Safe cracking for everyone!

Always wanted to learn safe cracking? No?
Well, this book is still for you!

By: 狄昭瑞

Introduction

At this point at which I am writing this, I am definitely still a beginner. I've manipulated my fair share of group 2 safe lock's but I have not yet tried as many as I wanted to. Some, such as the LaGard 3330, can give more trouble than the S&G 6700 series, which are simple and used as beginner locks and sadly, also the most common type of mechanical safe locks. If you are a beginner or don't even know anything whatsoever about this topic and you just want to learn this because it's cool or to impress a girl ;), then this book is definitely you. I know there are a couple other books/tutorials on this out there but I wanted to create my own. No matter how thorough the book, there will always be some missing piece of information and I'm hoping this fills in the gaps for others out there (and my girlfriend is also interested so this is dedicated to her <3). And I hope this will be able to address some of those questions and that this and all the different resources put together will be complete enough to get cracking! (Pun intended). If you have any information not in this; feel free to contact me! I have an account on keypicking.com under the username of Daggers; just shoot me a message and I'll get back to you!

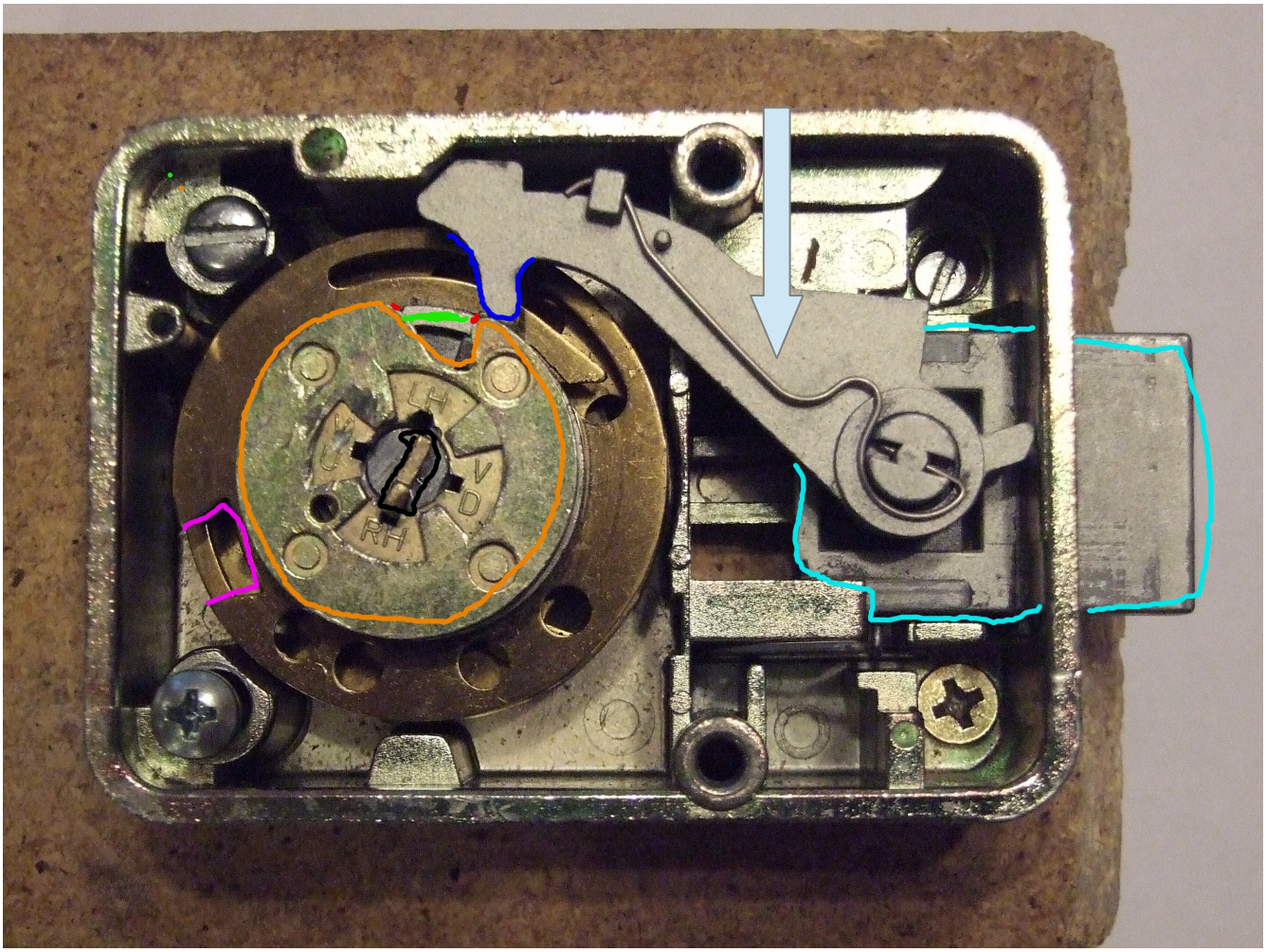
Group 2 mechanical combination locks are locks that are *supposed* to resist manipulation for 2 hours. That's the official rating. Yeah, right. Group 2M are slightly more manipulation resistant and feature things that make taking contact readings harder, false gates, etc. Group 1 is, again, *supposed* to resist manipulation for 20 hours. It's way better than group 2 and 2M but still not perfect. They feature things such as an extra step that needs to be done after you enter the combination to engage all the parts to open it. And then there is the group 1R. Same thing as group 1 but has several more features that make it impervious to x-ray and ultrasound attacks. These locks can not be x-rayed to see the combination unlike the other groups. Group 1R features things like wheels made out of delrin (low density plastic that don't show up well on x-ray), spacers in between wheels with false gates, and other precautions that confuse the x-ray image.

