LOCK PICKING

Cyber Security And Intel Club

Introductions

CIC will provide support for student learning by creating a community for those interested in cybersecurity and information security. Activities may range from student gatherings to industry speakers and professional conferences

President : Austin Turecek

Vice President: Samuel Munhal

Treasurer: Tyler Breuler

Secretary: Daniela Catrambone

Advisor: Doug White

LEGAL DISCLAIMER

- The Cyber Security and Intel Club, and its E-Board, do not hold any responsibility for any actions or consequences taken during or after this presentation. The information expressed in this presentation is purely for educational purposes. It is not to be used for any illegal or malicious actions. Any illegal or malicious actions are the sole responsibility of the perpetrator. The RWU Cyber Security and Intel Club holds no liability in these situations. However, any cool stories that occur due to this presentation should begin with "This one time at the Cyber Security and Intel Club, which you can join by signing up on Hawk Link, I learned…." By continuing to participate in this presentation and the demonstrations that follow, you agree to these terms and conditions.

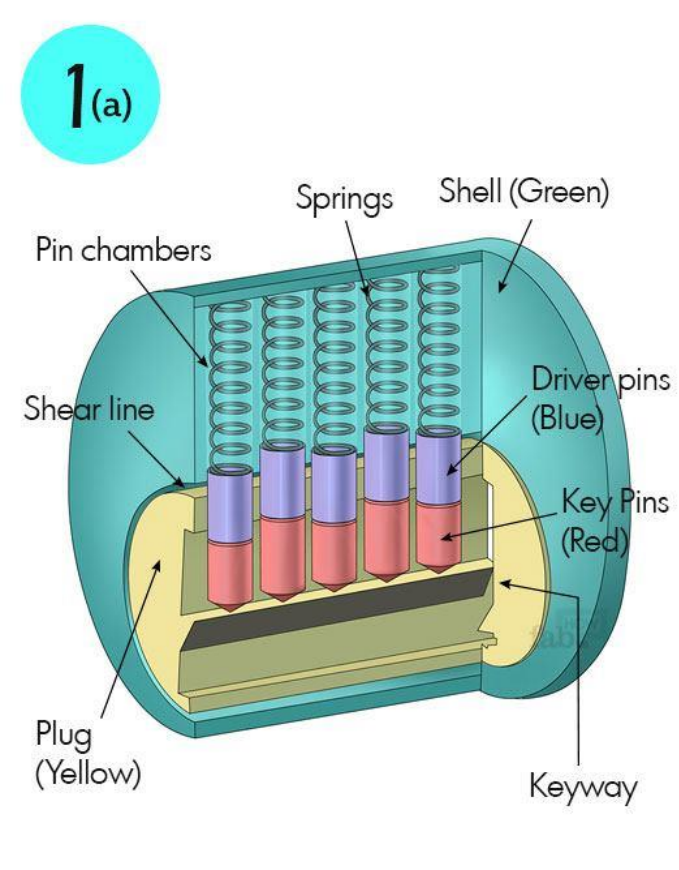
Lock Types

Lock Bypass Methods

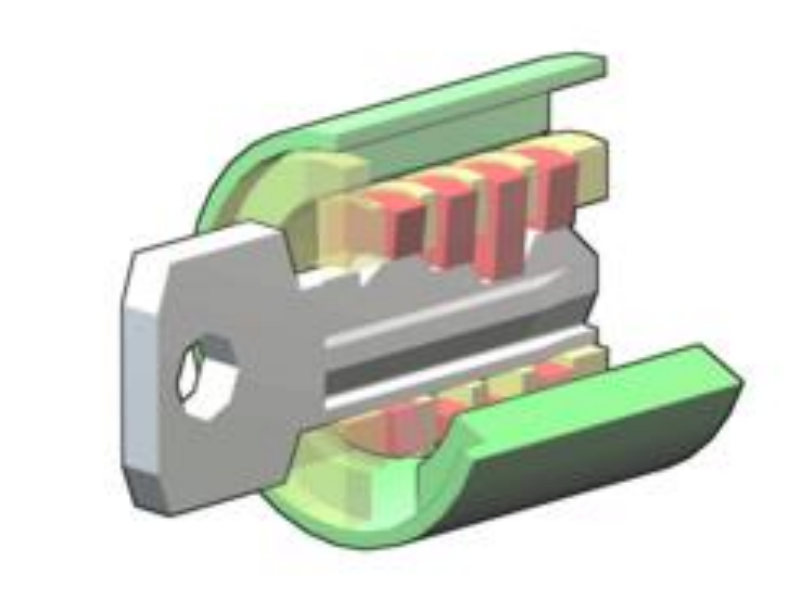
Least Noticeable

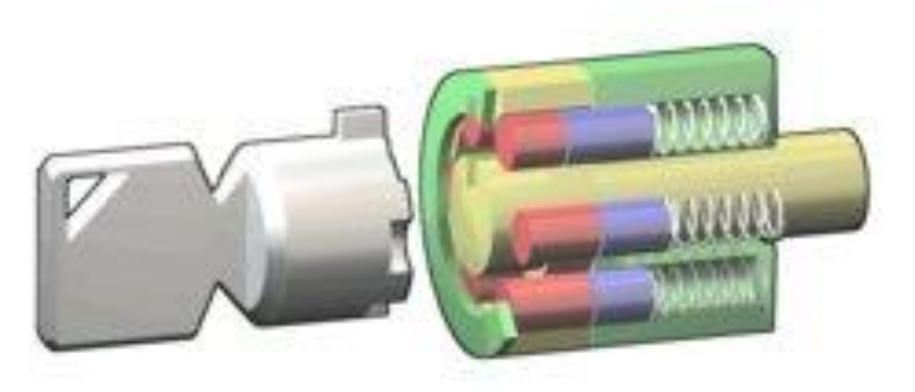
Most Noticeable

Lock Internals



Other Lock Guts





The Science of Picking

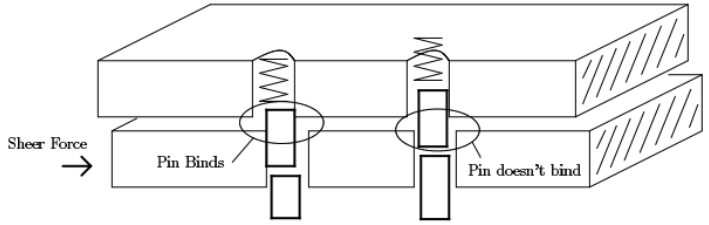


Figure 4.1: (a) Sheer force causes driver to bind

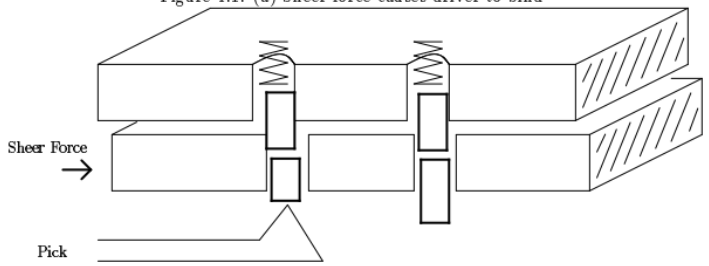


Figure 4.2: (b) Pick lifts the binding pin

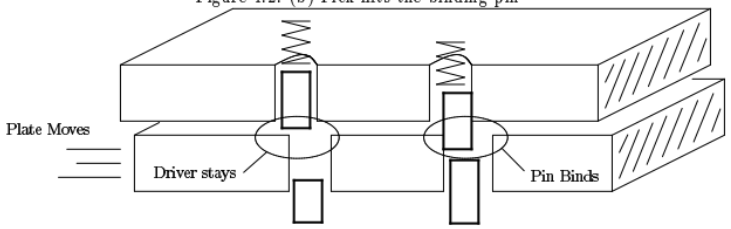


Figure 4.3: (c) Left driver sets and right driver binds

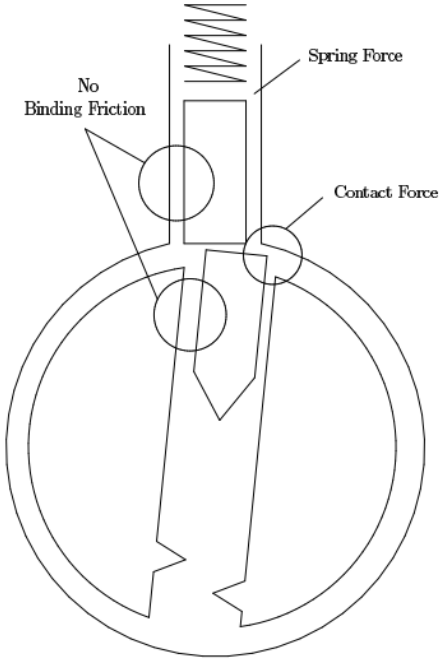


Figure 5.3: Pins at the sheer line

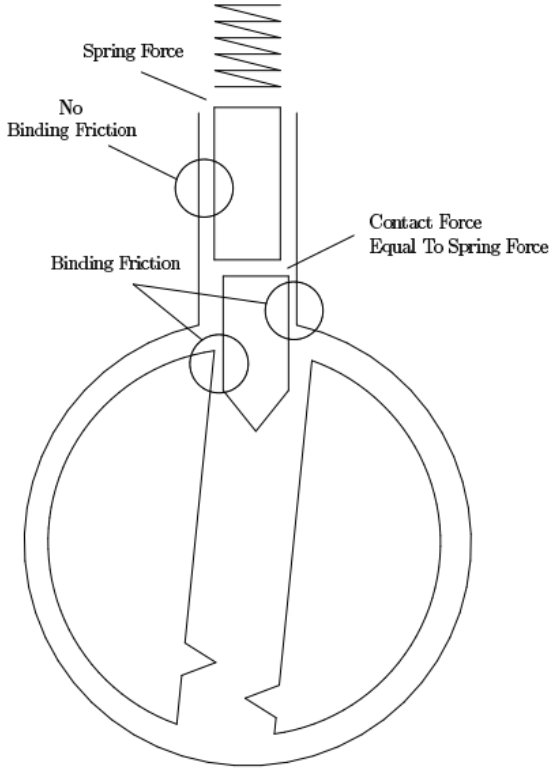


Figure 5.4: Key pin enters hull

The Actual Thing You Came Here For

1. Apply a sheer force.
2. Find the pin that is binding the most.
3. Push that pin up until you feel it set at the sheer line.
4. Go to step 2.

Table 4.1: Figure 5: Picking a lock one pin at a time.

1. Insert the pick and torque wrench. Without applying any torque pull the pick out to get a feel for the stiffness of the lock's springs.
2. Apply a light torque. Insert the pick without touching the pins. As you pull the pick out, apply pressure to the pins. The pressure should be slightly larger than the minimum necessary to overcome the spring force.
3. Gradually increase the torque with each stroke of the pick until pins begin to set.
4. Keeping the torque fixed, scrub back and forth over the pins that have not set. If additional pins do not set, release the torque and start over with the torque found in the last step.
5. Once the majority of the pins have been set, increase the torque and scrub the pins with a slightly larger pressure. This will set any pins which have set low due to beveled edges, etc.

Table 6.1: Figure 13: Basic scrubbing.

