MIT Guide to Lock Picking

Ted the Tool

September 1, 1991

Distribution

Copyright 1987, 1991 Theodore T. Tool. All rights reserved.

Permission to reproduce this document on a non-profit basis is granted provided that this copyright and distribution notice is included in full. The information in this booklet is provided for educational purposes only.

August 1991 revision.

Contents

Chapter 1

It's Easy

The big secret of lock picking is that it's easy. Anyone can learn how to pick locks.

The theory of lock picking is the theory of exploiting mechanical defects. There are a few basic concepts and definitions but the bulk of the material consists of tricks for opening locks with particular defects or characteristics. The organization of this manual reflects this structure. The first few chapters present the vocabulary and basic information about locks and lock picking. There is no way to learn lock picking without practicing, so one chapter presents a set of carefully chosen exercises that will help you learn the skills of lock picking. The document ends with a catalog of the mechanical traits and defects found in locks and the techniques used to recognize and exploit them. The first appendix describes how to make lock picking tools. The other appendix presents some of the legal issues of lock picking.

The exercises are important. The only way to learn how to recognize and exploit the defects in a lock is to practice. This means practicing many times on the same lock as well as practicing on many different locks. Anyone can learn how to open desk and filing cabinet locks, but the ability to open most locks in under thirty seconds is a skill that requires practice.

Before getting into the details of locks and picking, it is worth pointing out that lock picking is just one way to bypass a lock, though it does cause less damage than brute force techniques. In fact, it may be easier to bypass the bolt mechanism than to bypass the lock. It may also be easier to bypass some other part of the door or even avoid the door entirely. Remember: There is always another way, usually a better one.

Chapter 2

How a Key Opens a Lock

This chapter presents the basic workings of pin tumbler locks, and the vocabulary used in the rest of this booklet. The terms used to describe locks and lock parts vary from manufacture to manufacture and from city to city, so even if you already understand the basic workings of locks, you should look at figure 2.1 for the vocabulary.

Knowing how a lock works when it is opened by a key is only part of what you need to know. You also need to know how a lock responds to picking. Chapters 3 and 5 present models which will help you understand a lock's response to picking.

Figure 2.1 introduces the vocabulary of real locks. The key is inserted into the *keyway* of the *plug*. The protrusions on the side of the keyway are called *wards*. Wards restrict the set of keys that can be inserted into the plug. The plug is a cylinder which can rotate when the proper key is fully inserted. The non-rotating part of the lock is called the *hull*. The first pin touched by the key is called pin one. The remaining pins are numbered increasingly toward the rear of the lock.

The proper key lifts each pin pair until the gap between the *key pin* and the *driver pin* reaches the *sheer line*. When all the pins are in this position, the plug can rotate and the lock can be opened. An incorrect key will leave some of the pins protruding between the hull and the plug, and these pins will prevent the plug from rotating.