Before you begin, you must have a thorough understanding of how a safe lock works, how the wheels interact with each other, and be able to visualize the wheel pack and know the state it is in at all times. I would suggest first to read www.crypto.com/papers/safelocks.pdf by Matt Blaze. Very good intro to how safe locks work and safe cracking. You won't understand everything at first, but that's ok. That's just to get a basic idea of stuff. When I first started, I spent hours pouring over just that info; don't do that. Use as much of a variety of sources as you can! I would also recommend you to spend the couple extra bucks to get a cutaway safe lock to view how it works as you manipulate. You don't need a cutaway safe lock but you do need a safe lock! I recommend starting with an s&g 6741. If it just says s&g 6700 then it's most likely a 6741. A 6730 is the same thing but requires more preciseness when dialing in the combination and so is slightly harder for a beginner, but is still just as good. Do NOT start with a LaGard 3330! It's in the same group of locks, but has some features that I will cover later which makes it harder to start with.

Oh, and read the interview with Mark Bates at http://www.safeventures.com/news.php?id=16 and make sure you understand the different ways a lock can indicate a which numbers are in the combination. And this guy Oldfast has an AMAZING chronicle of his experiences with manipulation at http://keypicking.com/viewtopic.php?f=100&t=7432 He explains the terms used very nicely as well and I will be using those terms so it's best to get acquainted with those first.

Ch. 1: How safe locks work (or in other words, fail)

Ok, I have really bad photoshop skills so you'll just have to bear with me here. This is what the back of a typical safe lock looks like with the back cover removed:



This is a LaGard 3330. I highly recomment you have an s&g 6741/6730. It will for the most part, look the same. Ilco, Rench, Diebold, Mosler, these work too as long as you have a group 2 from them.

