First Published in *Keynotes* Magazine/ June 2000

Unmasking the Master Key
by Sal Dulcamaro, CML

In this article, I will explain the mechanics of (split pin) mechanical master keying. I will show how one can decipher the master key bitting and an assortment of intended and unintended consequences of master keying. The more information available about the tumblers and operating keys, the faster and easier the technique used to unmask (or reveal) the master key will be. Some techniques I have learned from others over the years, while others I have developed on my own. It is my intent to call attention to certain basic realities of master keying, that are generally known by most locksmiths who have been schooled in the fundamentals of master keying, but not necessarily obvious to all locksmiths who create master key systems. Methods of labeling master (and change) keys and the terminology of the process may vary, but the inherent mechanical operation does not.

The basic operation of a pin tumbler lock cylinder involves the interaction of pin shaped tumblers within a series of pin chambers that begin at the top of the outer component (or shell) and continue in line downward to the inner component (or plug). In each chamber is typically three parts: a tumbler spring (at the top), a top pin or driver (in the middle) and a bottom pin at the bottom of the stack. In a standard (non-IC, non-master keyed) pin tumbler cylinder, there should be no more than two pins per chamber. The cuts of a correct key should raise the pin stacks sufficiently so the point where the top and bottom pins split will all line up at the top surface of the plug (shear line) simultaneously. Within the manufacturer's machining tolerances, such a lock cylinder will open with just one key cut pattern. A key that has cuts of different heights (outside the accepted tolerances of the lock) will not allow the pins to split at the shear line, and will not be able to open the lock.

The Mechanics of Master Keying

The mechanics will vary between locks with different types of tumblers. The overall concept will be similar. Here, I am specifically explaining about pin tumbler locks. Many of these principles will be identical to most (although not all) other types of tumbler based locks.

Most knowledgeable locksmiths realize that master key systems are created primarily for convenience. In a facility or building where many individuals need unique access to specific areas (other individual's keys will not operate their locks), while others of greater authority need access to overlapping (or all) areas; master keying is sometimes the only practical option. The other possible option is to give people in authority copies of all the individual keys that open the individual locks. In a facility with ten doors, ten individuals would each have his/her own key that would only open one of the ten. The person who needed access to all ten doors would have ten keys. With such a small number of doors, it is already apparent how inconvenient it is to have ten additional keys on one's key ring. Imagine a building with one hundred or one thousand doors. I think you get the picture.

Earlier I explained how a standard pin tumbler cylinder will only open with one key cut pattern. Having one key, then, allows access to just one area. As a result, the use of standard coded cylinders requires the possession of larger numbers of keys to gain a higher level of access in the facility. The more convenient setup would be to have locks that could be opened by unique individual user keys, and (at the same time) special high level access keys. In that situation, the individual users would not be able to open other locks with their (one door specific) keys, but the high level person could open all the differently coded doors with just one key. That is effectively the definition of master keyed locks.

A standard pin tumbler lock cylinder would need another split point in order to have more than one key cut pattern open the same lock. That requires the addition of a third pin to the chamber previously limited to two pins. The actual size of a master key system will depend on the number of increments possible per chamber in combination with the number of chambers that contain a third pin. My point in this article is not to show you how to create a master key system, so I won't go into any further detail about the capacity or design of a master key system. I will explain how you can use the rules of master keying to unmask the identity of the highest level master key (TMK-Top Master Key), when you don't have that key.

Decoding the Pin Tumbler Cylinder

When you have a non-master keyed pin tumbler cylinder, it is possible to decode the key combination by disassembling the cylinder and removing the bottom pins. By measuring the lengths of the bottom pins, you can compare the dimensions with the pin length specifications of that particular brand lock and convert those values to the direct digit bitting code. Since there is only one possible key cut combination, the pin pattern you find will coincide with the bitting of the one and only operating key cut pattern. When you start out with a master keyed pin tumbler cylinder and have no operating keys (individual change key or any level master key), the decoding process will involve a certain level of trial and error. Every chamber with a master pin will have two possible cut depths for that chamber position. With no operating keys available, you can't be certain as to which depth coincides with the master key and which with the change key. To minimize confusion, I will just make up a sample pinning pattern for a lock cylinder and go through the steps involved in finding the master key.