Challenges You Gotta Deal With

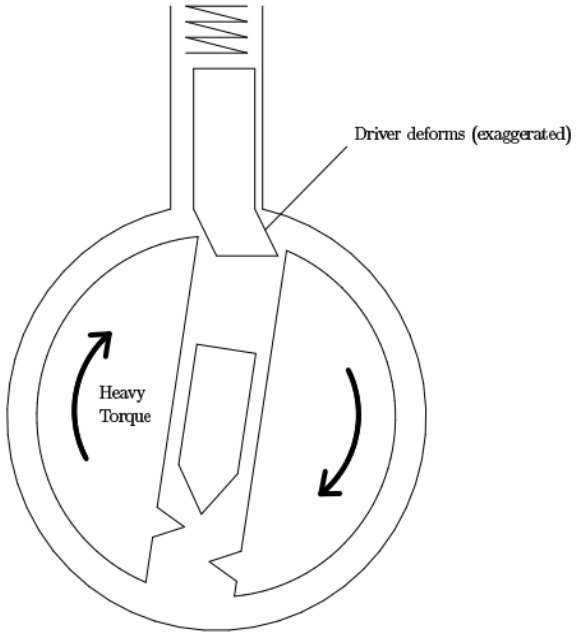


Figure 9.2: Driver pin false set by elastic deformation

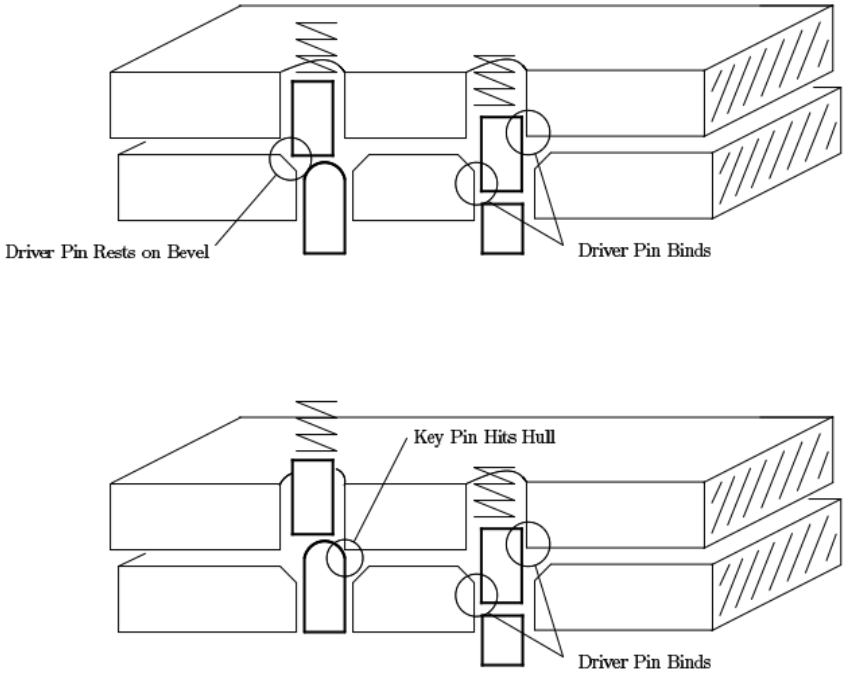


Figure 9.4: Beveled plug holes and rounded key pins

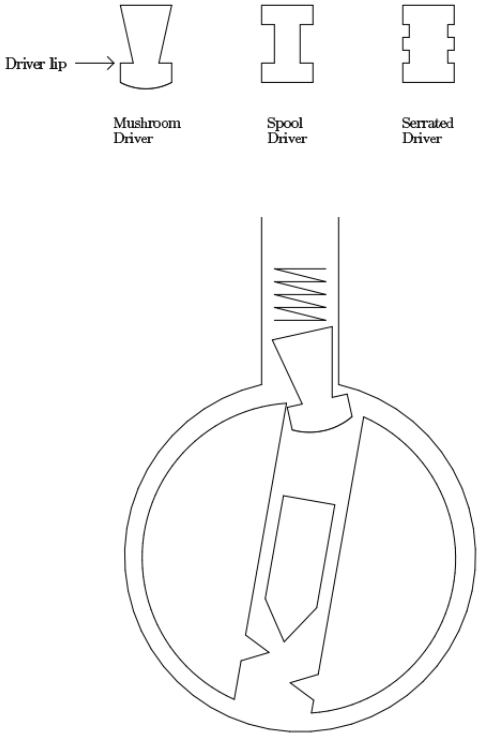


Figure 9.7: Mushroom, spool, and serrated driver pins

More Challenges You Gotta Deal With (Sorry)