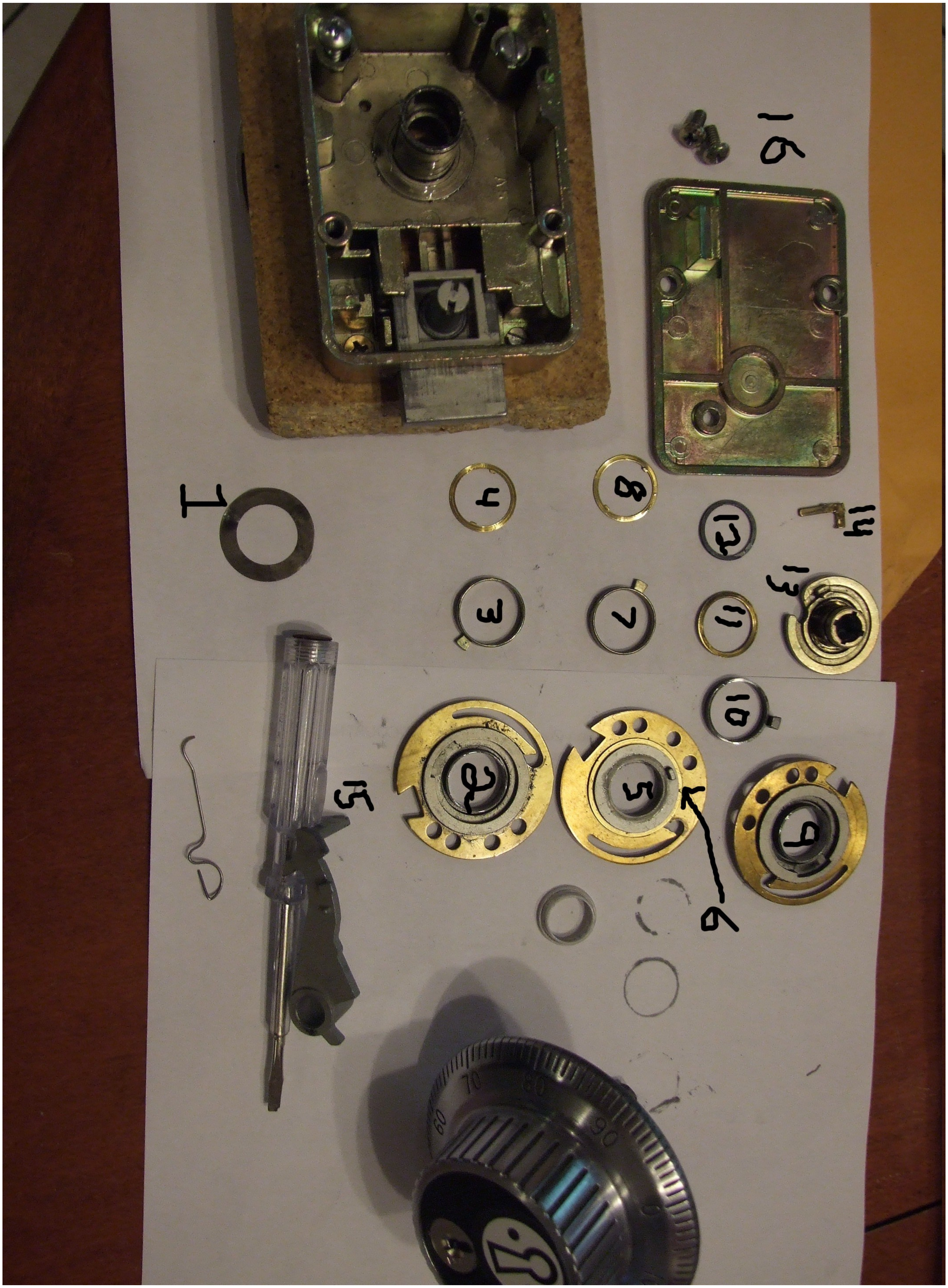
The part outlined in blue is called the nose. It rides along the drive cam which is circled in orange. There is a metal wire, at the end of the arrow, that you can see pushing the nose down onto the drive cam. This means it is a spring loaded fence type of lock. The thing the spring is on is called the lever or arm. Because the nose is being pushed down onto the drive cam when the gap is under the nose that means it'll drop into the gap ever so slightly. That's where the two little red dots come into play. They are called the contact points. The nose hits those points every time it is coming out of the contact area which is the space between the two contact points as indicated by the green line. The part in the very middle of the drive can is called the **spline key**. It's outlined in black because it's such an easy

color to see amid other dark colors..... nah, I just ran out of colors :P The shaft of the dial screws into the drive cam (you can see the silver shaft behind the **spline key)**. It has a little notch for the spline key to fit into so that it will stay in place and not unscrew out.

