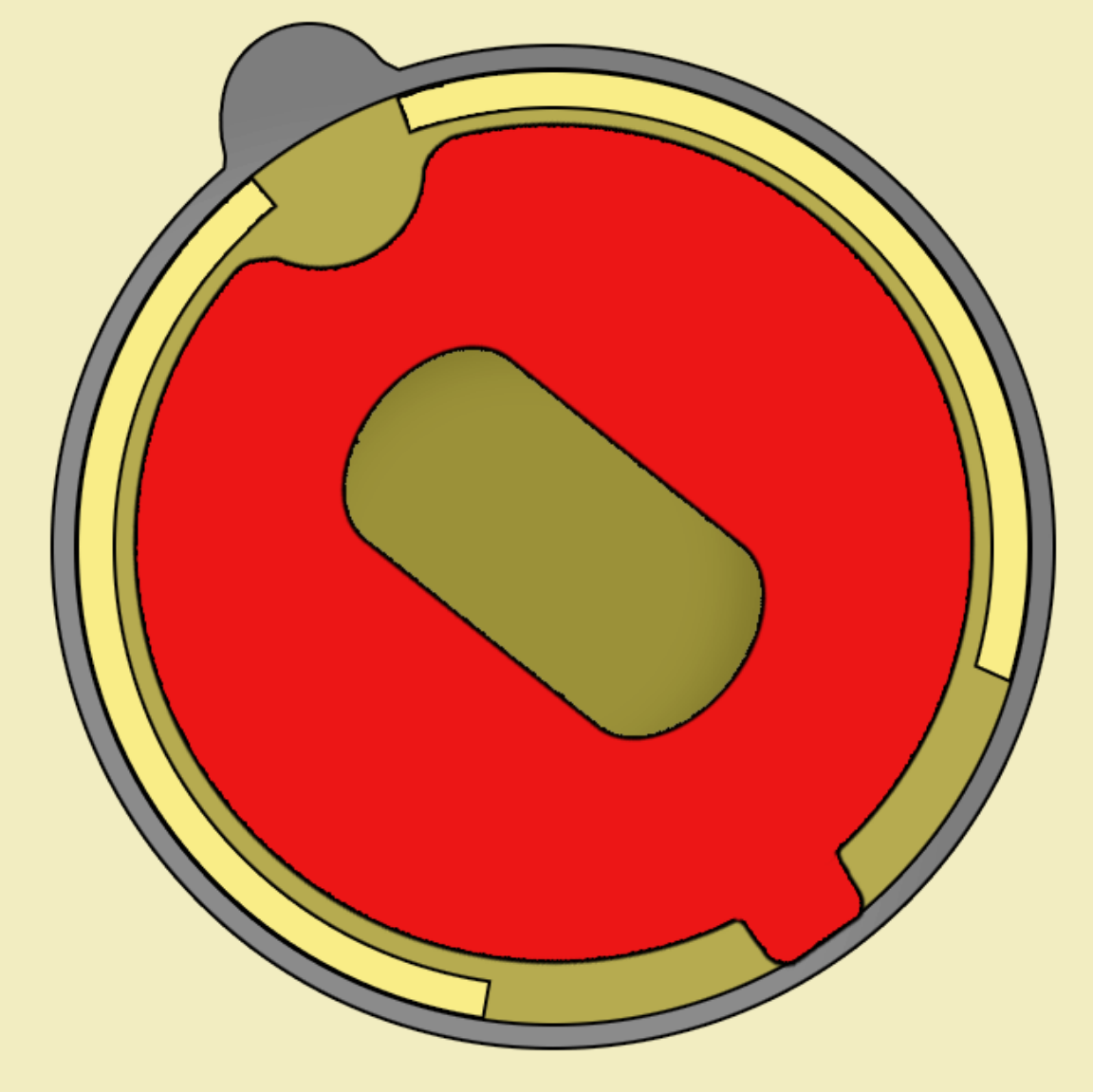
Rotating Discs



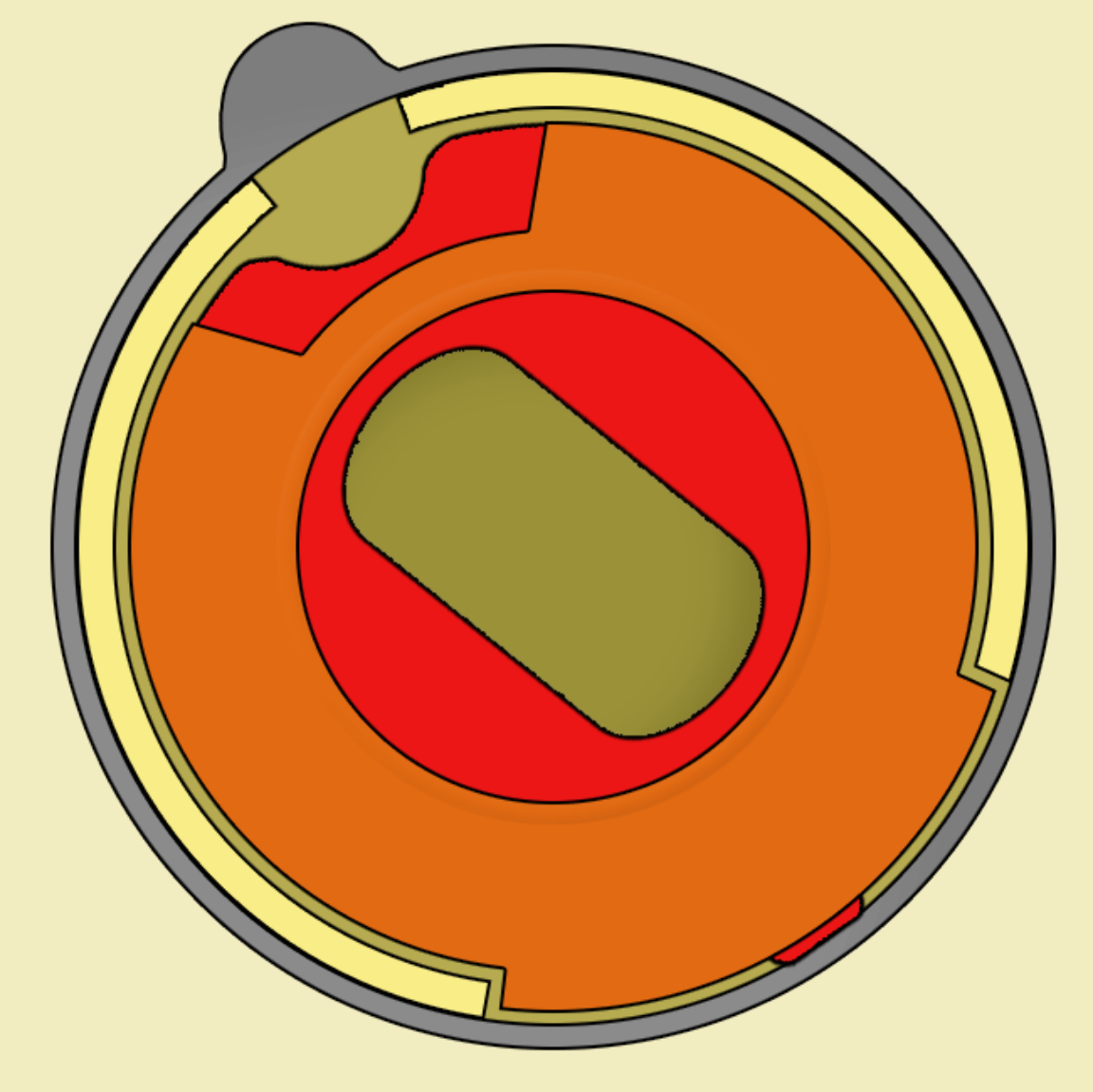
Rotating Discs



