Cybersecurity Engineering – Lab Visit (2023)

Te Roopu Owhiti

Cybersecurity Research Group

VICTORIA UNIVERSITY OF WELLINGTON
TE HERENGA WAKA

What is lock picking?

Non-destructive way to bypass locks.

Mimic action of key without having one.

Focus pin tumbler (common and 6,000 years old).

Why is it like cybersecurity?

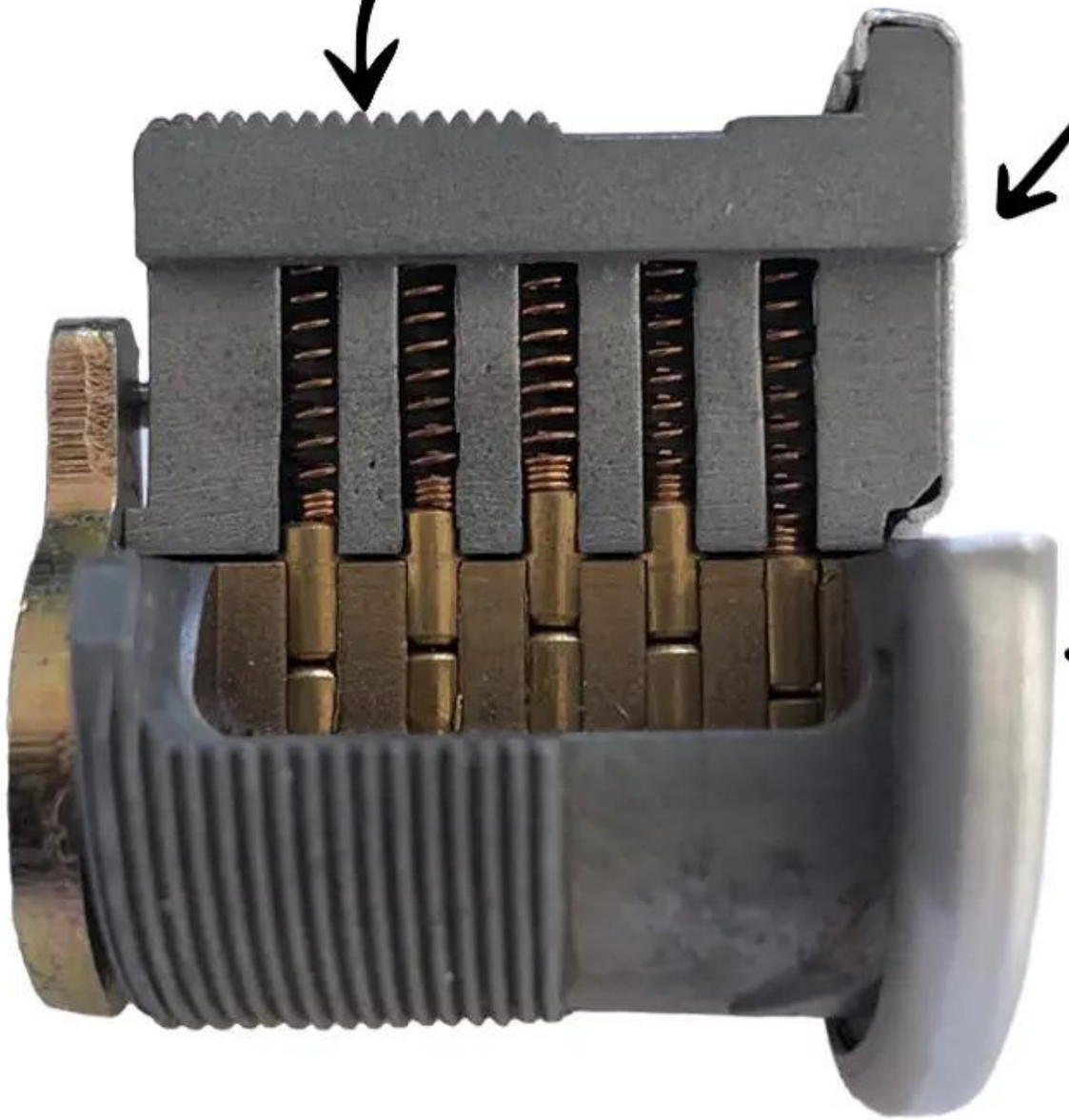
Code of conduct.

Everything can be opened.

Depends on flaws.

Battle of wills attacker and defender.