Are you still following along? Okay good! Now, the brass circle behind the drive cam is one of the 3 wheels in the lock. The purple part cutout in the wheel is called a gate. These terms are very important for later so make sure you remember all these. Oh, and the part circled in teal is called the bolt. It locks the handle of the safe the lock is on. The lock doesn't actually lock the safe, it locks the handle which is turned to retract all the bolts along the door of the safe and allow it to be opened.

Your lock might have this little brass arm thingy at the bottom below the bolt. Don't worry about that yet, I'll get to it. We will be learning more about what they all do later but for now, remember these parts and what they look like! Seriously, remember all these terms and commit it to your mind. Know them like you know apples are apples and bananas are bananas.

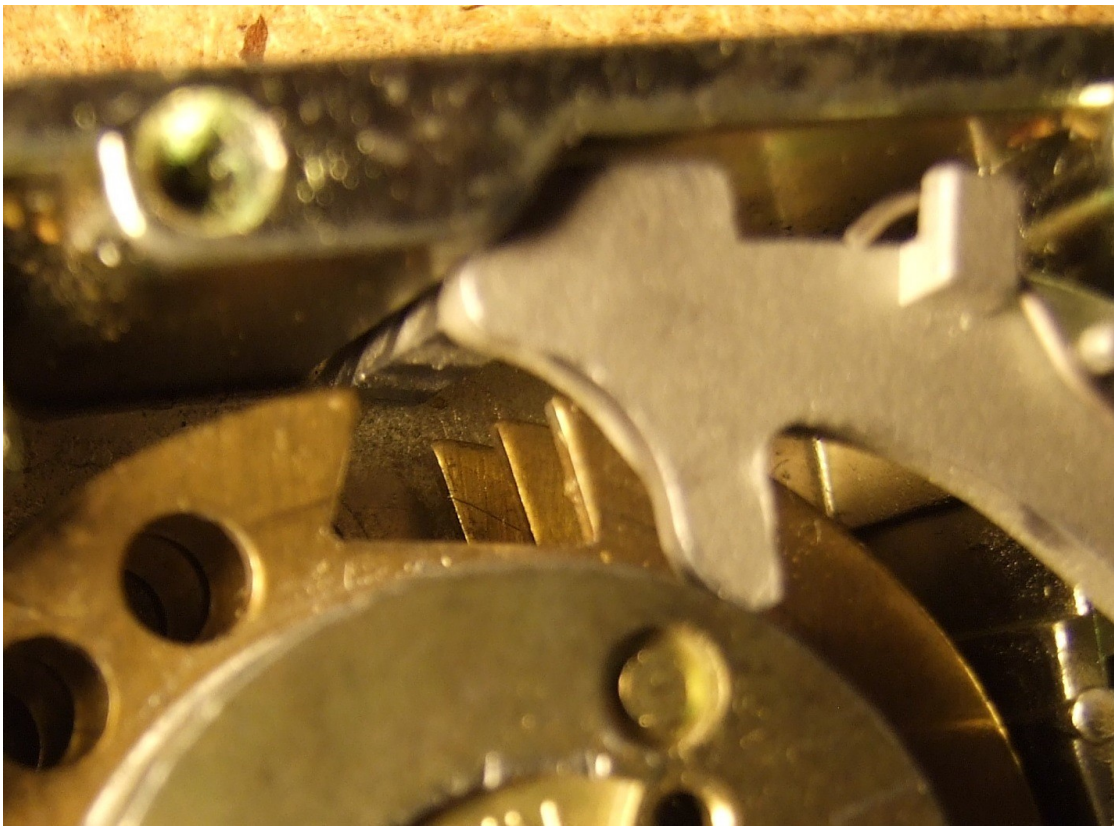
I'm going to take it all apart now and show how all the different components fit together to make this lock function! Study it carefully!



