Lock Picking—

a pin tumbler design primer

While a little physical dexterity and patience goes a long way, lock picking is a skill, and you can learn it.

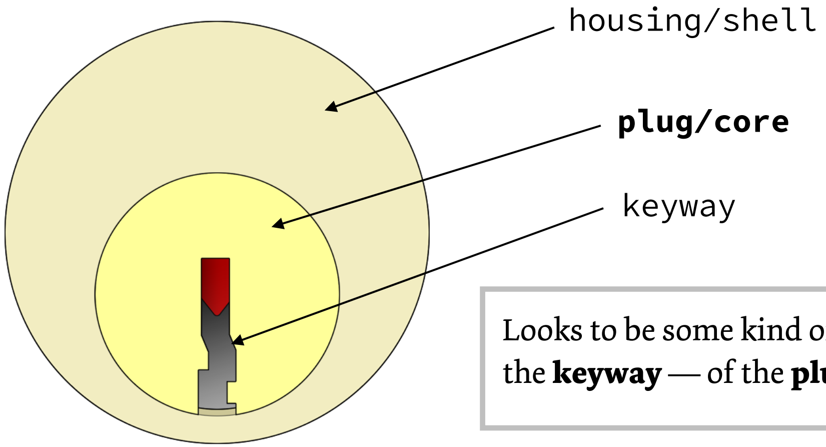
Locks can be picked because:

1. they're made of **mechanical components** with **tolerances** and **imperfections**
2. there are **design flaws** (related: the security–usability intersection)

In understanding how to pick a (pin tumbler) lock it's helpful to begin with how the key unlocks the mechanism.

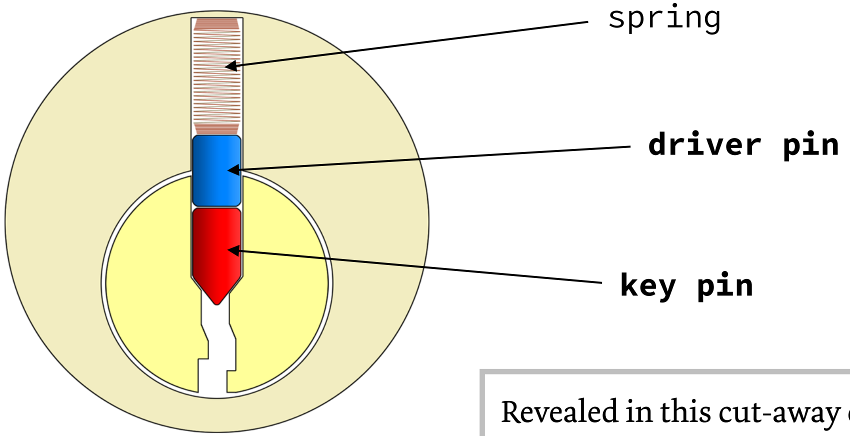
Once you understand this design you'll understand the fundamentals to vast majority of current locks, and have grounding to understand many, if not currently most other designs.

1. The outer view



Looks to be some kind of *pin* inside the opening — the **keyway** — of the **plug** or **core**...