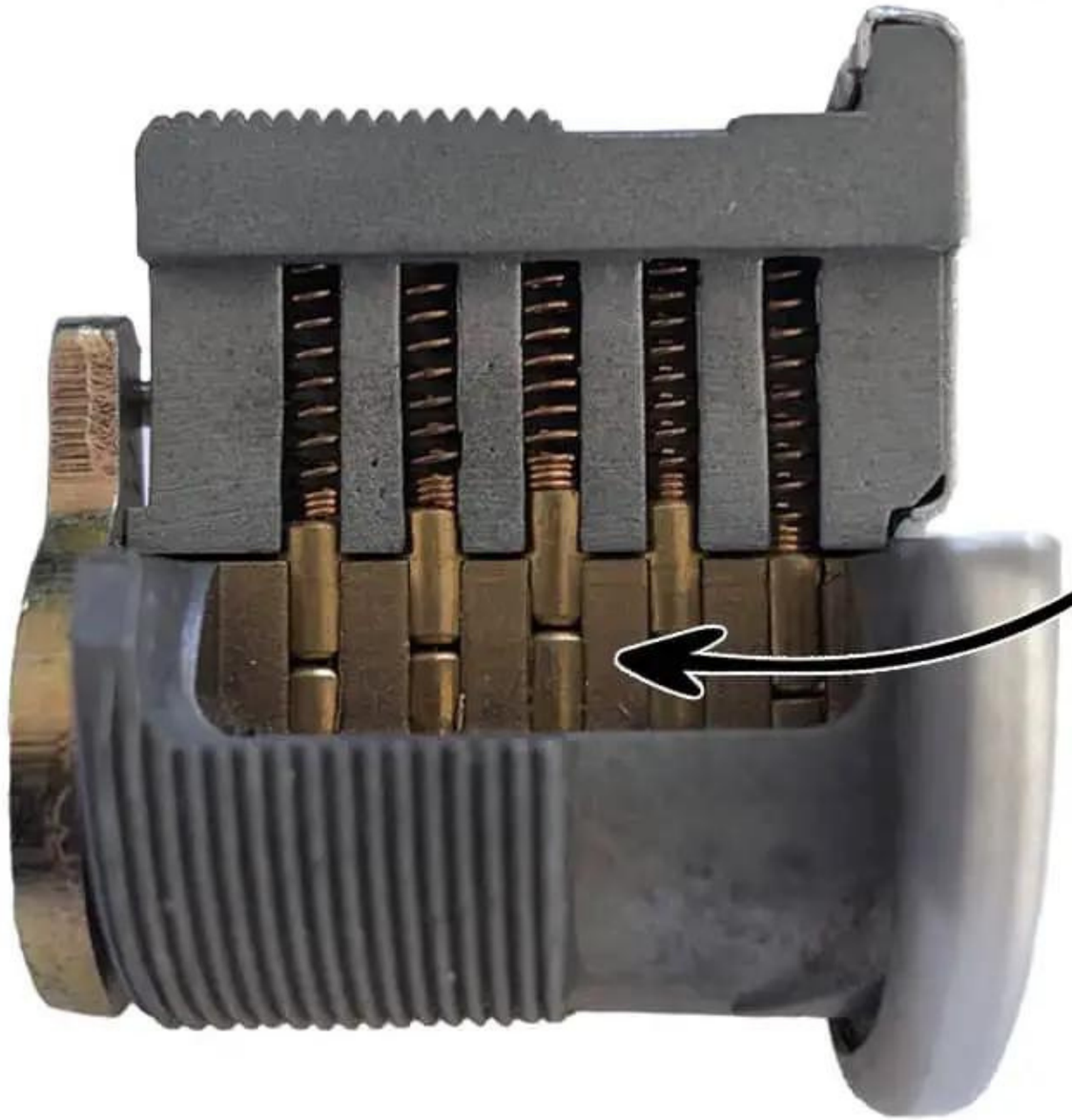
The Cylinder



CONTAINS EVERYTHING ELSE

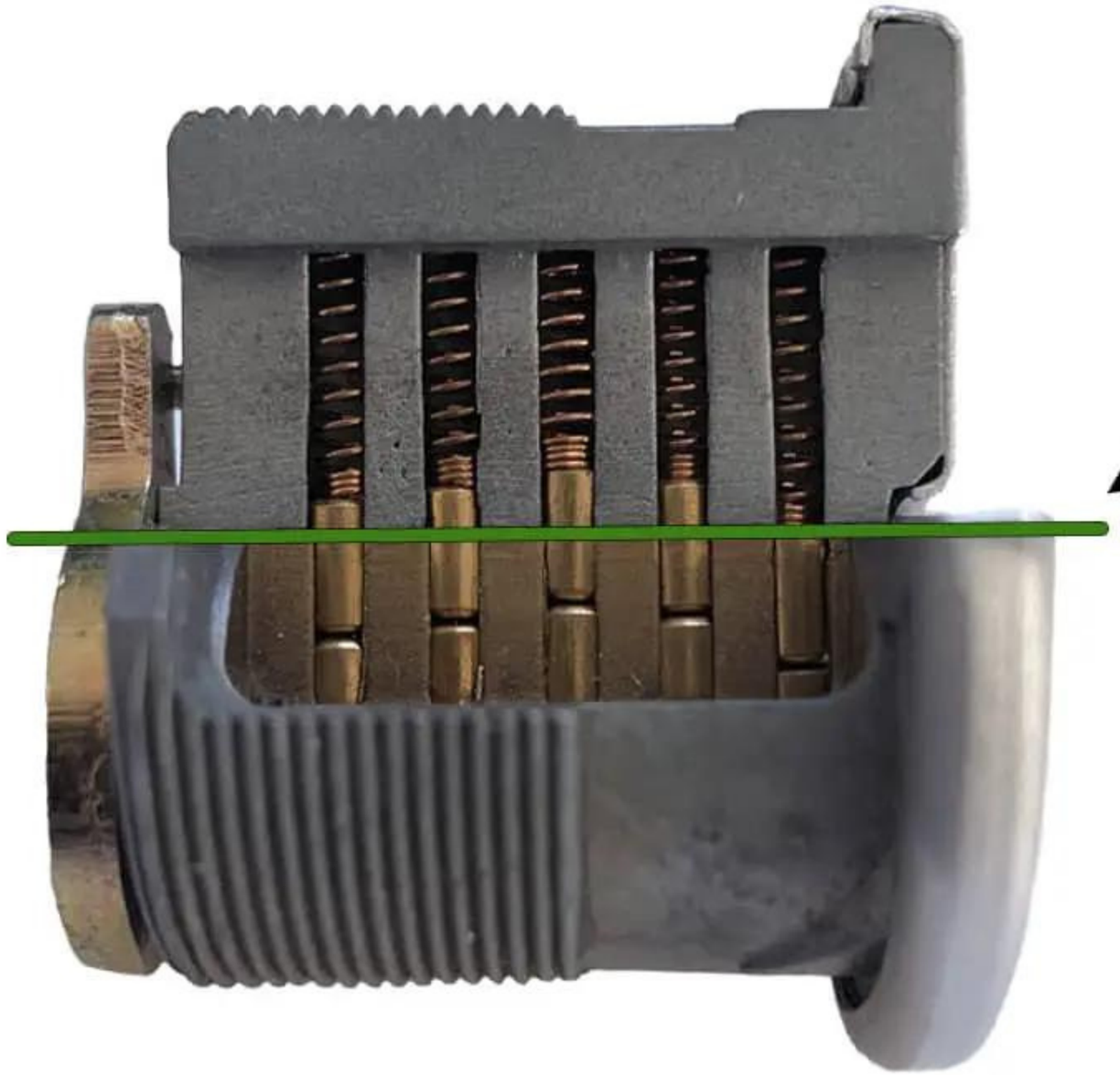
Art of Lockpicking

The Plug