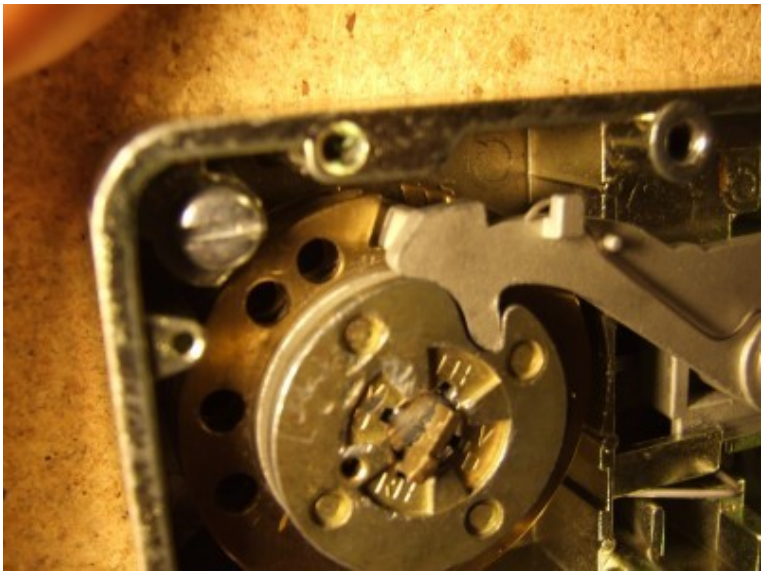
So I numbered them. #1 is a tension washer. It's slightly wavy so it acts like a spring and keeps all the wheels (#'s 2, 5, & 9) lightly pressed against each other so nothing wobbles and it all fits snugly together. #2 is wheel number 1. You can see the gate in the wheel. The position of the gate is what determines the combination. Wheel number 1 goes on first when being reassembled and will the be wheel closest to the dial. Wheel 3 is the wheel CLOSEST to the drive cam! This will be explained shortly. #3 is called a fly. Specifically, a movable fly. It fits directly on top of the first wheel as pictured and the fly has a slot on wheel 1 it fits into. #4 is a spacer. It spaces the wheels out from one another so they don't rub on each other. #5 is the second wheel. I have it laying upside down in the picture and for a purpose. #6 is pointing to a stub sticking out from the bottom of the second wheel called the drive pin. It fits into a groove on the top of wheel 1 and when spun, hit the fly that is laying on top of wheel one. This causes wheel one to turn with wheel two. Wheel 1 has no drive pin since there is no wheel under it that it needs to spin. #7 does the same thing as #3 and goes on the top of wheel 2 (the other side of wheel two than what's shown in the picture). #8 is the same thing as #4. #9 is the 3rd wheel. It is the same in appearance as wheel number 2 including a drive pin (since it has to move wheel 2) except that it has a larger fly (#10). The reason it's bigger will be explained later. #11 is another spacer but thicker than #'s 4 and 8. #12 is a retainer. After all the other parts are on the shaft, it snaps on to lock them into place. #13 is the drive cam with an upside down view. It goes on after the retainer. What holds it on is the spindle (the shaft of the dial) which screws into it as explained earlier. #14 is the spline key and it holds the spindle to the drive cam. #15 is a metal bar above and behind the nose and is called the fence. When the nose is in the contact area on the drive cam, the fence lowers onto the wheels. Refer to the next picture to kinda visualize how that works. If the drive cam isn't holding up the nose, then the fence falls down onto the top of all the wheels. And I forgot to mark it but that plastic ring between and to the right of the 2nd and 3rd wheel is to keep the dial running smoothly and so there's no metal on metal interaction. It goes on the spindle.