I will start out with the bottom and master pin combination for my sample lock. I will pretend it to be a five pin Schlage pin tumbler lock, but you could subsitute other brands with ten size increments with the same results. The pin combination is as follows.

Chamber Positions:	1	2	3	4	5

Master Pins:	2	4	4	4	4
Bottom Pins:	2	3	0	1	2

If you don’t already know it, here is how you determine the possible key cut depths for a pin chamber containing a bottom pin and a master pin. This will be determined chamber by chamber. The size of the bottom pin will always determine the depth of the shallower of the two possible cuts. The total combined value of adding the bottom pin size and the master pin above it will indicate the cut depth of the deeper of the two possible cuts for that chamber position. In the first chamber, the #2 bottom pin indicates a shallow cut depth of 2. Adding the #2 bottom pin and the #2 master pin, totals 4, which would be the deeper cut depth for that position. So either a #2 or #4 cut depth will cause a split at the shear line in chamber #1. You can do the math yourself, if you wish, but I will list the shallow and deep cut values possible with the bottom and master pin patterns shown above.

Chamber Positions:	1	2	3	4	5
Shallow Cut:	2	3	0	1	2
Deep Cut:	4	7	4	5	6

There is no rule that the shallow or deep cut is normally for the change key or Top Master Key (TMK). Any permutation of those two sets of cuts could be the TMK. I will list all the possible permutations with that set of numbers. One on the list will have to be the TMK.

The total will come to 32 possible key cut patterns. You can figure that by raising the number 2 to the nth power, with n equalling the number of chambers with three pins. That is 2 to the 5th power or: 2x2x2x2x2. If you had problems in school with math, this might not make a lot of sense to you. You don’t need to know how I determined that there would be 32 possible key cut patterns, so I will list all 32 here for you to see.

1)	23012	2)	23016	3)	23052	4)	23056
5)	23412	6)	23416	7)	23452	8)	23456
9)	27012	10)	27016	11)	27052	12)	27056
13)	27412	14)	27416	15)	27452	16)	27456
17)	43012	18)	43016	19)	43052	20)	43056
21)	43412	22)	43416	23)	43452	24)	43456
25)	47012	26)	47016	27)	47052	28)	47056
29)	47412	30)	47416	31)	47452	32)	47456

You might be surprised if you thought that only two key cut patterns would operate the lock cylinder. After all, it may have been designed as a two level master key system with only a Top Master Key being issued and every other issued key being a specific change key that would not open any other lock cylinder than its own. On this list, one key bitting is the change key for the specific cylinder decoded, and one is the Top Master Key. The remaining 30 key bittings listed are for theoretical mid-level master keys. Some of these master keys could operate groups of lock cylinders operated by as few as only 4 different change keys (on the low end) to as many as 256 different change keys. At this point, we would have no way of telling which was which. Every combination is still a possible candidate for the TMK.

To identify the TMK, it could be necessary to cut all 32 keys listed. If you didn't disassemble any more lock cylinders, you could try each of the 32 keys in some other lock within the same master key system. Every key that didn't open the next lock cylinder would be either the specific change key for the cylinder decoded or a master key at a level lower than the Top Master Key. All the keys that opened the other cylinder would remain as possible candidates for the TMK, although only one of them could actually be it. You would have to approach another lock cylinder and again test all the keys that were not eliminated by the previous cylinder. By a process of elimination, you would ultimately get down to only one key that would not be locked out by any cylinder within the master key system. That key would be the TMK. As you can see, this method can be somewhat tedious and time consuming, but that is the price for not having any additional information. If you had only one cylinder that had its specific change key available for you, it would be a piece of cake.