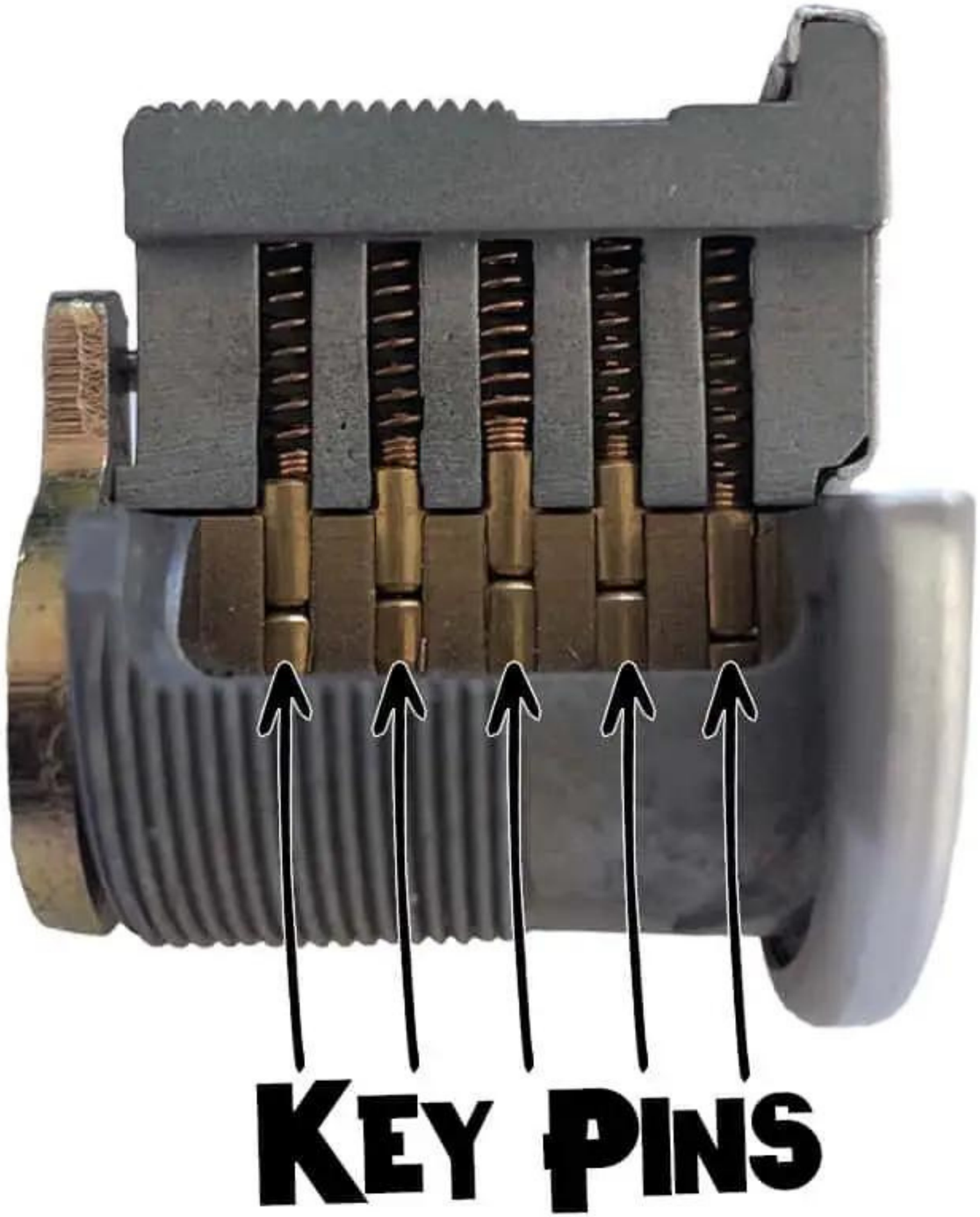


CONTAINS LOCK'S PINS
CAN ROTATE

The Shear Line

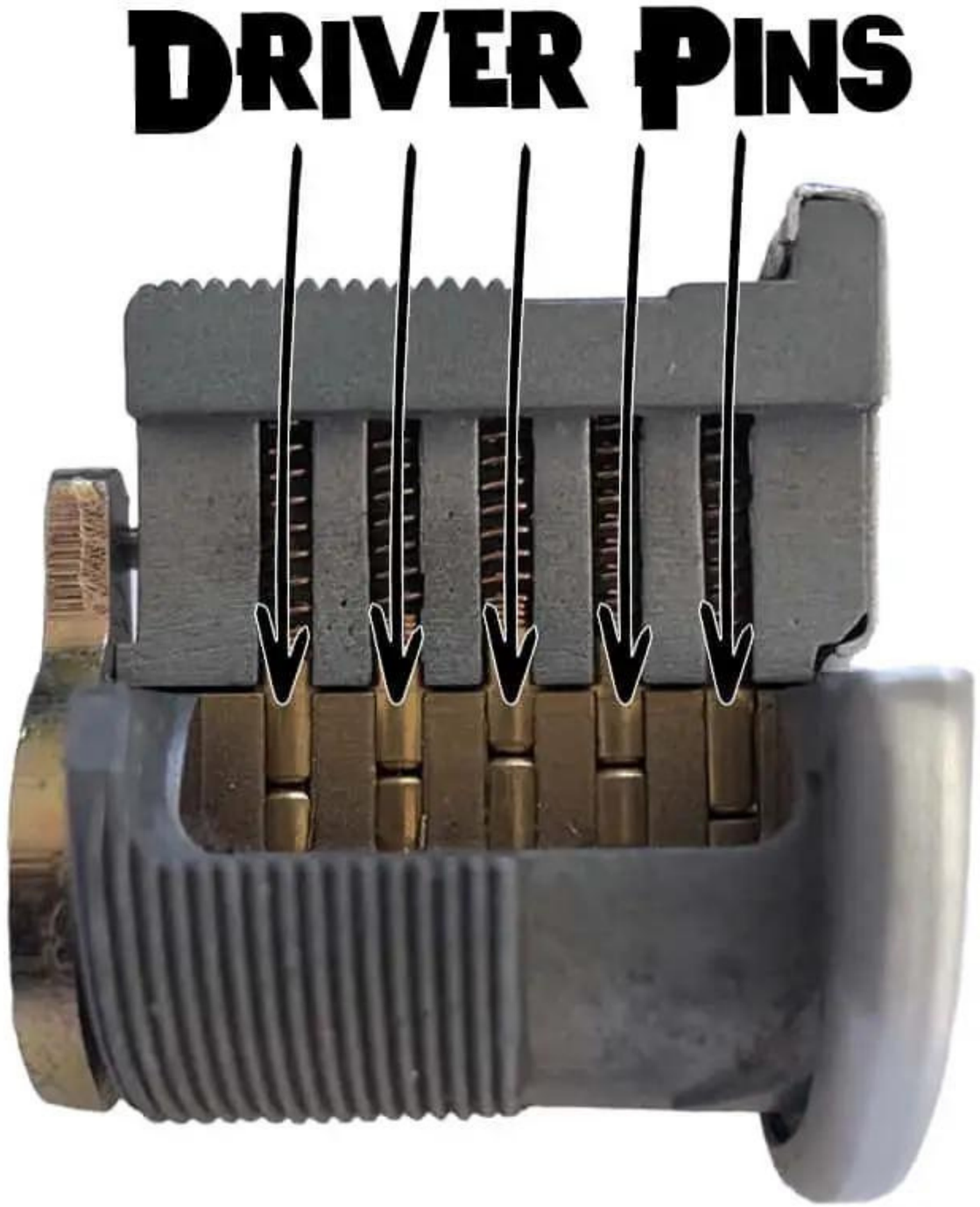


MUST BE CLEARED TO ALLOW PLUG TO TURN