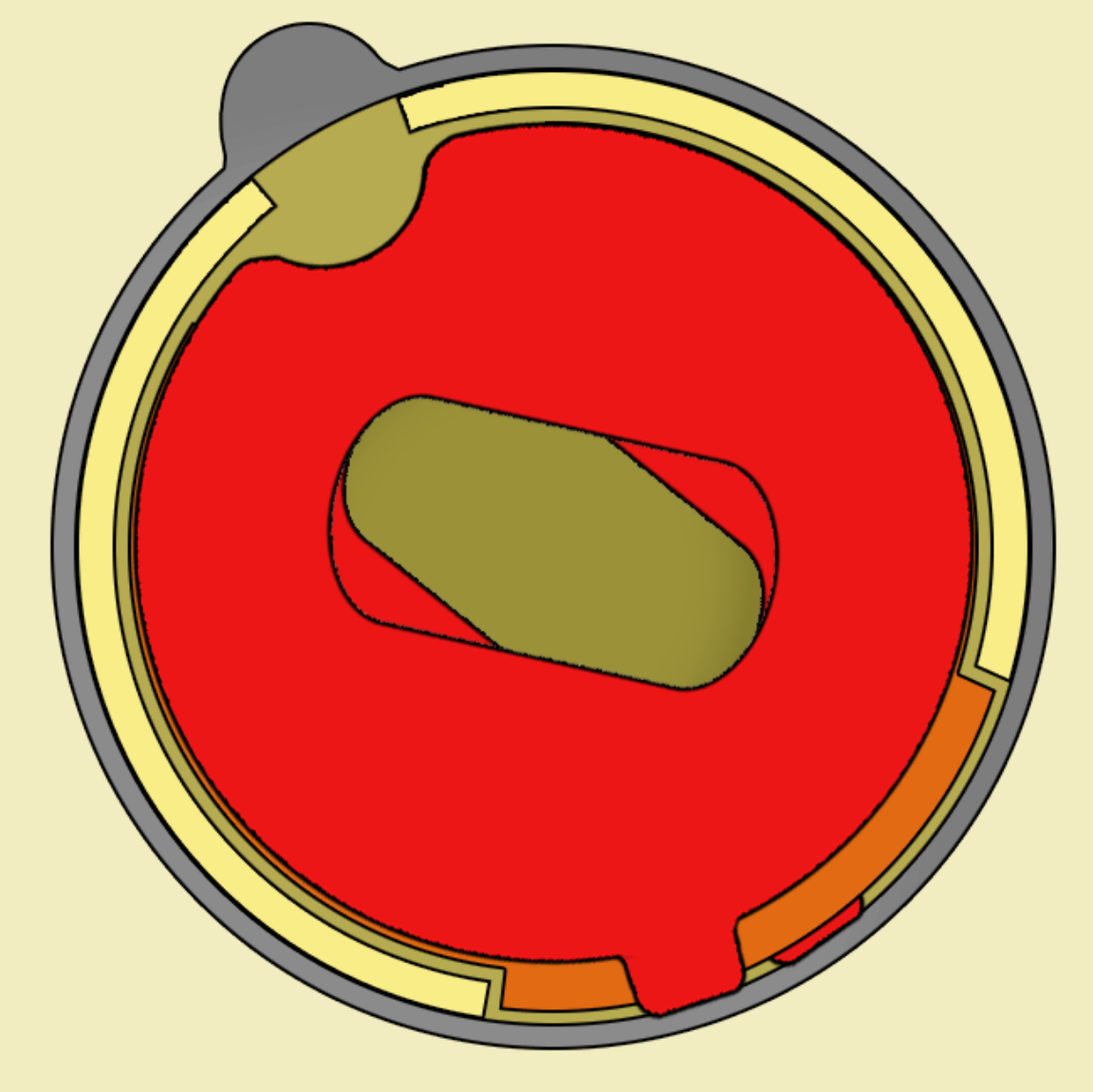
Rotating Discs



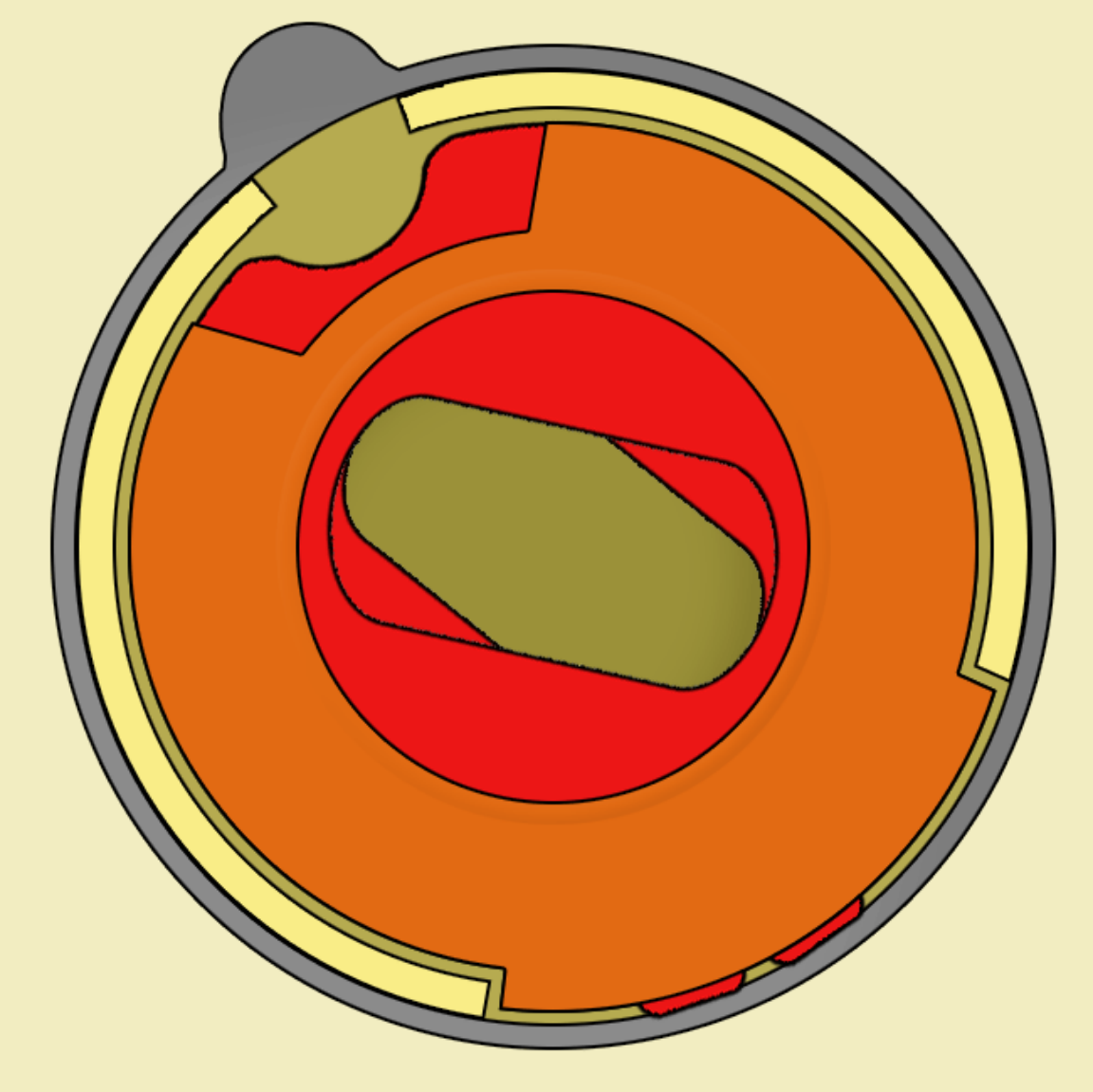
Rotating Discs



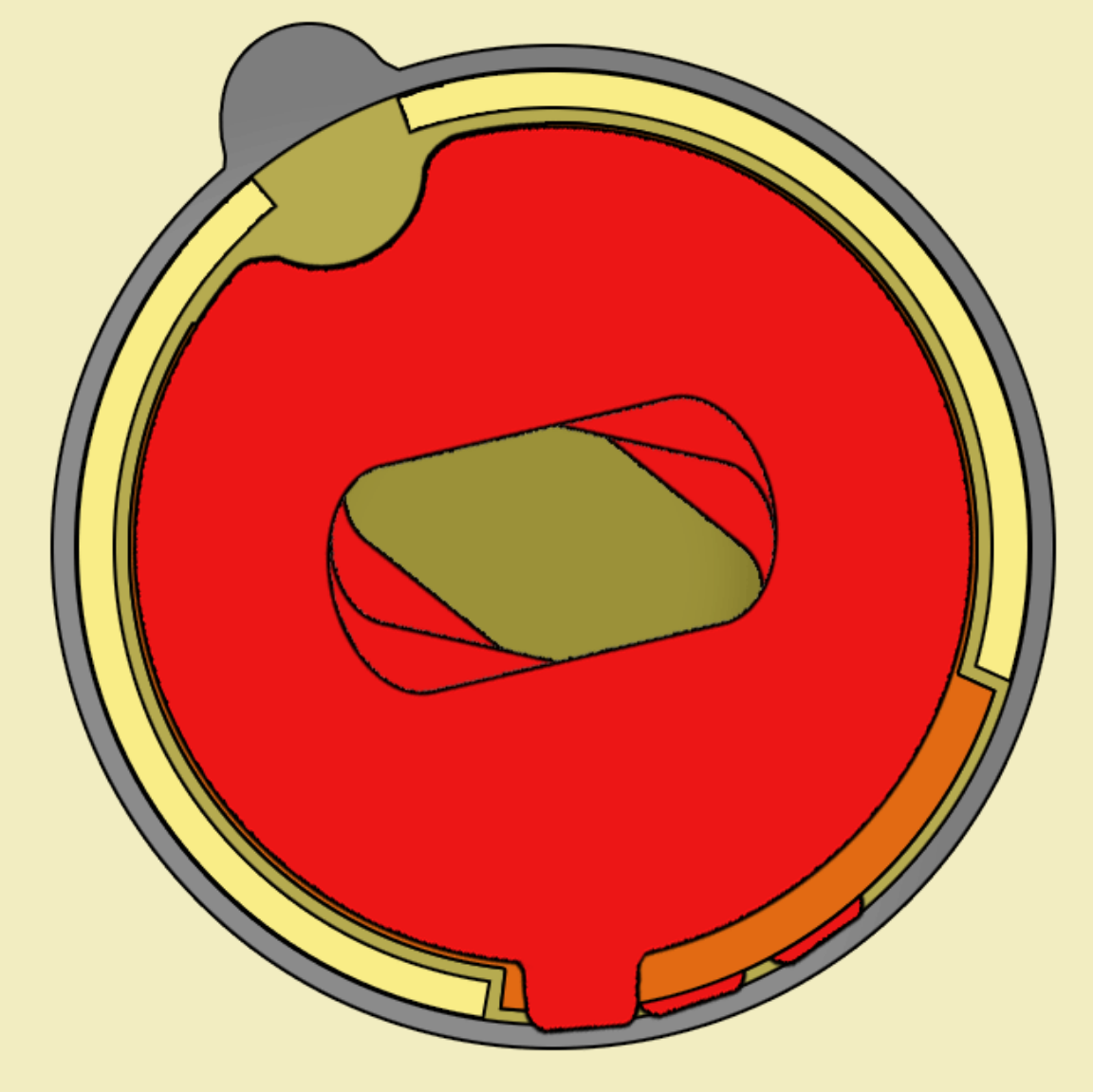