In Like Flynn

It is amazing how one additional piece of information can make a somewhat complicated process, virtually effortless. I'm going to stick with the cylinder already decoded, but this time I'll pretend that I had the operating change key for the cylinder. Here is the cut pattern for the change key: 43052. Go back and look at the listing of the shallow and deep cut possibilities in each of the five chambers. Chamber by chamber we will compare the shallow and deep choices to the known values of the change key cuts. We see whether the change key cut is the shallow or deep cut listed for that chamber position. By a very simple process of elimination, the cut depth that doesn't belong to the change key, **must** be the TMK cut depth.

It is important that the key be the specific change key for the cylinder decoded. If it is just a key that works the cylinder, it could very well be some mid-level master key. In that case, we probably wouldn't be much further ahead than if we had no key at all. Presuming we have the change key, here is the process. The choices for the first chamber are 2 or 4. The change key cut is 4, so the TMK cut must be 2. In the second chamber, the choices are 3 or 7. The change key is 3, so the TMK cut has to be 7. For chamber #3, it is either 0 or 4. The change key cut of 0 dictates that the TMK cut is 4. The fourth chamber has a choice between 1 and 5. The change key is 5, making the TMK cut 1. For the final chamber, the possible cuts are either 2 or 6. The change key uses the 2 cut, so the last cut of the TMK must be 6. The Top Master Key has to be: 27416. If you look at the list of 32 possible cut combinations, you will find both the change key combination and the TMK. The remaining 30 are mid-level master keys.

It may be surprising to a lot of locksmiths, but the combination of a master keyed lock cylinder and its specific change key are all that is needed to unmask the identity of the TMK. Every lock cylinder in the system has the same potential for revealing the identity of the Top Master Key. Although nobody ever gave me a step by step process, as I have just done, I was clued into the basic concept by locksmiths from whom I learned master keying. I discovered another method of decoding the TMK without disassembly of the lock cylinder on my own, by deductive reasoning. For all I know, I may be the only one who knows this method. If I could figure it out on my own, it is possible that someone else followed the same trail of logic to the identical conclusion. Well either way, if I was the only one who knew it before I wrote this article, I'm definitely not the only one who knows it any more. You all appear to be in on the secret now.

Decoding the TMK Without Disassembly

They say that necessity is the mother of invention. To find the master key, I would typically use the process just mentioned. I would write down the change key cuts, decode the bottom and master pins, identify the shallow and deep cut possibilities and choosing the cut value that didn't belong to the change key. It's a very simple and straighforward way to find the identity of the master key. I had an interesting situation. Somebody brought me a group of Master brand padlocks that were master keyed.

Each padlock had its individual change key, but the master key that would open all the locks had been lost. These were not rekeyable padlocks, and I didn't really want to have to drill out the rivets and take everything apart. I set them aside since I didn't have any spare time to mess with the locks at that moment. It must have been more than a year later that I pulled them back out and had a brainstorm and figured a way to decipher the master key without disassembly. I will explain the essential process in relation to the lock cylinder I've been using as an example for this entire article.

Because this process doesn't require disassembly, we will start out only with the known value of the change key. That was already determined to be 43052. We already know the master key cuts too, but we will only use them to confirm the process. Otherwise, I'll act as if they are unknown. To start out, I don't necessarily know if every chamber has master pins, but the process should confirm that. I know in every chamber that has master pins that the change key cut will work and some other value currently unknown. I set up the process so that I could recut test keys repeatedly to minimize the actual numbers of key blanks wasted in the process. I will potenially have to waste one less key blank than the number of pin chambers in the lock. For a five pin lock, no more than four key blanks should be wasted. Here it goes.

I know for a fact that a key with the first four cuts being: 4305_ will allow the pins in those four chambers to split at the shear line. The next part will depend on the person who created the master key system. If he or she followed typical master keying conventions, the system will use two step increments. That means that an odd number for the change key (in that chamber position) would indicate an odd number for the master key. The same applies to even numbers. An even depth for the change key means an even depth for the master key. Since I will use all the change key cuts for the first four positions, the only chamber that won't be certain to have pins splitting at the shear line will be the fifth chamber.