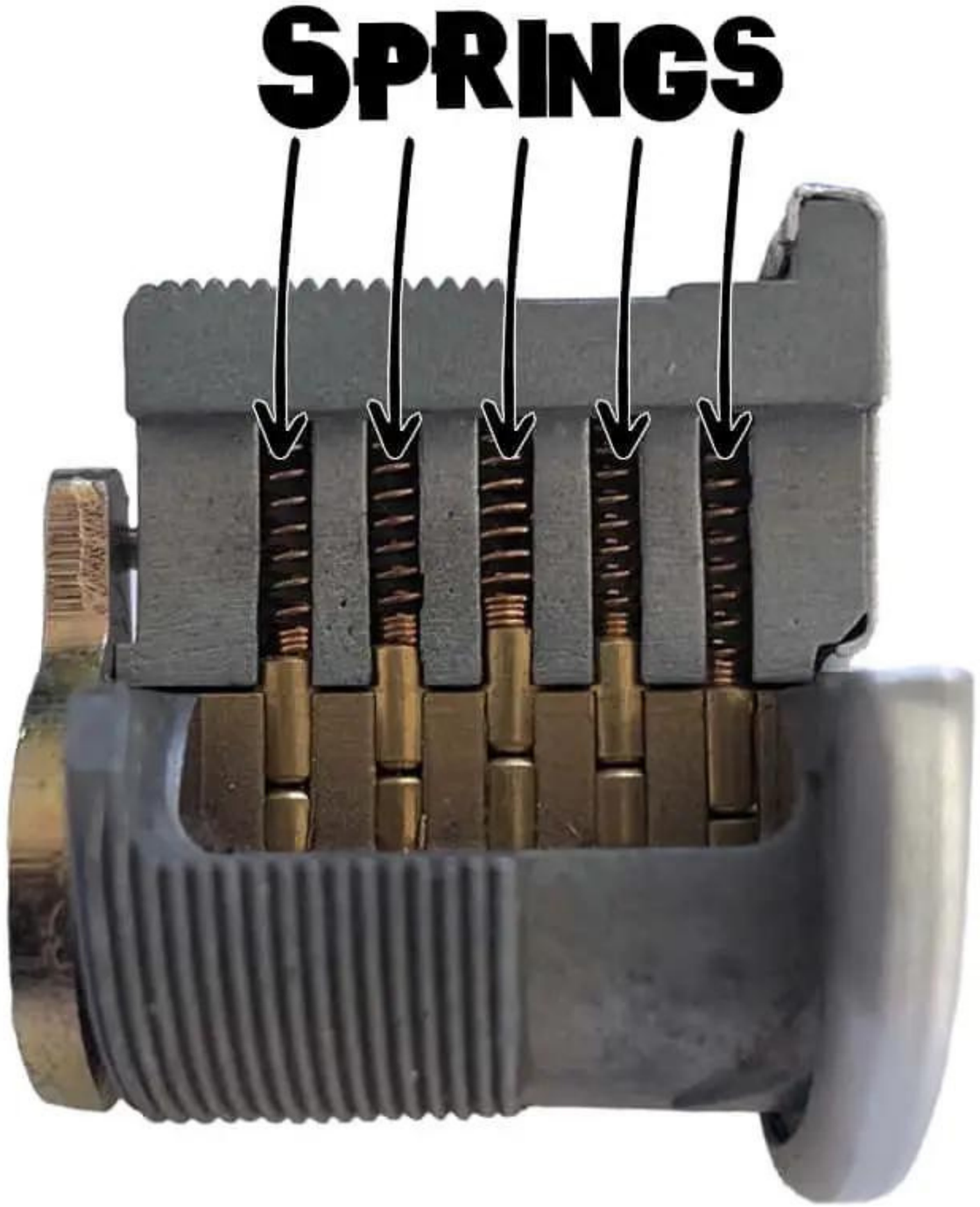
KEY PINS DIFFERENT LENGTH AND ARE PUSHED UP BY KEY

ART OF LOCKPICKING



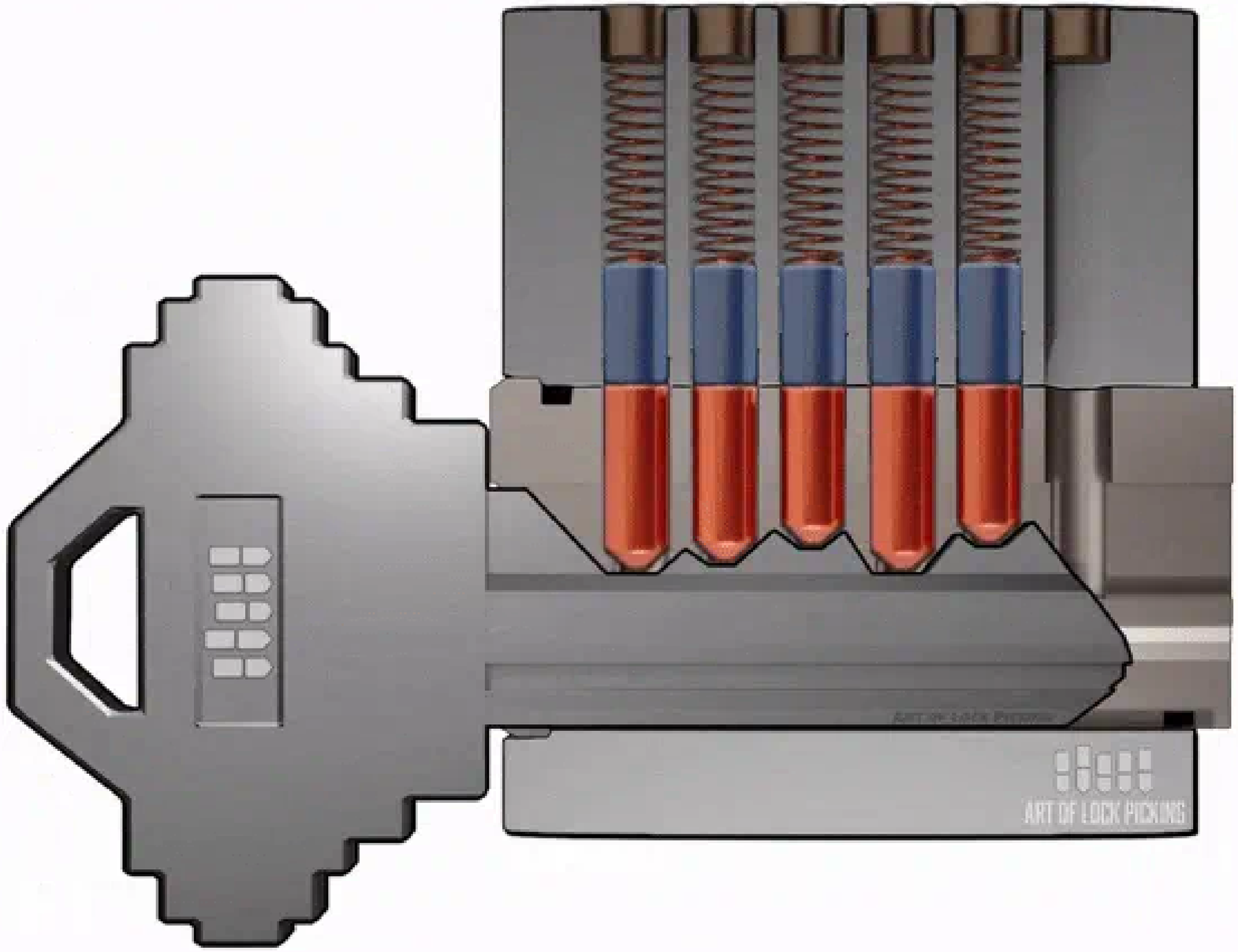