Rotating Discs



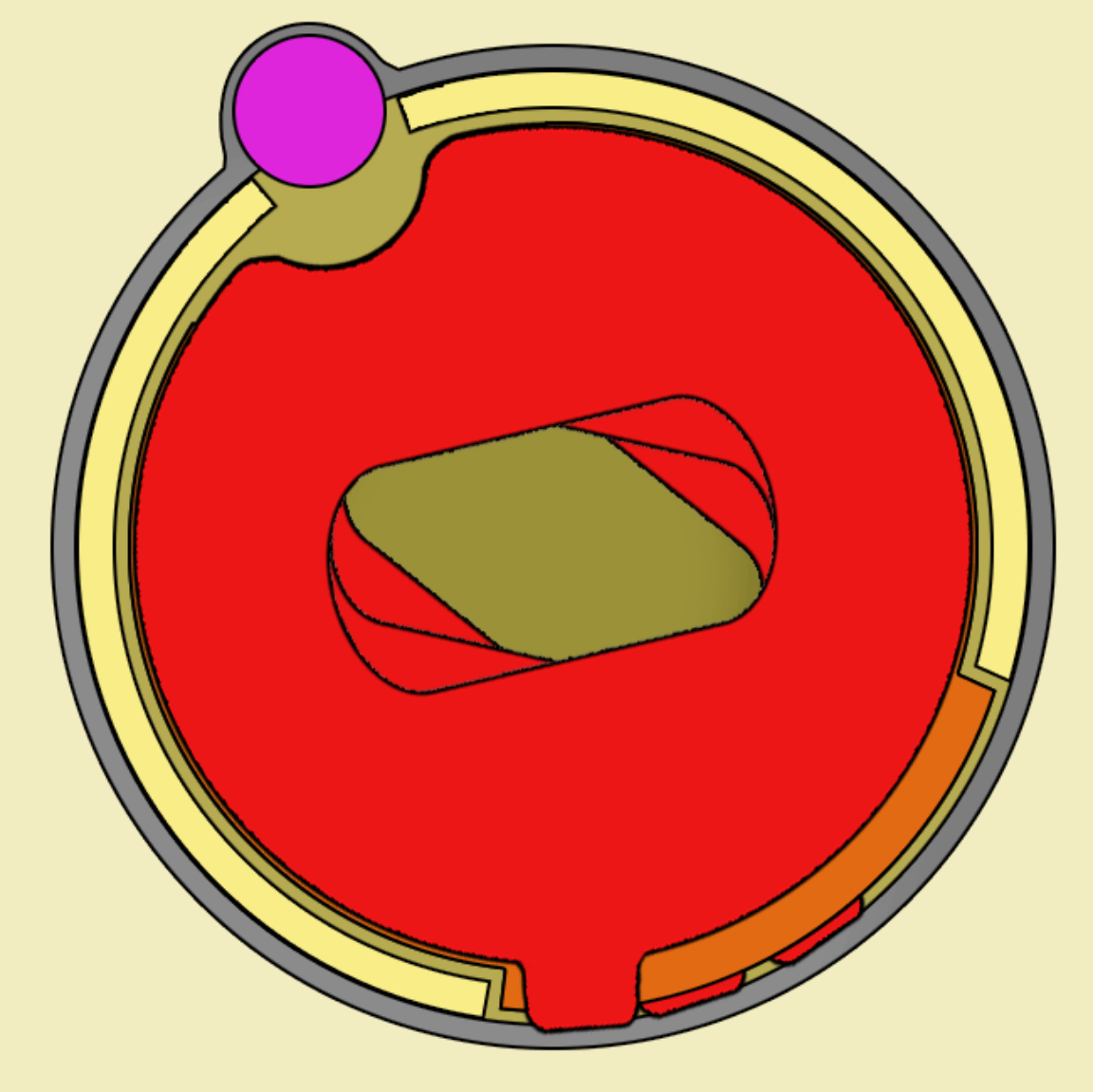
Rotating Discs



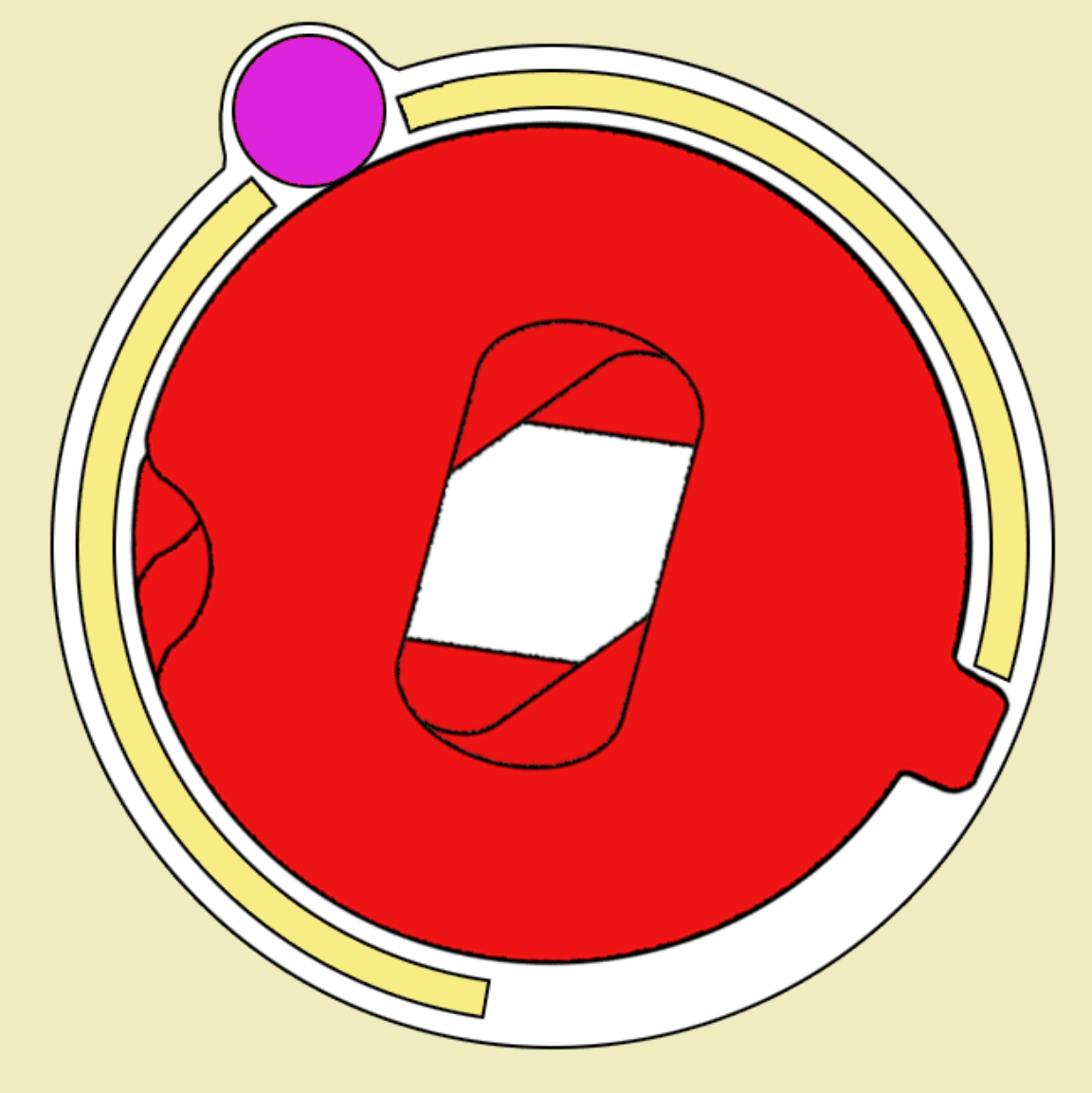