This change key has 2 as its fifth cut. I would then start with the shallowest even number which is 0. My key would then be cut as follows: 43050. We already know that 0 is not the master key cut, but if we tried such a key in the cylinder, it wouldn't turn. Going deeper in increments of two, so we could reuse the same key over again, our next deeper even number would be 2. Since 2 is the change key cut, there would be no reason to try it, since we already know it works. We would take it deeper by 2 more to make the cut 4. Its not the right cut, and such a key would not open the lock. Taking it deeper again, the next even number would be 6. The cut combination would be: 43056. If you check back on the list of 32 key cut combinations that will open the lock, you'll find that bitting pattern on the list. The key would turn. That confirms the master key cut of 6, for the fifth chamber. There are still four chambers unknown.

We now know the master cut for the fifth chamber to be 6. The fourth chamber has a change key cut of 5. It is an odd number, so we will start at the shallowest possible odd depth, which is 1. The first three cuts would remain the same as the change key to be certain that they would split on the shear line.

The test key for the fourth chamber would have the cuts: 43016. If you look at the list of 32, you will find it there. The key would turn, and identify the master key cut in the fourth chamber as 1. The third chamber would be next. The 0 in the third cut position of the change key is an even number, but since it is the shallowest even number already, it is possible to reuse the key just used to decode the fourth chamber. It would be recut to 43216. If tried in the cylinder, it would not turn. Taking the third cut deeper by 2, makes the cut combination: 43416. That is one of the 32 possible working keys, and it would turn. The master key cut for the third position is confirmed as 4. Starting another key, we would use the three discovered master key cuts in the third, fourth and fifth positions. We would use the first cut from the change key, so we could be certain that four of five chambers split at the shear line. The change key cut in the second position is 3. It is an odd number, therefore we choose the most shallow odd cut possible, which is 1. The key cuts would be: 41416. It is not a usable combination for this cylinder, so we would have to re-cut the key again. Two increments deeper would make it 3, which is the change key depth, so we would skip past that and take it further by 2. That would make the second cut a 5. The new cut combination would be: 45416. That wouldn't work either, so it would be cut 2 deeper to make the combination: 47416. That is on the list, and it would turn. We have determined the second cut of the master key as 7. Now only one cut is missing from the identity of the Top Master Key.

The final step is to make a key with the four known master key cuts. Only the first cut is yet undetermined. The change key cut is a 4. That means the first cut for the master key will also be an even number. The shallowest possible even depth is a 0. The final key would be cut as follows: 07416. When tested it would not turn. The last four cuts bring the pin splits in those chambers to the shear line, but the first one still does not. The key would be cut 2 deeper in the first position, making the key combination: 27416. If you go back to the list of 32 usable combinations, you will find that bitting there. Also if you look at our earlier determination, you'll see that 27416 is the TMK. That key would turn and reveal the last cut of the master key.

Mission accomplished. The actual time involved will depend on how fast you can cut and re-cut the keys. It is surprisingly simple. I'm not sure what inspired me to figure the process out, but it is rather effective, even on locks that can be disassembled. If you suspect or know that you are dealing with a master key system with single step increments, you would have to progress one depth at a time and you wouldn't have "odd only" or "even only" chambers.

What Does it Mean?

Besides phantom master keys and reduced pick resistance, split pin master key systems have other vulnerabilities. You know now that the identity of the Top Master Key (in the master key systems you designed) is very vulnerable. With just a modicum of simple math, a change key and cylinder will reveal your TMK to anyone who chooses to look. Does that mean that you should never set up another master key system? Not necessarily. But you shouldn't create a master key system without knowing the vulnerabilities. It may give you enough ammunition to convince your customer to go with a truly restricted key system. Although having a restricted key won't prevent someone from determining the master key identity, if they can't get the proper key blanks, they can't create the key. The other less vulnerable option is an electronic lock where only the programmed codes will open the lock. Incidental or accidental master keys will not typically exist the way it is found in mechanical locks. Ignorance could be costly.