So this is a pretty good picture on how the fence rests on the wheels:

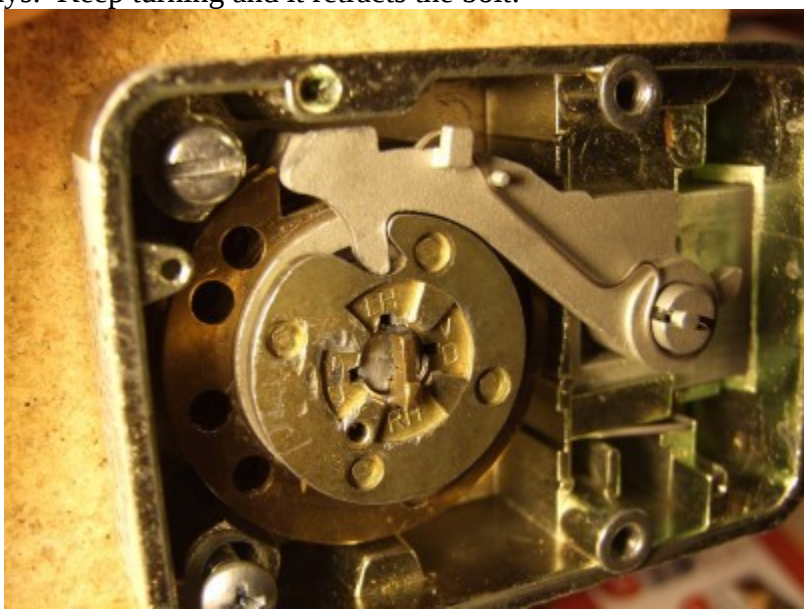
When the nose is on the drive cam, the fence is higher. Other wise, you would be able to feel the gates as you turn the dial and they scrape underneath the fence. Here's a picture:



Notice how high the fence is now? In this picture, the combination has been entered and all the gates are aligned. But even if they weren't, the fence still wouldn't be touching them because the nose is resting on the drive cam. Now, when we turn the dial to the contact area/drop in area in this next picture:



The whole lever arm falls in! Low enough that the metal protrusion at the top doesn't block it from moving sideways. Keep turning and it retracts the bolt:



The lever arm moves under the metal protrusion from the top of the lock body. Now, You see the little metal spring below the bolt? It's called a re-locker. It has a little arm going under the bolt and the bolt has a cut in it for the arm. The arm goes up into the bolt so the bolt can't retract into the lock. The back cover pushes the arm down so the bolt is free to move. This is because instead of manipulation, some people drill the lock and punch off the back cover to see the combination. With the cover off, the bolt is blocked by the re-locker. S&G's have a little brass arm that goes down into a hole in the bolt instead of up from the bottom. The back cover pushes down one end of the arm and that raises the other end to allow free movement of the bolt.

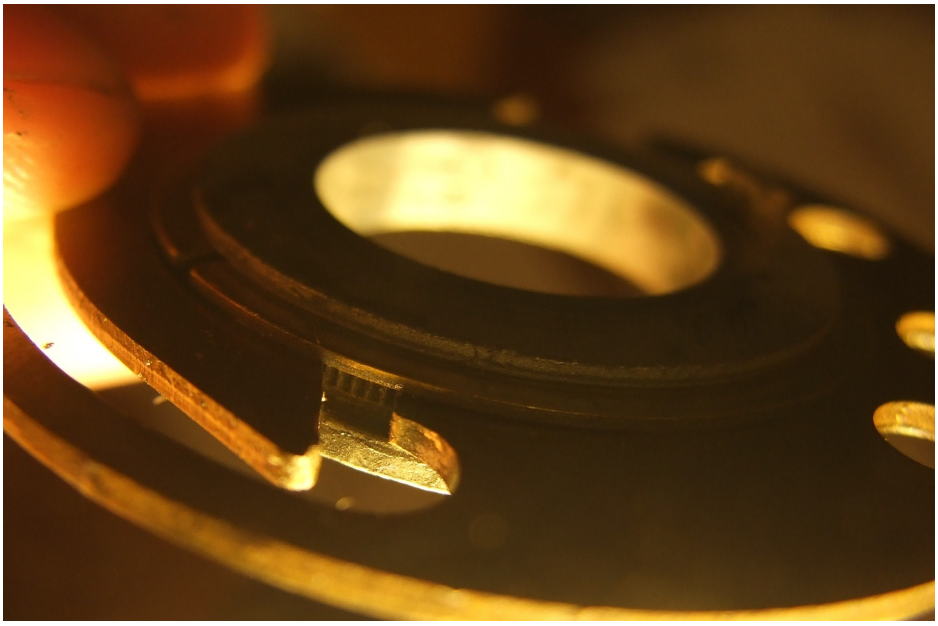
Basically the most important paragraph here!!!