Rotating Discs



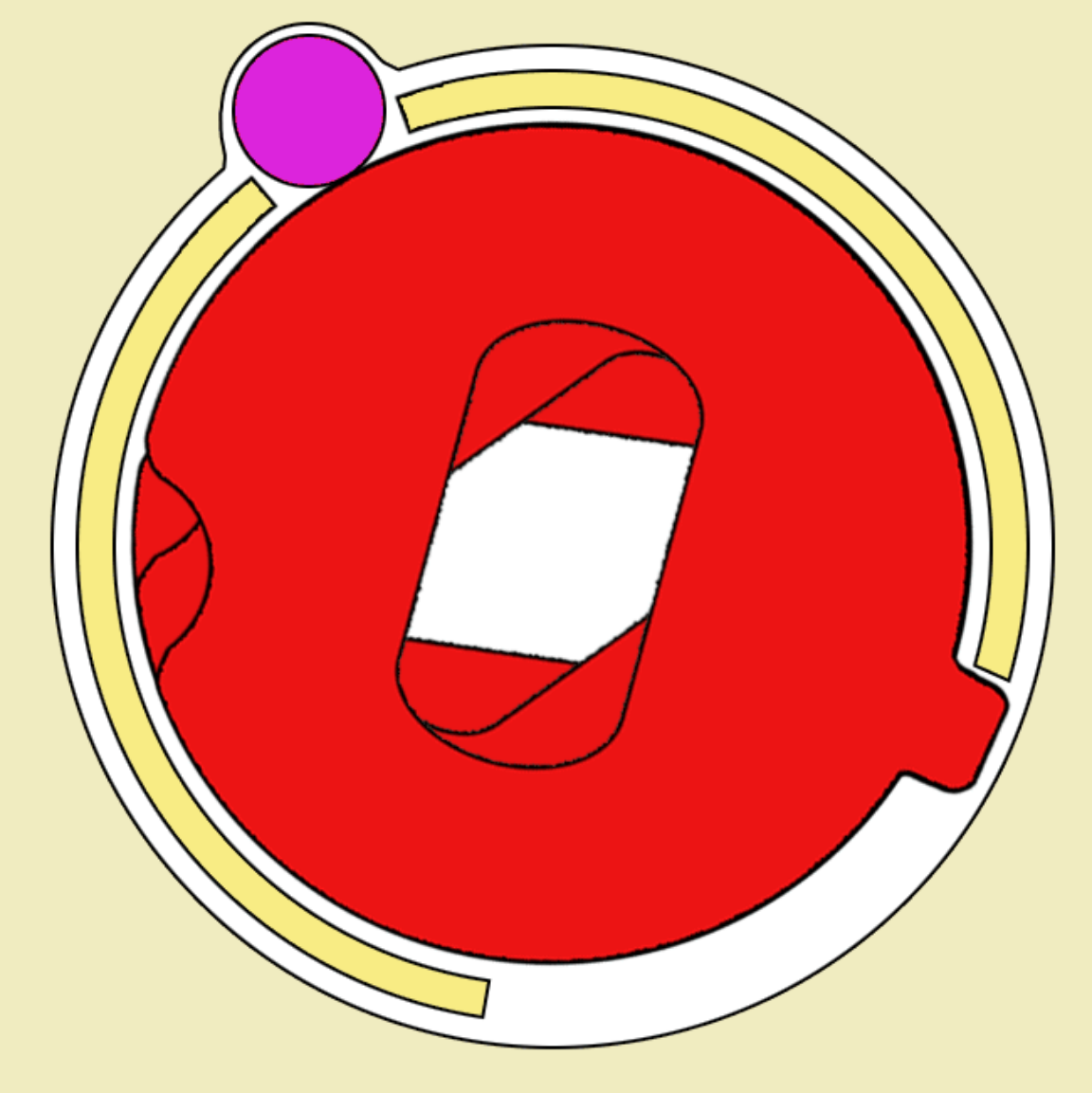
Rotating Discs



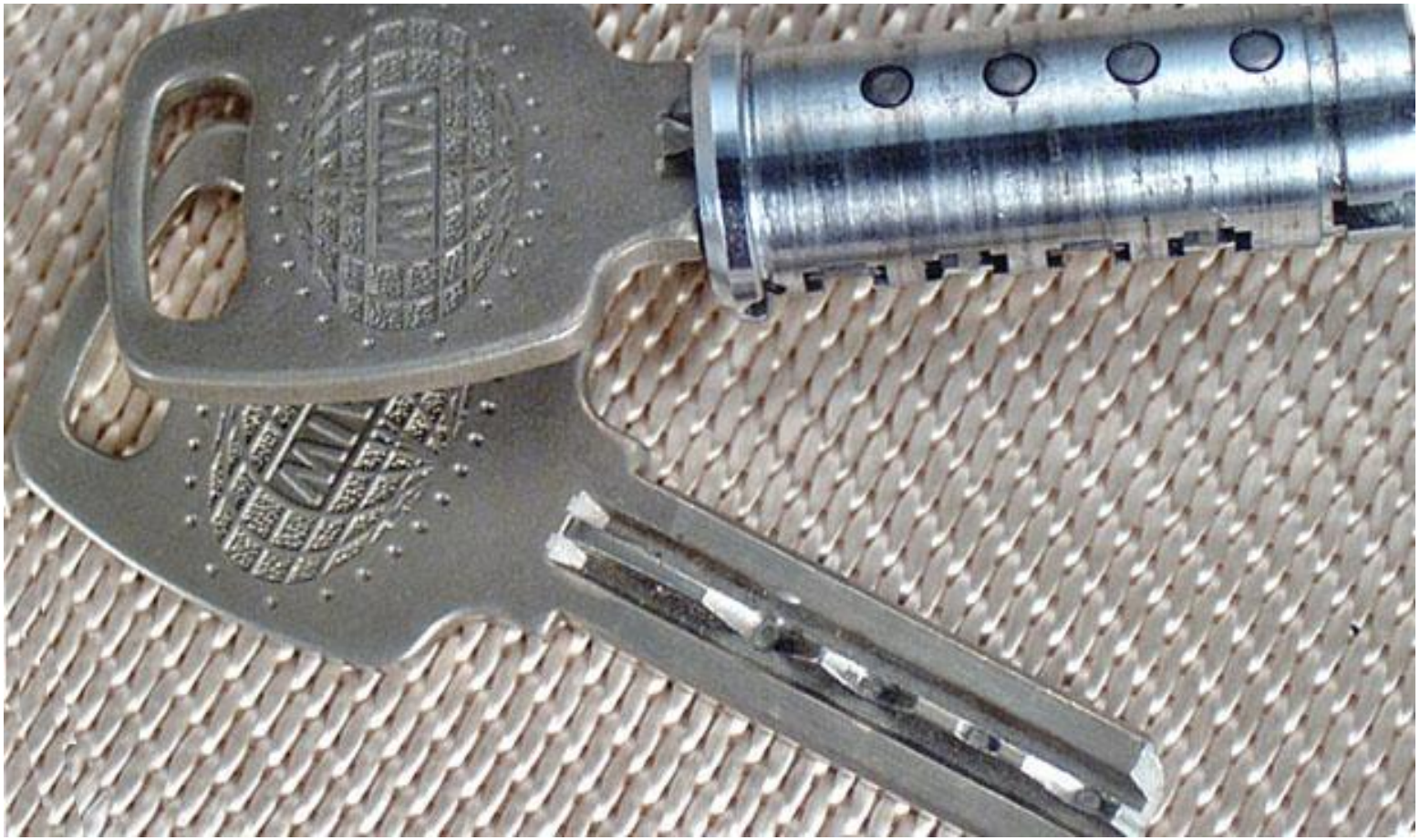