OBSTRUCT THE SHEAR LINE KEEPING LOCK CLOSED

ART OF LOCKPICKING



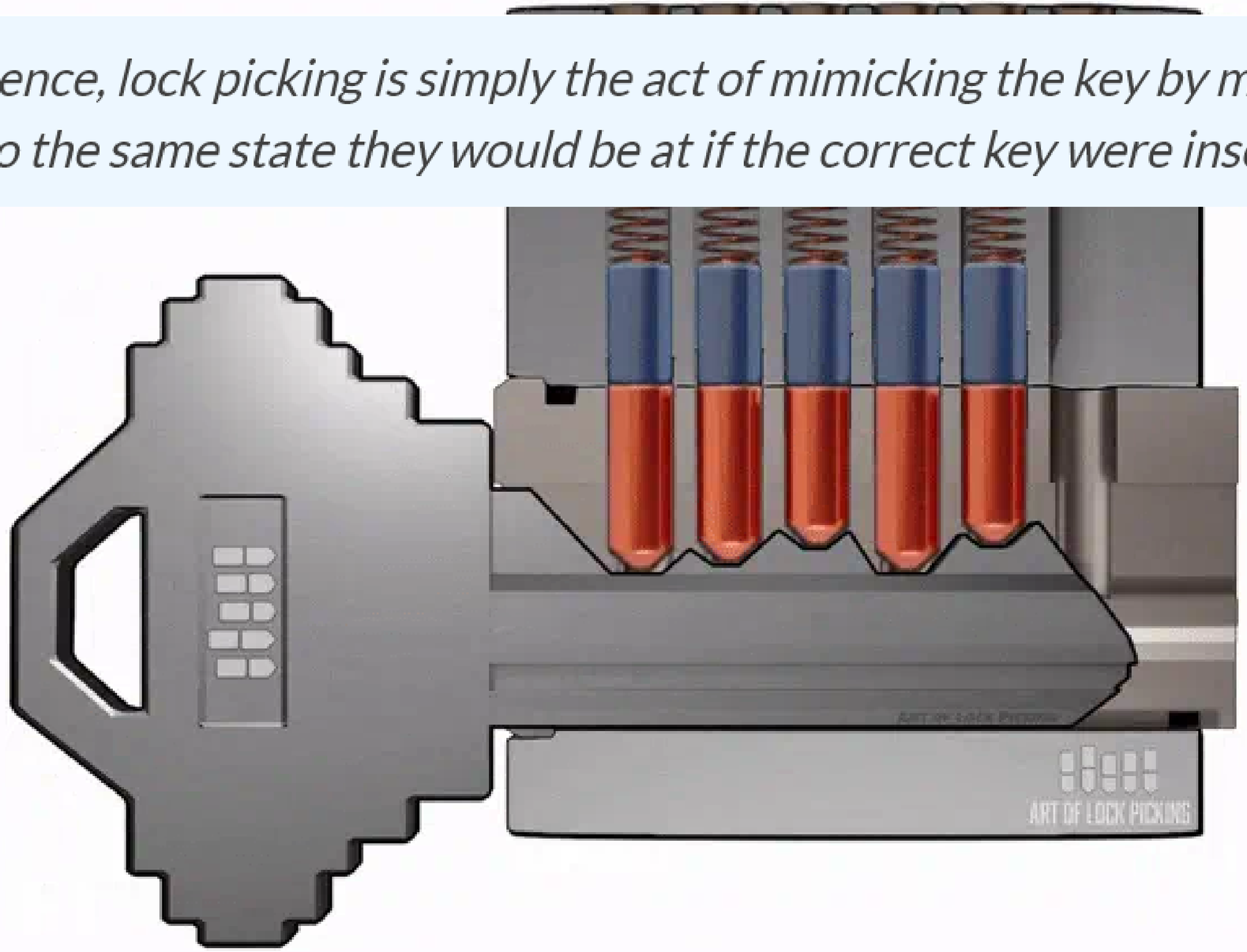
PUSH PINS INTO
THE PLUG BUT LET MOVE