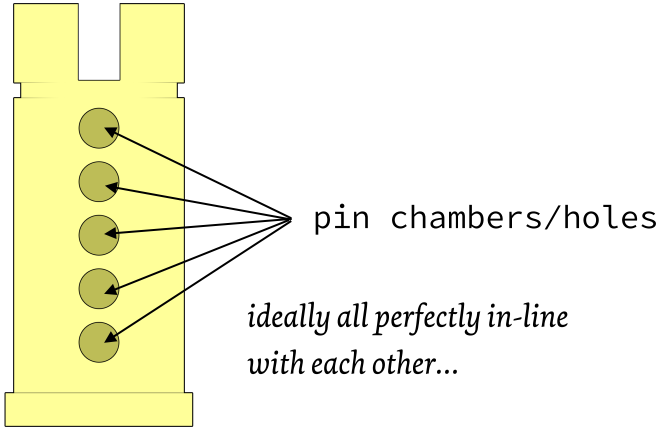
2. The inner view



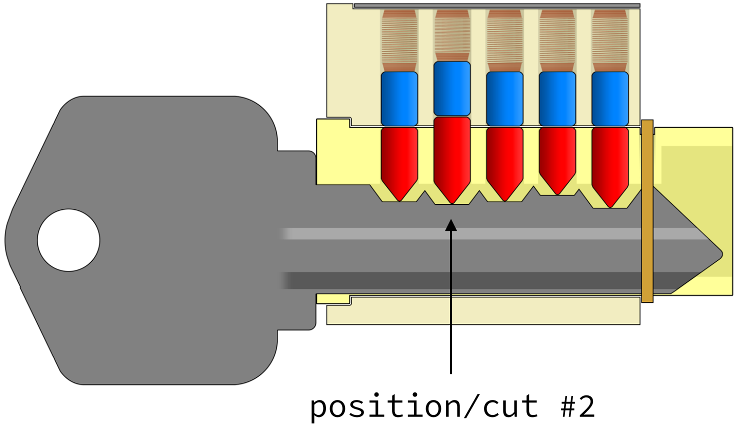
Revealed in this cut-away diagram are further pins — **driver pins**. These obstruct the free rotation of the **plug** inside the **housing** or **shell**.

To understand how **key pins** and **driver pins** interact let's look the **plug** from the top and side-on:

3. Core/plug, top view

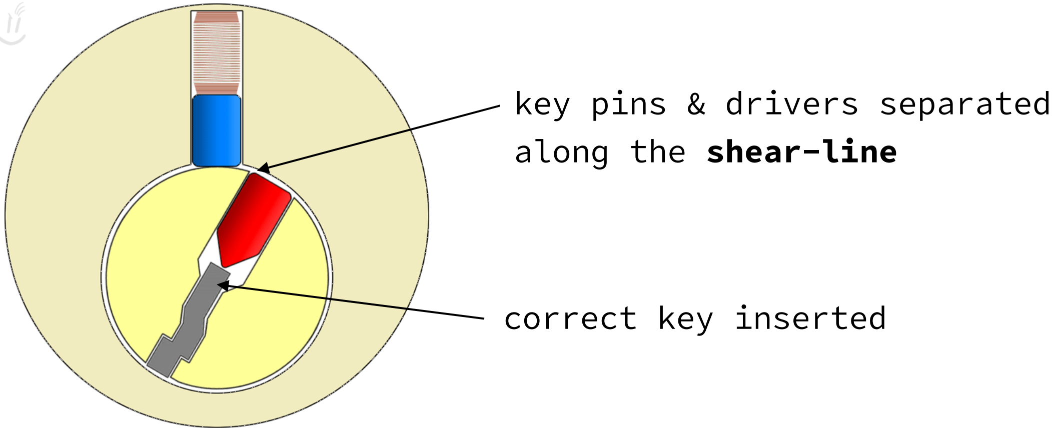


4. Side-view (wrong key)



Each chamber holds a **pin stack** — a **spring**, a **driver** and a **key pin**. When a key is inserted, the *cuts* on the key will determine how far each *pin stack* is compressed against its spring. A *working key* compresses all stacks such that all key pins and drivers *divide* neatly along the **shear-line**, allowing the plug to *rotate* freely inside the housing.

5. Operating key

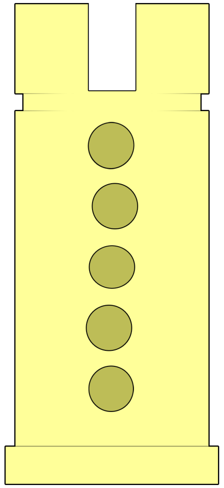


Returning to diagram #4, observe the second cut on the key (from the left; the *key shoulder*): it's *cut too high* — this key is not the correct operating key for this lock because the cut compresses the key pin *above* the dividing **shear-line** between the plug and the housing. Similarly, if a key's cut is *too low* then the corresponding **driver pin** would also block the plug's rotation.

So, picking? How do we use these two tools to open the lock without a key?