Rotating Discs



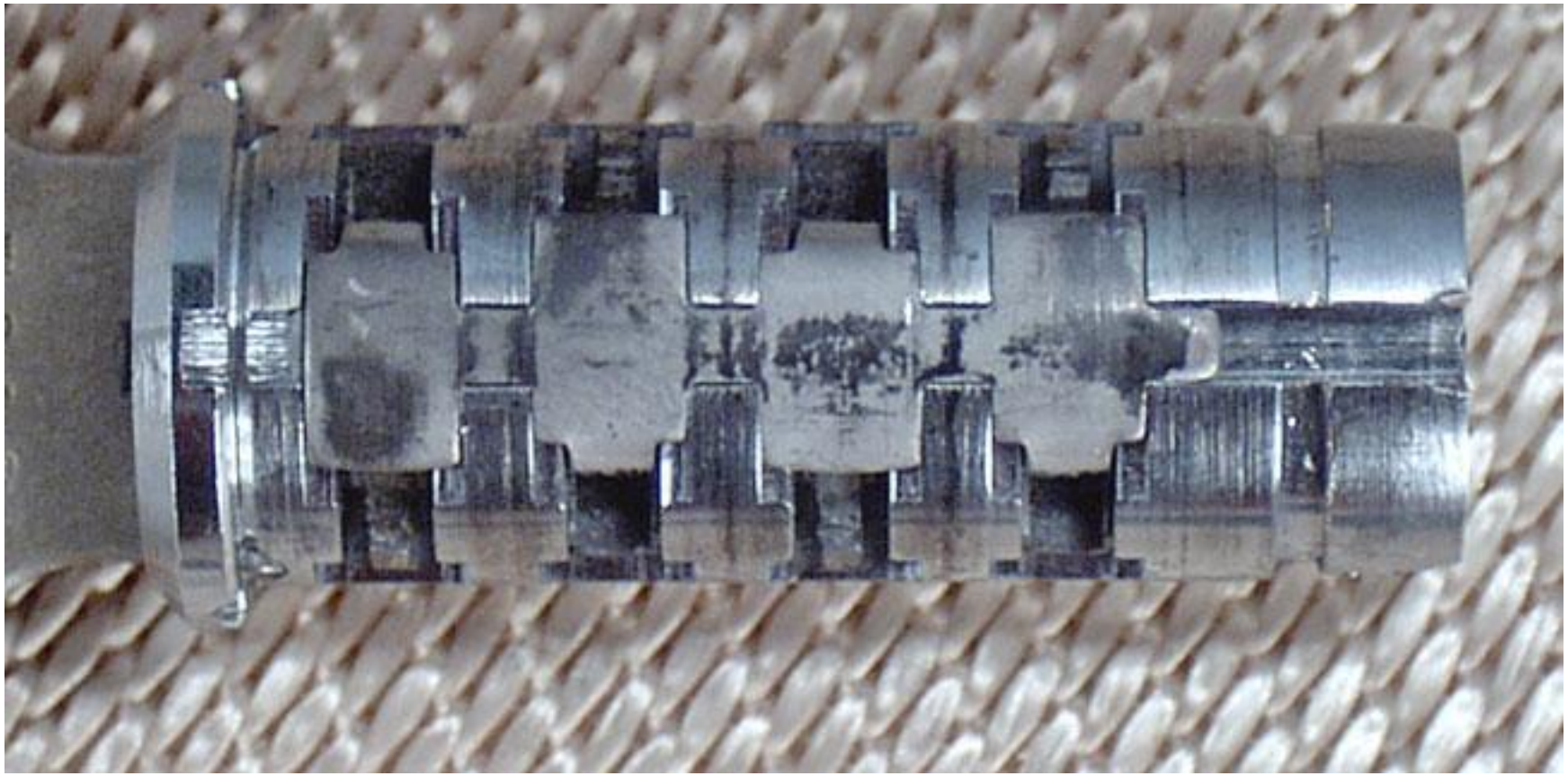
Rotating Discs



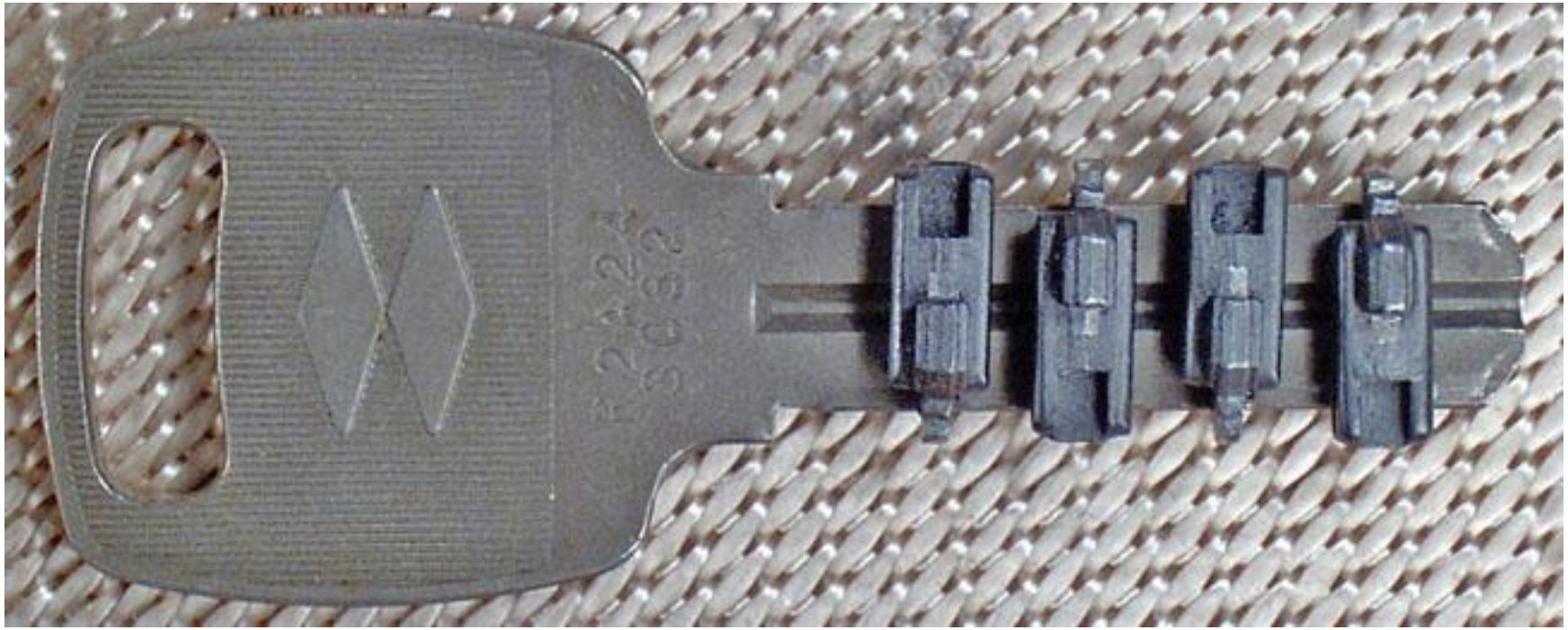
Magnetic Locks