WHEN KEY INSERTED

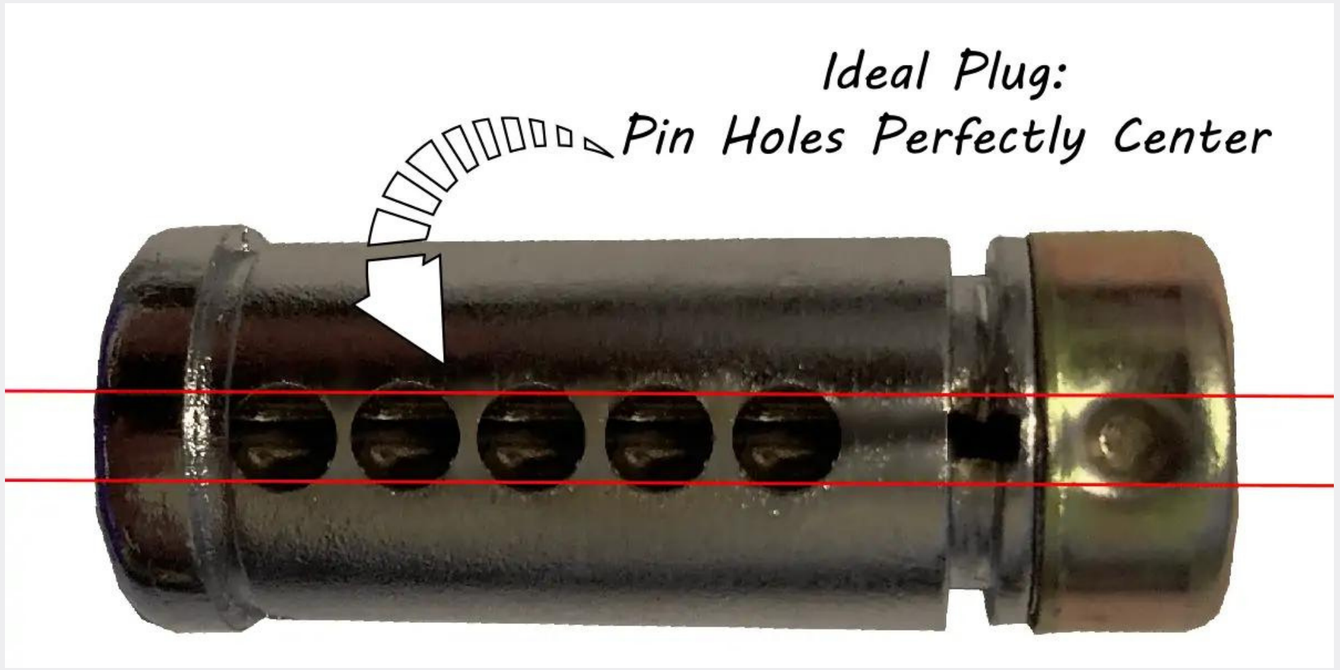
ART OF LOCKPICKING



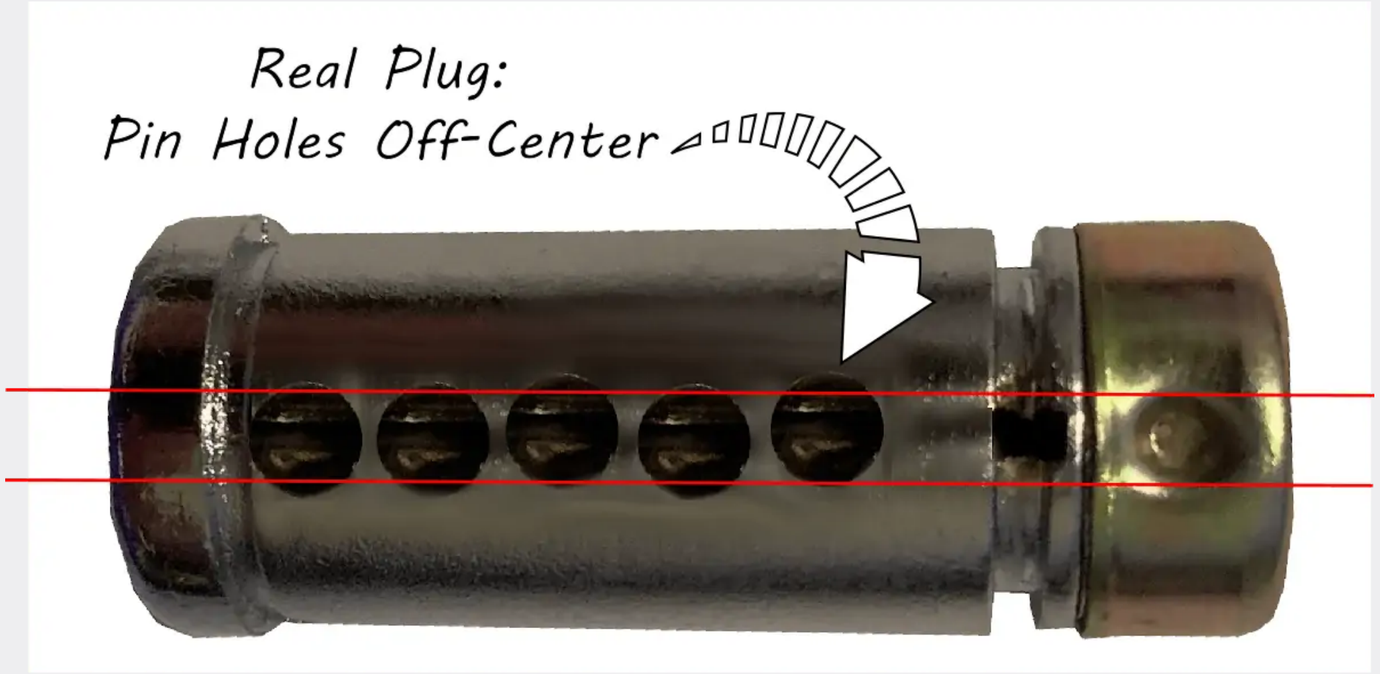
INSERTING KEY CLEARS SHEAR LINE

> *In essence, lock picking is simply the act of mimicking the key by manipulating the pins to the same state they would be at if the correct key were inserted.*