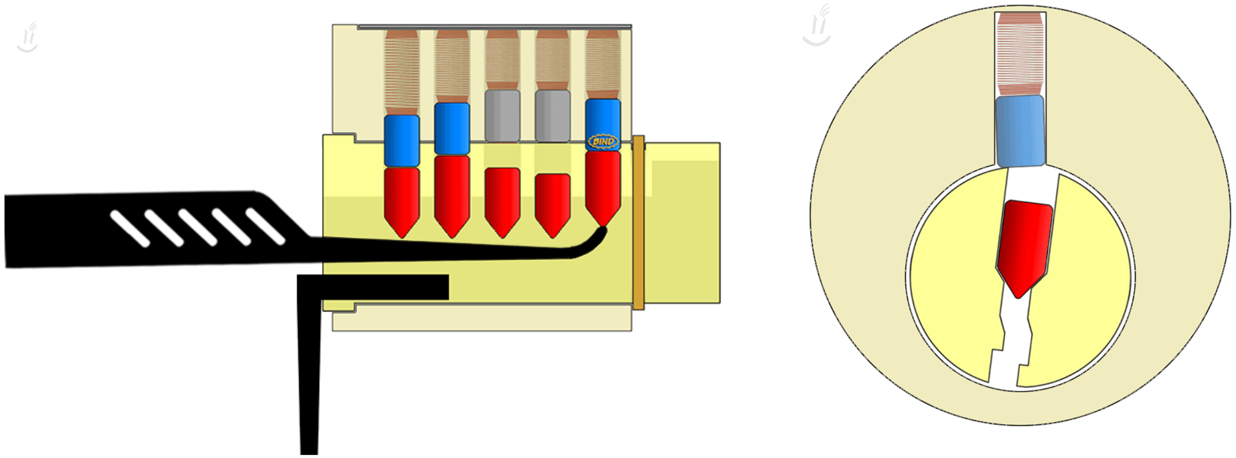
IN SHORT: (due to tolerances and imperfections) when applying *tension/torque* to the plug via a **tension** or **torque tool** it is possible to manipulate the key pins, *compressing* each **pin stack** such that they **bind,** between the **plug** and the **housing**, and ultimately **capture** or 'set' a driver pin at the **shear-line**, *separating* the pin stack.

Notable imperfections include the *alignment* of the plug's chambers or holes, and the *widths* of both the key and driver pins.



Even very good locks have tolerances to exploit.

When *torque* is applied to the plug of a lock in its locked state *one or more* **pin stacks** will *bind against* the walls of the chambers/holes. In locks with poorer tolerances multiple stacks may bind at once; in locks with tight tolerances only a single stack might bind at a given time.



What now? Find the **binding stack** or 'binder' and gently compress the stack without applying too much torque (to avoid seizing up the lock completely). You may have to let off a little tension — just enough — to **clear** or **set** that pin stack. Be careful though: if you let off too much previously-set pins will fall back/reset themselves due to the pin stack's spring!

Torque or **tension control** is *more important* here than the manipulation of the key pin.

I keep resetting pin stacks? Locks with tighter tolerances have a **binding order**. This is the order in which the pin stacks bind, successively, after picking the previous pin stack(s). Herein lies the skill: differentiating *picked* from *unpicked stacks*, and identifying the stack that is binding the most (that which needs to be picked next).

Addendum

This is just a primer — talk to us about...

- security pins
- kinetic attacks (bumping, raking, snappers)
- lock–bolt interaction
- bypass attacks

...and anything else lock-related!

Credits

Deviant Ollam — `diagrams`

Topaz — `instructor`

Wily — `instructor`

klepas — `instructor`

License

Resources

Docs / Guides / Info

The MIT *Guide to Lock Picking* — PDF. Google it. Indispensable.

TOOOL — *The Open Organization of Lockpickers*. In particular, Deviant's diagrams: `http://toool.us/deviant/index.html` and *Resources* `http://toool.us/resources.html`

Deviant Ollam's slides for his presentations: `http://deviating.net/lockpicking/slides.html`

YouTube

Amongst many others, '*BosnianBill*' (particularly prolific and educational picker): `https://www.youtube.com/user/bosnianbill`

Forums (en)

Forum: `https://keypicking.com`

Forum: `http://www.lockpicking101.com`

Gear

Local: `https://www.lockpicksaustralia.com.au`

Local: `http://pickpals.com.au`

[Don't pick locks you don't own, or do not have express permission to pick, and avoid picking operational locks (or you might damage them).]