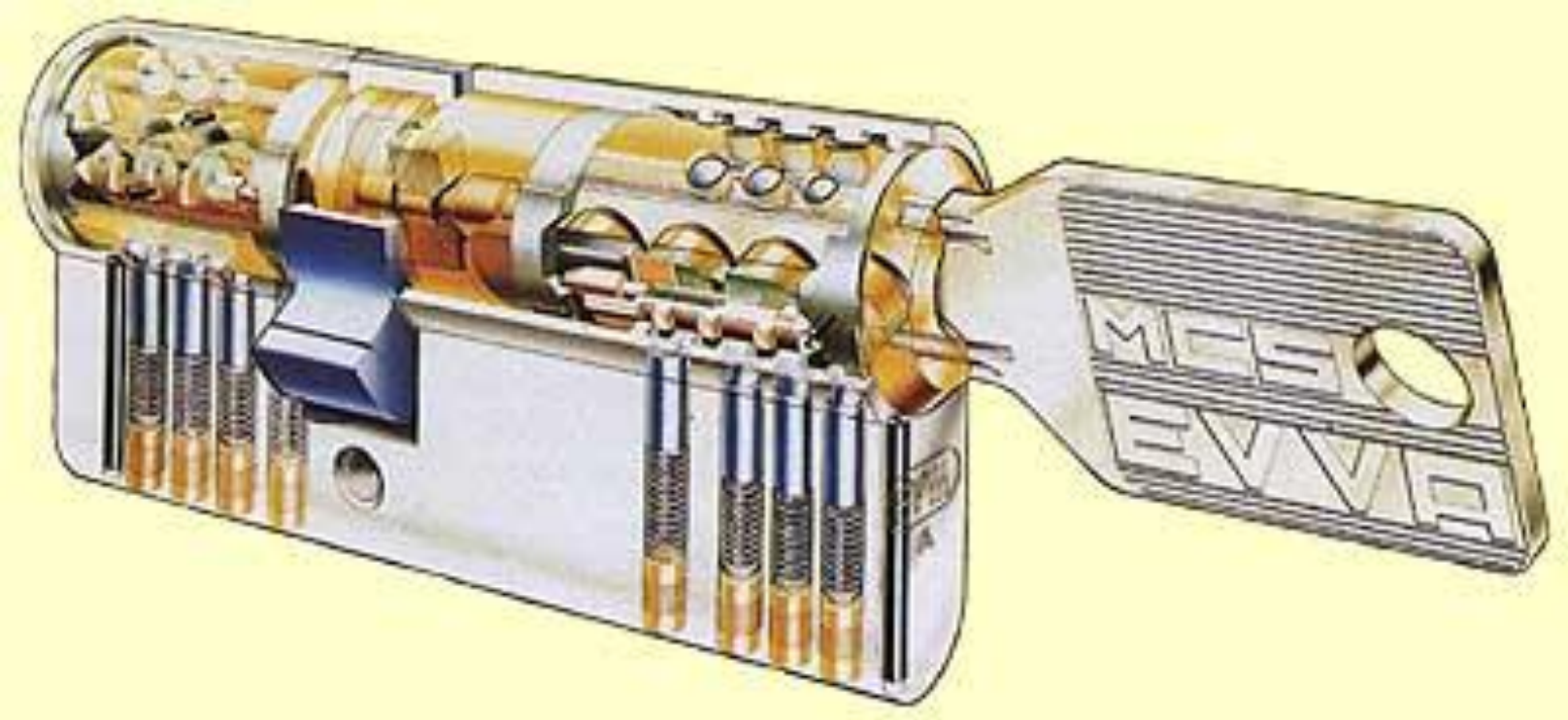
Magnetic Locks



Magnetic Locks



Magnetic Locks



Magnetic Locks

Magnetic Locks