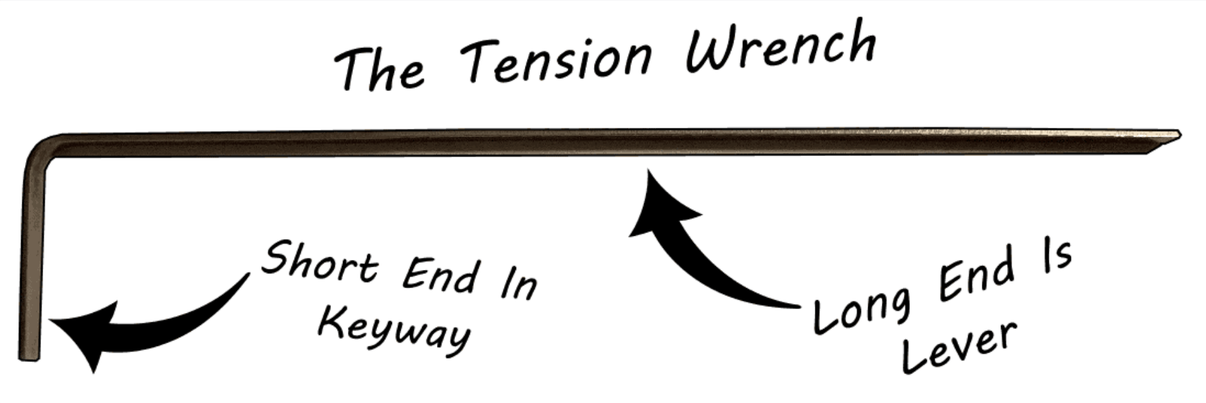


Misaligned holes means that as rotate plug that some pins will get stuck (“bind”).

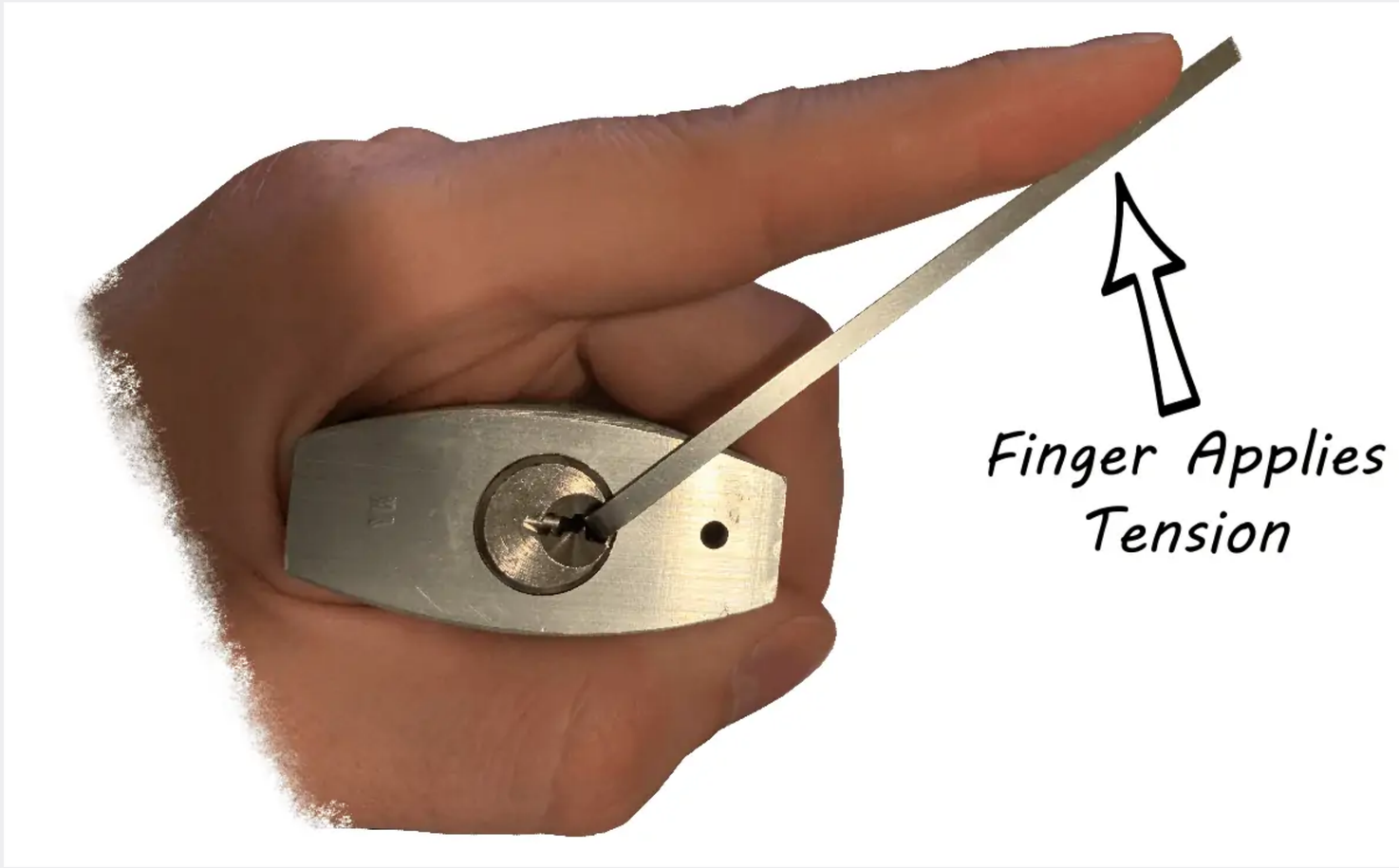


Allows pins to be popped one at at time until got them all.

Hook for popping pins.



Tension wrench for torque and binding pins.



Finger Applies Tension