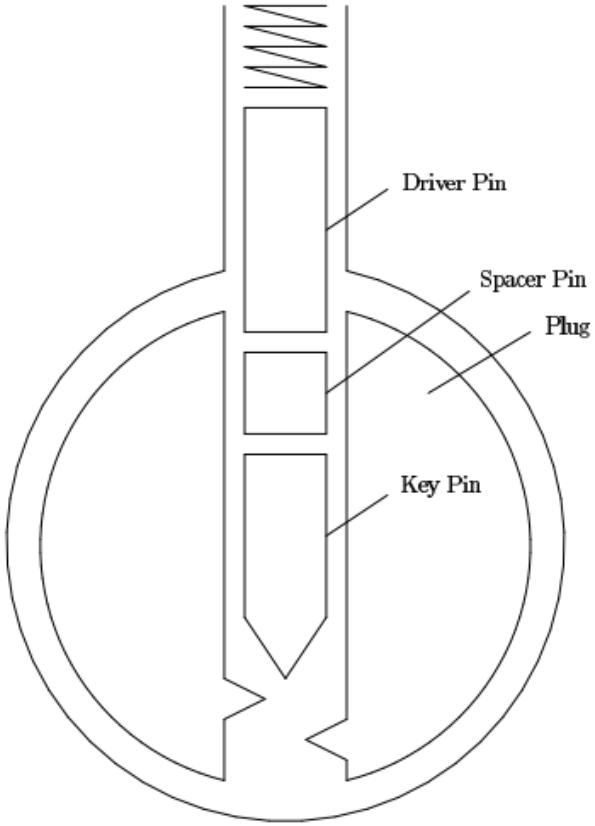


Figure 9.8: Spacer pins for master keying

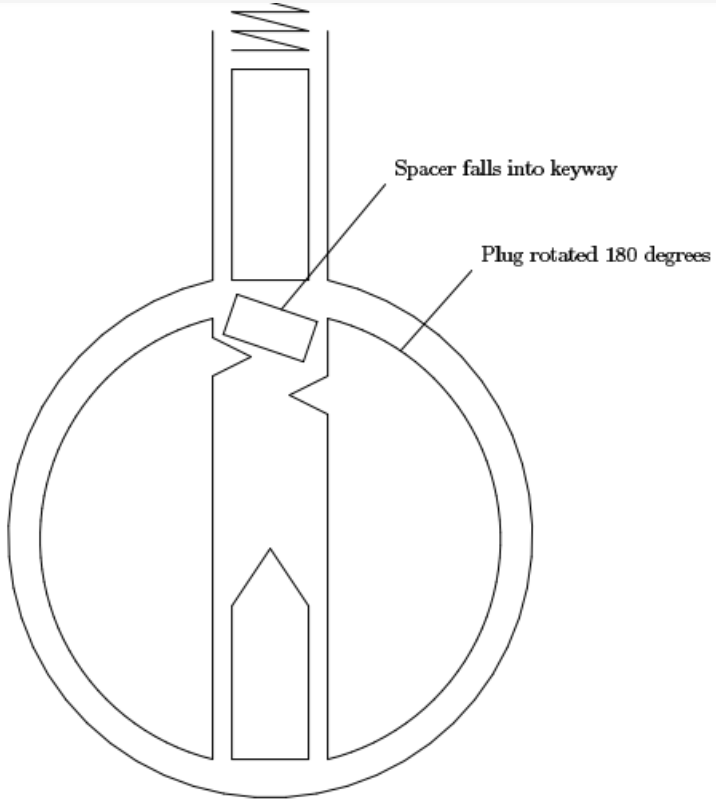
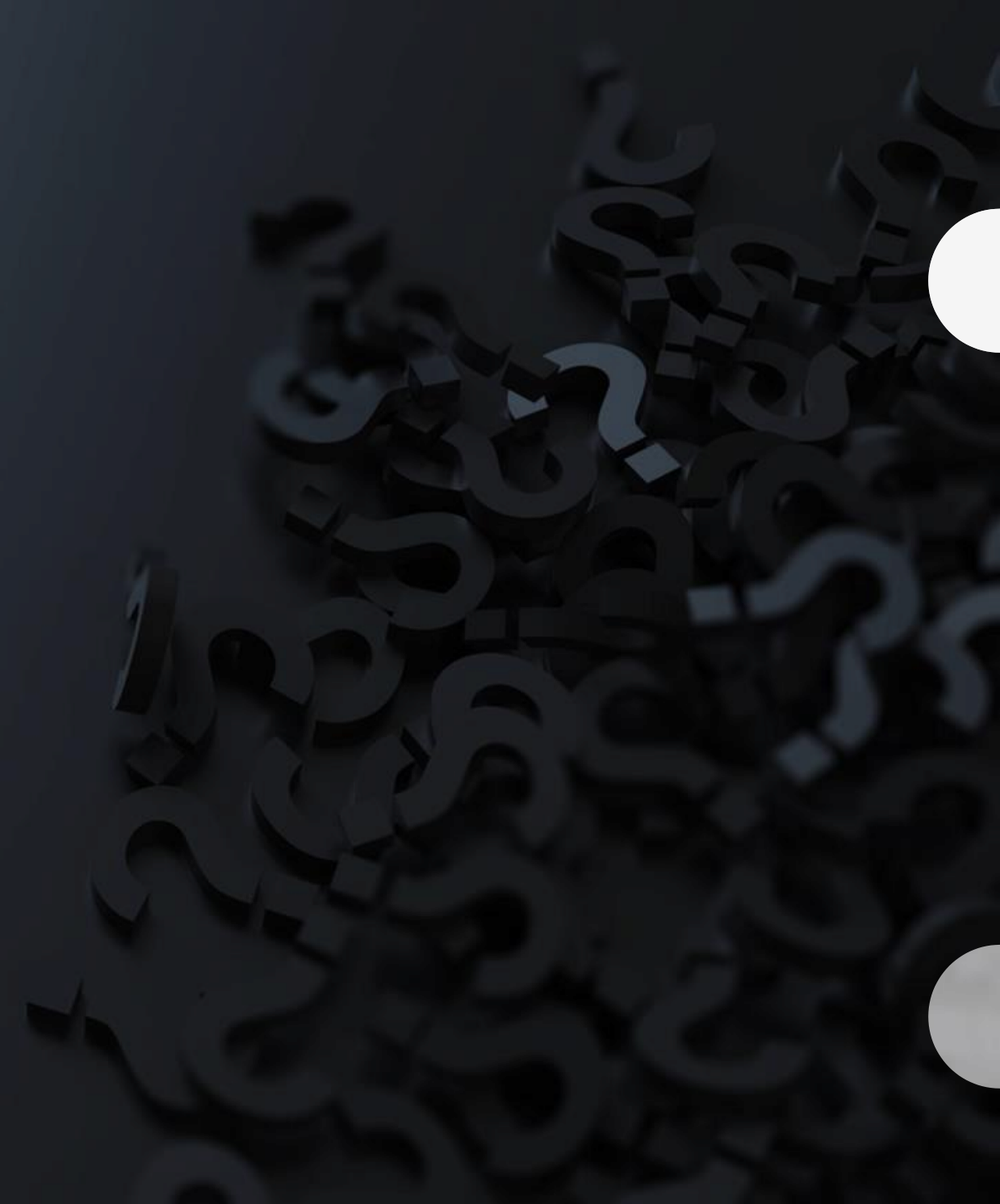


Figure 9.9: Spacer or driver can enter keyway

QUESTIONS?



DEFCON®

THANK YOU

- https://www.lysator.liu.se/mit-guide/MITLockGuide.pdf
- http://www.lockpickguide.com/

Resources

LET'S PICK SOME LOCKS