photo courtesy of Eric Schmiedl

Magnetic Locks

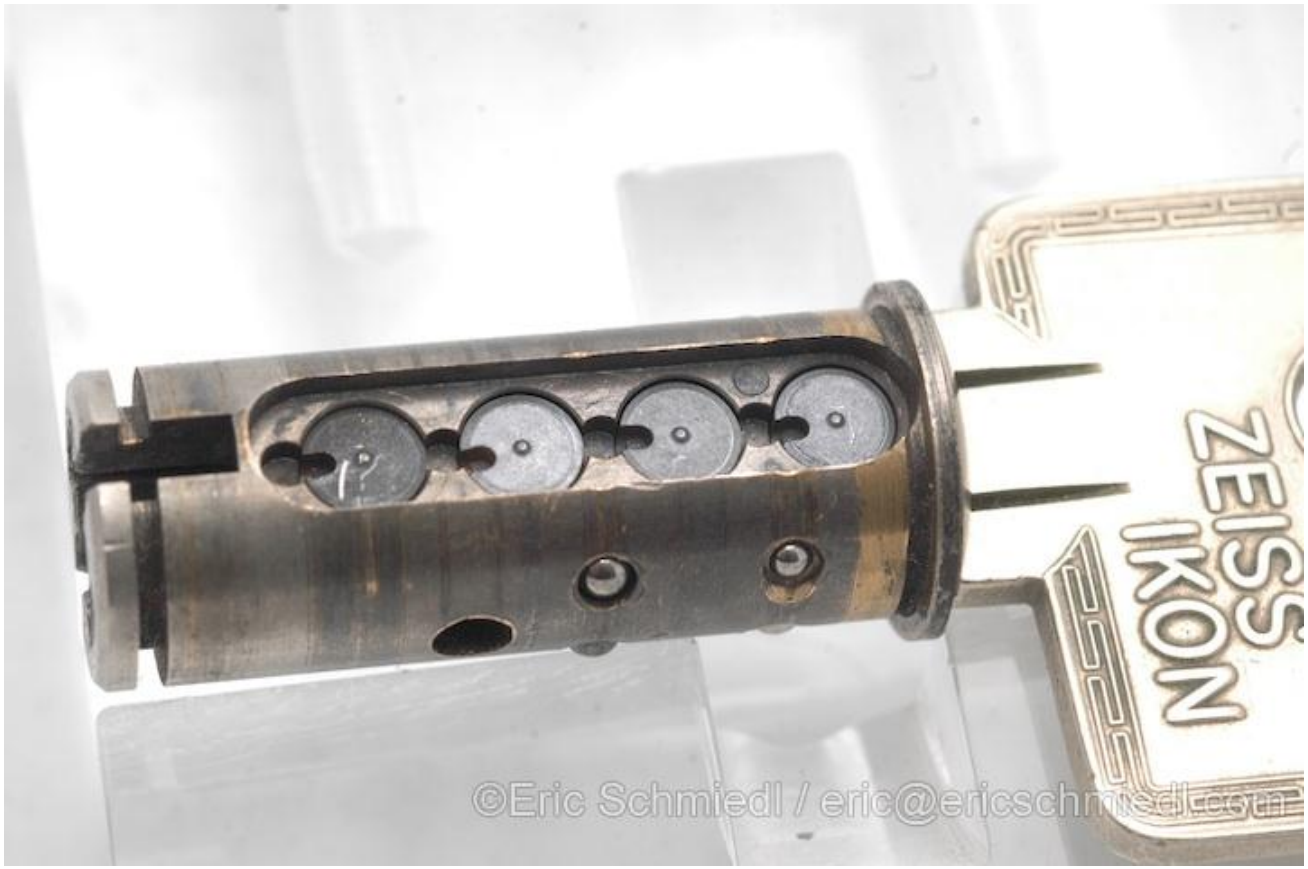
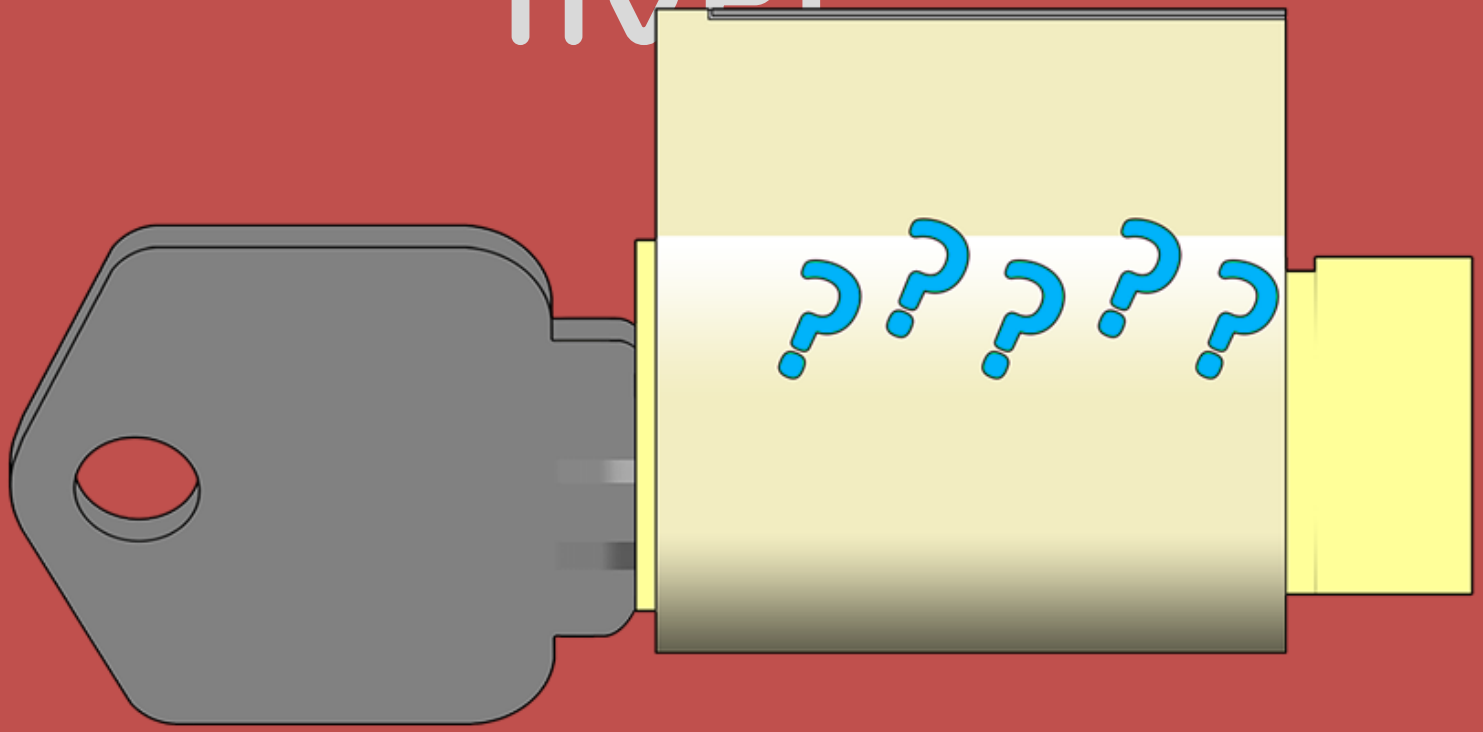