Ok, now it's time for you to learn how the wheels move. The dial is directly connected to the drive cam so amount that the dial moves, the same movement is done by the drive cam. If you spin the dial at least one whole rotation to the right, it will take one full left rotation of the drive cam (and dial) to start the 3rd wheel moving left. Keep going and it will take another full rotation left to move the second wheel and again for the 1st. The reason the first wheel to get picked up is called the 3rd is because it's the 3rd # in the combination. Think about it; spinning the dial 4 times left sets the first wheel and 1st # in the combo. Now, you reverse direction 2 whole rotations to the right to pick up the 2nd wheel and then keep going until you get to the second number in the combination. Reverse direction again to the left one rotation to pick up the 3rd wheel and then stop at the 3rd number. You can't set the 3rd wheel first because then, how are you going to set the 1st and 2nd wheel without messing up the 3rd? Combinations are usually dialed by spinning the dial left 4 times to 1st #, right 3 times to 2nd #, left 2 times to 3rd #, then you spin the dial to the right to the drop in area and retract the bolt. When I say left 4 times to the 1st #, that's saying pass the 1st # 3 times and stop on the fourth. When I say right 3 times, pass the 2nd # 2 times and stop on the 3rd. Because of how they work, it takes 2 rotation (two passes of the second number) to pick up the second wheel. To PICK it up, not set it on where it's supposed to be. Then you have to move the dial to the 2nd number for the third time and leave it there. That's why you stop the 3rd time.

Basically the most important paragraph here!!!

How combination changing works

In the next photo you can see there are small serrations in the wheel. The brass bit from the wheel locks into those. You can see a circular-ish shape hole by this. When the combo is change, all these holes line up and a special metal rod called a change key slips into there. On the back of the lock casing there is a hole in the bottom left for this. The change key is turned and the brass arm going into the serrations is lifted off and then a new combo is dialed. The brass (which includes the gate of the wheel) is in a different relative spot to the silver center of the wheel (which has the drive pin and fly) and the combo is now different. Not all wheels will look like this but if they use a change key, they will work on the same principle, the change key moves the arm off the wheel, and then back on to the new combo.



Ch. 2: Exploiting these failure points

You made it through learning how these locks work! Or maybe you didn't..... just go back and re-read, you'll get it soon enough. No one gets it on their first go anyways! You're probably wondering what failure points did I go over? Well, learning how something works is the same thing as learning all the ways that it can be defeated. You just have to recognize what it is and that's why you're still reading! Locks to practice on: In this I will be using the example of an s&g 6741. I recommend either the 6741 or 6730. The only difference is the 6741 has a dialing tolerance of +/- 1.25 and 6730 has +/- . 5. This means with the 6741 if a number in the combination is 10, you can dial 8.75 or 11.25 and with the 6730 only 9.5 or 10.5 and the lock will still open.