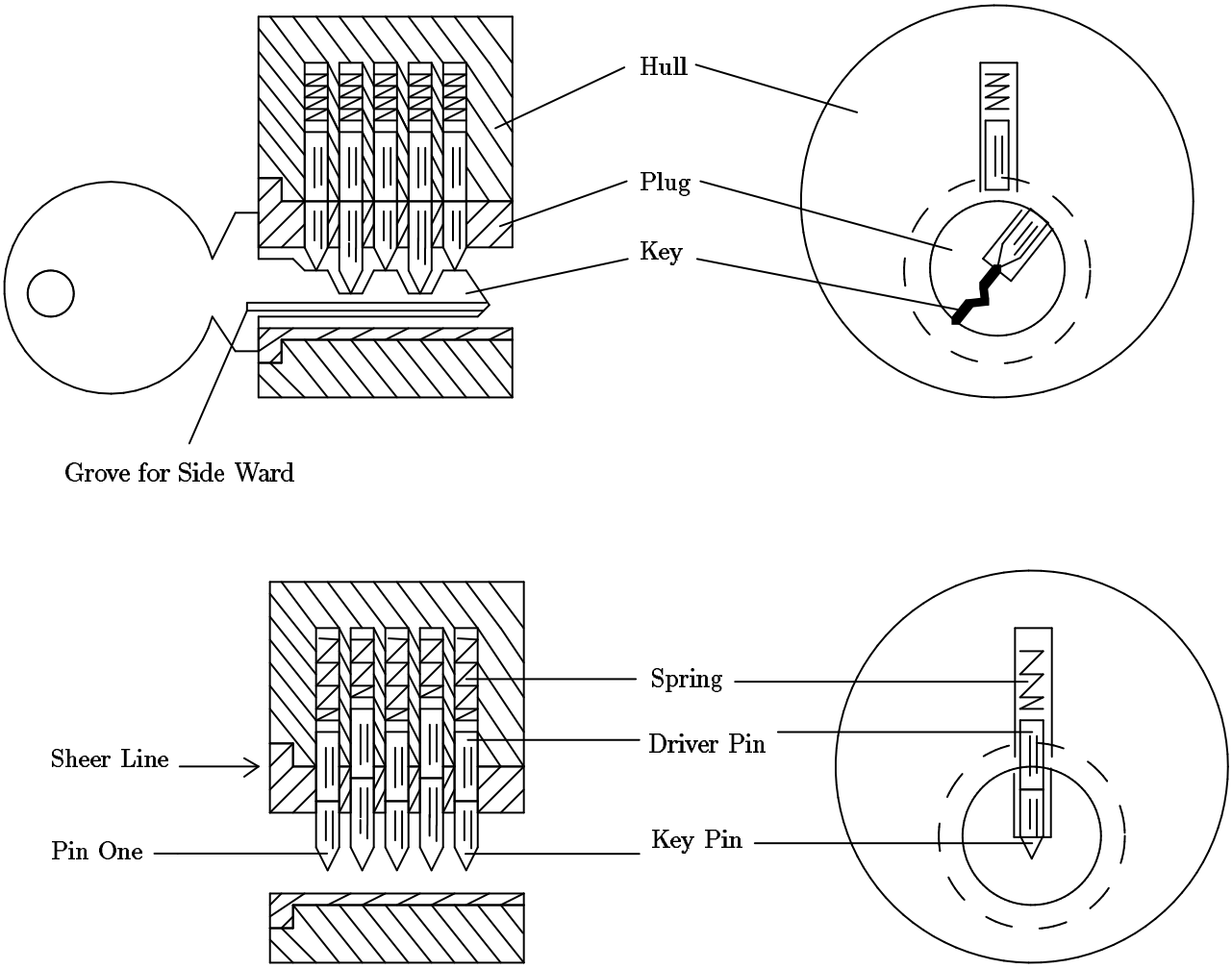

Figure 2.1: Workings of pin tumbler locks

Chapter 3

The Flatland Model

In order to become good at picking locks, you will need a detailed understanding of how locks works and what happens as it is picked. This document uses two models to help you understand the behavior of locks. This chapter presents a model that highlights interactions between pin positions. Chapter 4 uses this model to explain how picking works. Chapter 9 will use this model to explain complicated mechanical defects.

The "flatland" model of a lock is shown in Figure 3.1. This is not a cross section of a real lock. It is a cross section of a very simple kind of lock. The purpose of this lock is to keep two plates of metal from sliding over each other unless the proper key is present. The lock is constructed by placing the two plates over each other and drilling holes which pass through both plates. The figure shows a two hole lock. Two pins are placed in each hole such that the gap between the pins does not line up with the gap between the plates. The bottom pin is called the *key pin* because it touches the key. The top pin is called the *driver pin*. Often the driver and key pins are just called the driver and the pin. A protrusion on the underside of the bottom plate keeps the pins from falling out, and a spring above the top plate pushes down on the driver pin.

If the key is absent, the plates cannot slide over each other because the driver pins pass through both plates. The correct key lifts the pin pairs to align the gap between the pins with the gap between the plates. See Figure 3.3. That is, the key lifts the key pin until its top reaches the lock's sheer line. In this configuration, the plates can slide past each other.

Figure 3.3 also illustrates one of the important features of real locks. There is always a sliding allowance. That is, any parts which slide past each other must be separated by a gap. The gap between the top and bottom plates allows a range of keys to open the lock. Notice that the right key pin in Figure 3.3 is not raised as high as the left pin, yet the lock will still open.