photo courtesy of Eric Schmiedl

A New Contest At HOPE



Master-Key Escalation Contest

Master-Key Escalation Contest

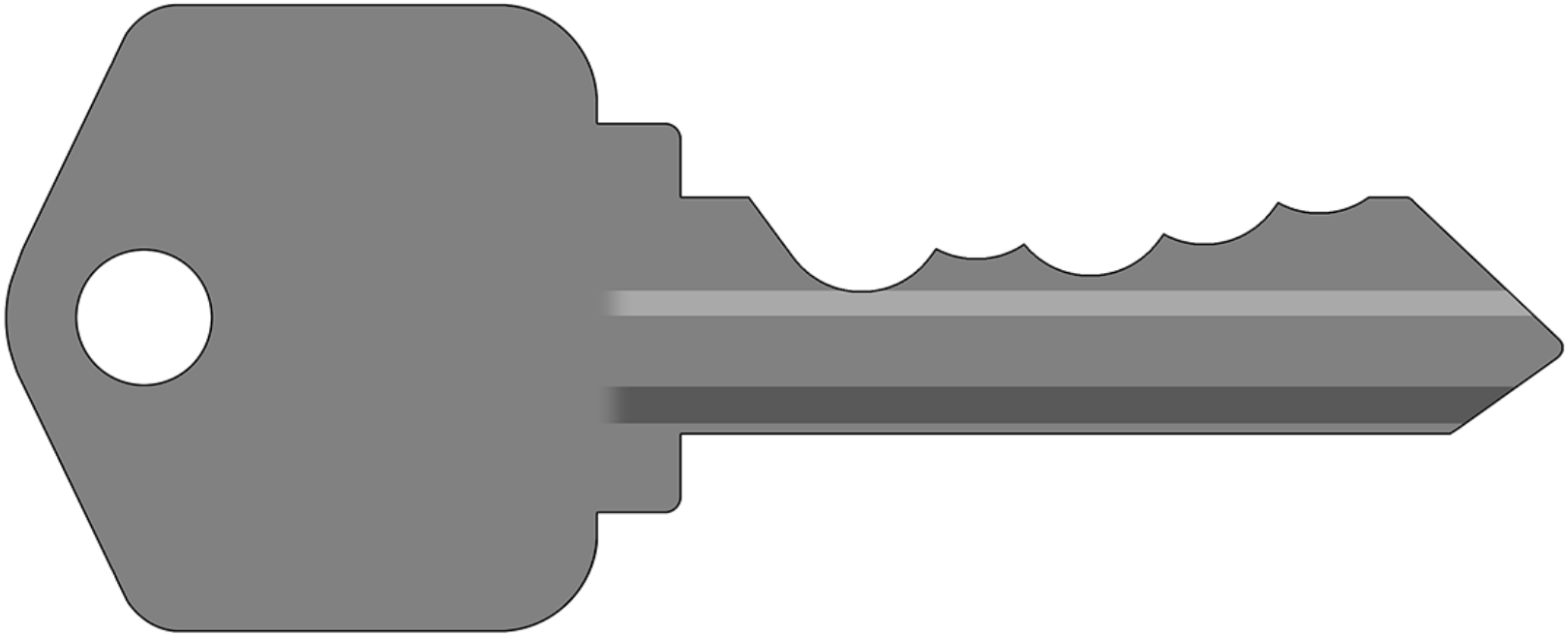
Master-Key Escalation Contest

Master-Key Escalation Contest

Master-Key Escalation Contest

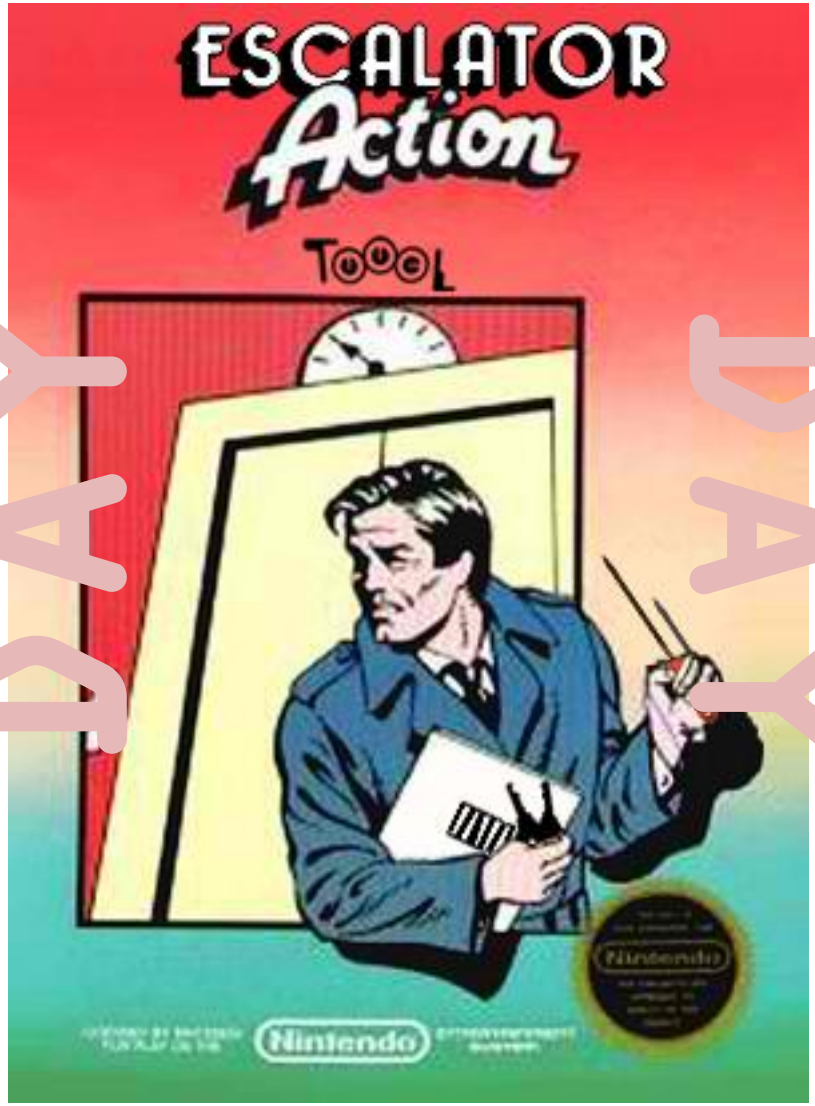
Master-Key Escalation Contest

Will j00 be teh winnar?!?



Master-Key Escalation Contest

SATURDAY



SATURDAY

Thank You Very Much!

TOOL
The Open Organisation Of Lockpickers

http://tool.us

info@tool.us