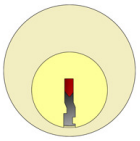
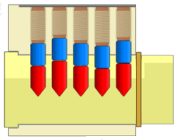
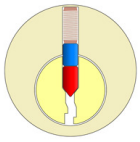
The One Page Guide to Lockpicking *by* Eric Van Albert, *pictures by* deviant, *courtesy of* TOOOL

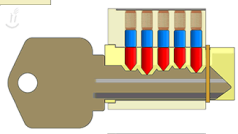


A pin tumbler lock is composed of a **hull** and a cylindrical **plug**. A **keyway** cut into the plug allows access to the lock internals. The plug rotating with respect to the hull constitutes **opening the lock** and will actuate other mechanisms such as retracting a bolt or freeing a shackle.

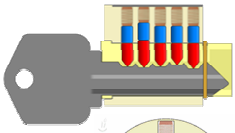




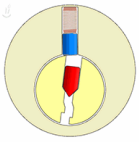
Vertical holes penetrate the hull and the plug, creating several **chambers**. These chambers are populated with **pins** that can slide up and down. The plug cannot rotate because pins span the **shear line,** the interface between the plug and the hull.



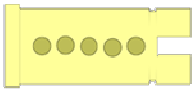
Each chamber contains a **pin stack** and a spring. The pin stack consists of the **key pin** (red), and the **driver pin** (blue). The spring pushes the pin stack into the keyway. The correct key interacts with the key pins and raises each one so that the split in the pin stack lies at the shear line. This removes all obstructions from the shear line and allows the plug to rotate.



A key whose cuts are too high or too low will cause the pin stacks to be raised too high or too low, blocking plug rotation with either the key pin or the driver pin, respectively.

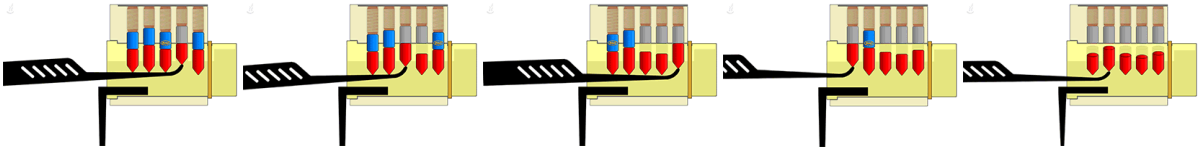


A one-pin lock may be picked by applying a slight amount of torque to the plug, creating a shear force at the shear line. The plug will not rotate because the driver pin will **bind**. Raising the pin stack until it reaches the shear line will cause the driver pin to fully enter the hull, at which point the plug will rotate and the key pin will drop back down into the plug, no longer under spring force.



Mechanical defects allow for locks with multiple pins to be picked. The chamber holes must be slightly larger than the pins to allow easy vertical movement, and to account for slight misalignments between the holes in the hull and the holes in the plug.

This means that when light torque is applied to the plug, only one pin stack will bind. When it is raised to the shear line, the plug will rotate until another pin stack binds. Due to this slight rotation, the first pin stack will experience a pinch-off effect, holding the driver pin up and the key pin down and loose. The pin stack is said to be **set**. The process is repeated until every pin stack is set and the lock opens. Using this technique, a lock with several pins is reduced to several locks with one pin. However, the **binding order** is unpredictable and must be determined by feel.



The tool used to apply torque is called the **tension wrench**, and the tool used to manipulate the pins is called the **pick**. There are many different types of picks, the most common being the **hook pick**, shown here.

Depending on manufacturing tolerances, the displacement at the shear line due to setting a pin may be less than one thousandth of an inch. This makes it very easy to accidentally un-set a pin. It also makes it very easy to **over-lift** a pin (lifting the key pin above the shear line and binding it in place.) If a pin is over-lifted, the lock will never open unless pressure on the tension wrench is removed. The easiest way to avoid over-lifting pins is *light pressure on the torque wrench*, preventing pins from binding too tightly, and a *light touch on the pick*, preventing over-lifting.

One technique for setting pins is **raking,** which uses a long tool called a **rake** that interacts with multiple pins. By jiggling the rake around inside a lock, pins will set randomly. Unfortunately, they can also over-lift and un-set randomly if too little or too much force is used. Raking can be fast, but it is not very precise, and often needs to be supplemented by **single-pin-picking** (the technique pictured above.)

A Potential Danger of Lockpicking

Rotating the plug 180 degrees may cause the driver pins to fall into the keyway, locking the plug in place. Worse yet, a thin **master wafer** (a third pin in a pin stack, used for master-keyed systems) may fall into the keyway and out of the lock entirely. This prevents the lock from working when the key is inserted.

This can be avoided by pressing the back of the pick against the bottom of the keyway, thus holding back the drivers and master wafers as the lock is rotated past the 180 degree point.

Another technique for opening a lock is called **bumping**. Bumping involves using a specially cut "bump" key and a hammer to apply large amounts of energy to the pins. While they are bouncing around, there is likely to be an instant where they are all split at the shear line, at which point the plug can turn. While simple and quite effective, bumping wears down locks much faster than picking, and can easily damage them if done recklessly.

Several variations exist on this simple **pin tumbler** design, ranging from pick-resistant pin shapes to secondary locking mechanisms such as the sidebars present on the Medeco Biaxial and Schlage Primus. Most of these features make the locks difficult to pick, but they may have other exploits. In any case, it is important to research a lock before attacking it.