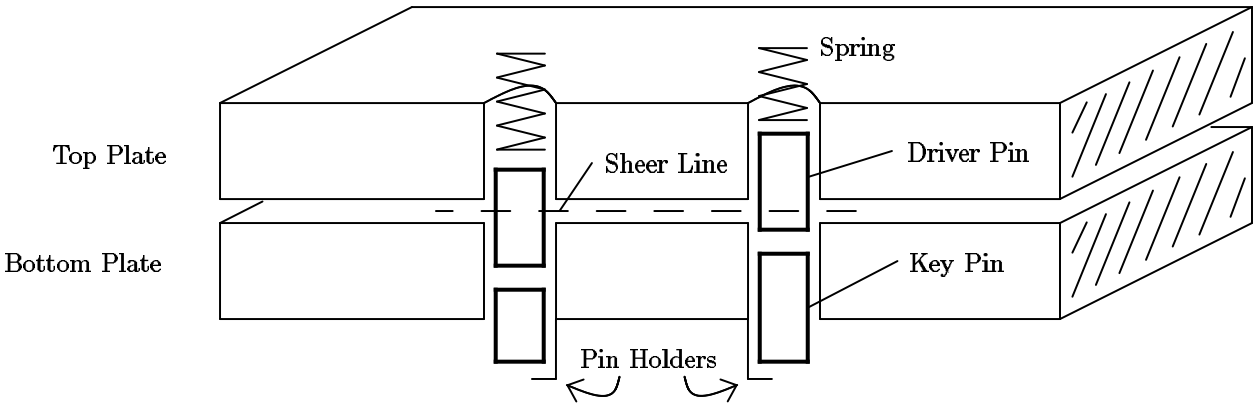

Figure 3.1: Flatland model of a lock

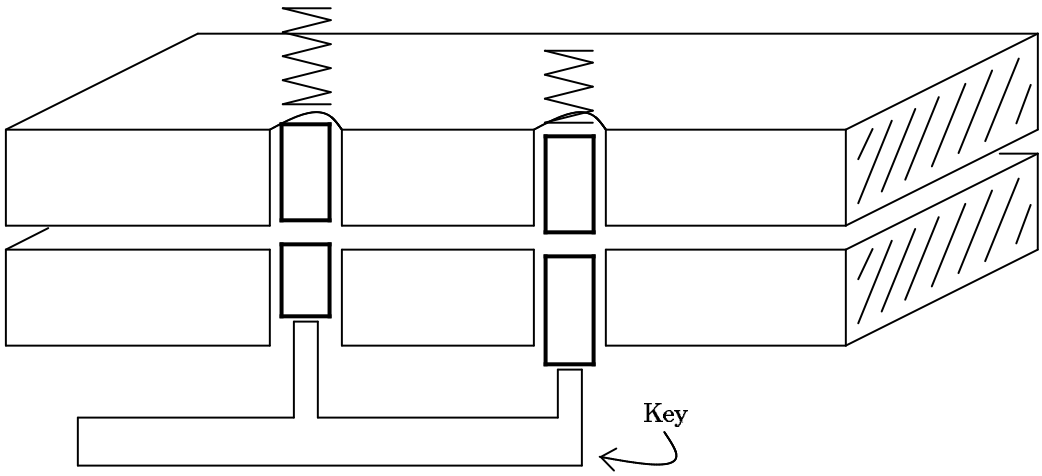

Figure 3.2: (a) Flatland key raises pins

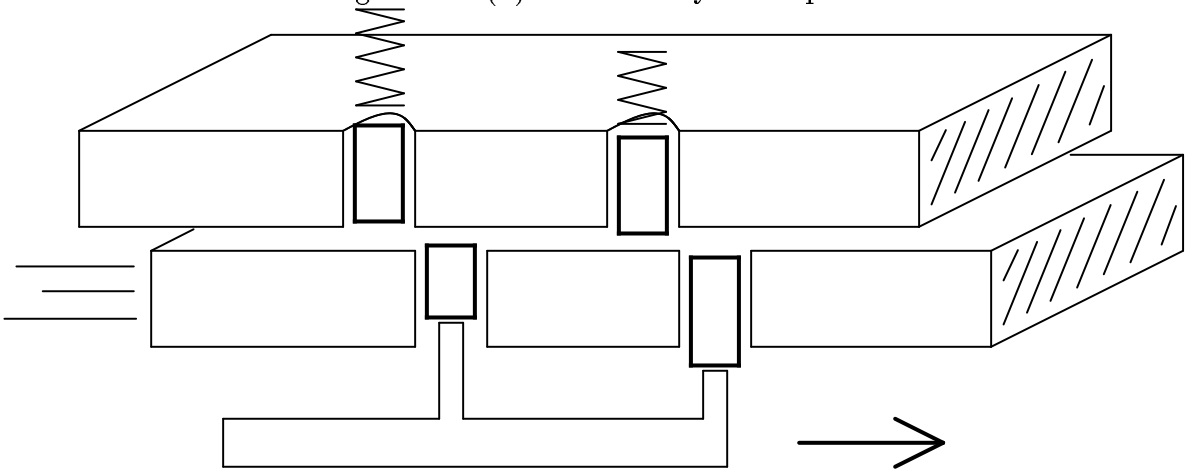

Figure 3.3: (b) Proper key allows plates to slide

Chapter 4

Basic Picking & The Binding Defect

The flatland model highlights the basic defect that enables lock picking to work. This defect makes it possible to open a lock by lifting the pins one at a time, and thus you don't need a key to lift all the pins at the same time. Figure 4.3 shows how the pins of a lock can be set one at a time. The first step of the procedure is to apply a sheer force to the lock by pushing on the bottom plate. This force causes one or more of the pins to be scissored between the top and bottom plate. The most common defect in a lock is that only one pin will bind. Figure 4.3a shows the left pin binding. Even though a pin is binding, it can be pushed up with a picking tool, see Figure 4.3b. When the top of the key pin reaches the sheer line, the bottom plate will slide slightly. If the pick is removed, the driver pin will be held up by the overlapping bottom plate, and the key pin will drop down to its initial position, see Figure 4.3c. The slight movement of the bottom plate causes a new pin to bind. The same procedure can be used to set the new pin.

Thus, the procedure for *one pin at a time picking* a lock is to apply a sheer force, find the pin which is binding the most, and push it up. When the top of the key pin reaches the sheer line, the moving portion of the lock will give slightly, and driver pin will be trapped above the sheer line. This is called *setting* a pin.

Chapter 9 discusses the different defects that cause pins to bind one at a time.

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.

Thank You for previewing this eBook

You can read the full version of this eBook in different formats:

- HTML (Free /Available to everyone)
- PDF / TXT (Available to V.I.P. members. Free Standard members can access up to 5 PDF/TXT eBooks per month each month)
- Epub & Mobipocket (Exclusive to V.I.P. members)

To download this full book, simply select the format you desire below