Why and how it's possible

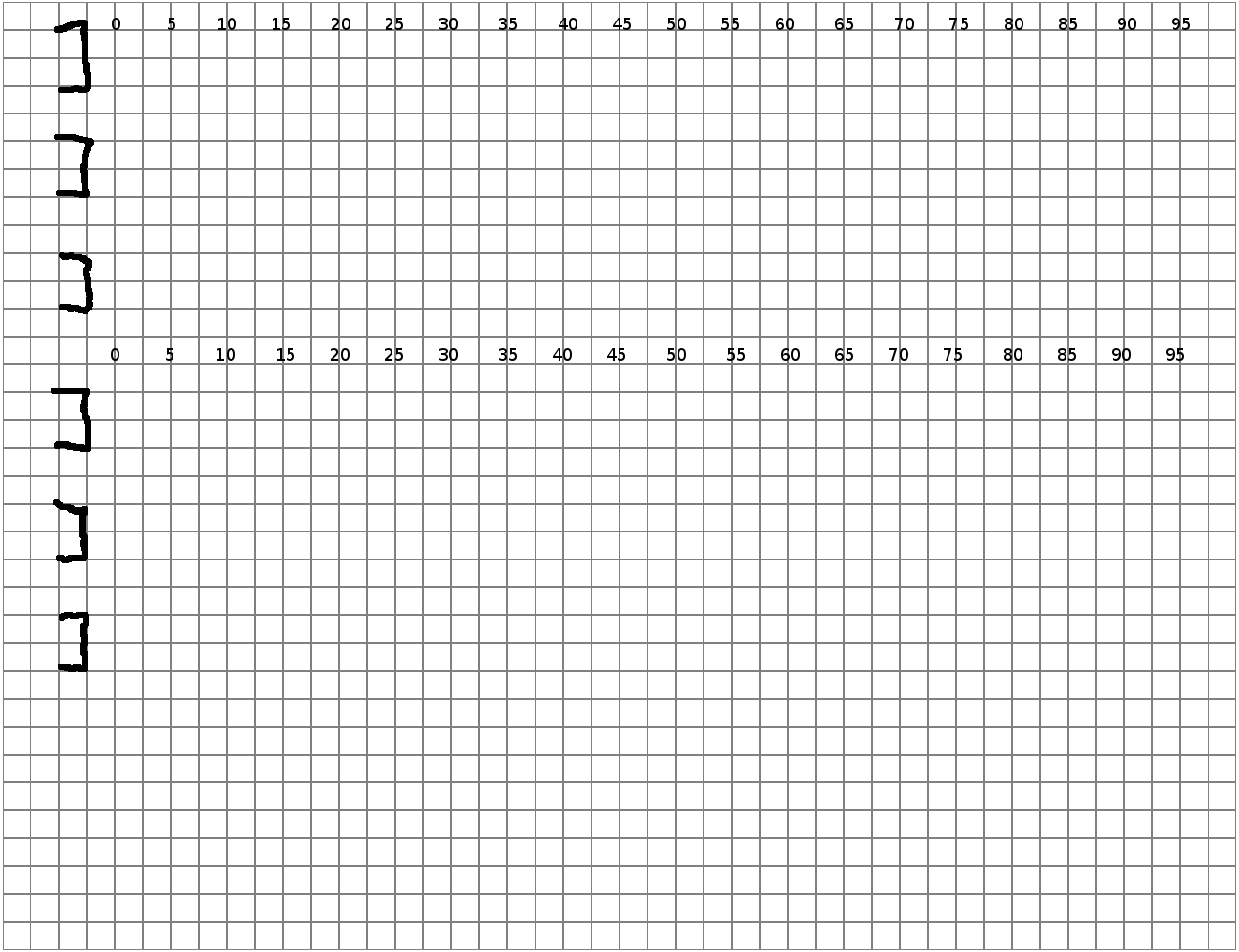
These locks seem pretty secure right? The only thing you can use to move or do anything with is the dial. It's not like a key lock where you can stick some lockpicks in and pop it open, what you see is what you get! Safe cracking works through the measurement of where the contact points are located. On my lock, it's 96 for the left contact point and 6 for the right. You can feel these points on your lock. They will always be in the same general area. They will move, but only to a maximum of an increment and a half or so.

Now, remember how when the contact area is under the nose the fence rests on the wheel pack? This is the key. Look at the drop in area on the drive cam; it's sloped. The further down the nose is, the less wiggle room there is for it until it's all the way in there and fits snugly. The contact point on the sloped side is the right contact point and the other side is the left one. Imagine it as if you are staring at the front of the lock (not the back) and you can see through it to the contact points. Left and right. You have to turn the dial left to touch the right contact point. If you turn it right, the nose drops down but you can't feel exactly where the contact point is. So you feel the right contact point only by hitting it from the left side of it. Opposite for the left contact point. And when I say hit, I mean to just lightly feel it. If you put too much force, the nose will ride up on it and go past.

Now you know how to find the contact points! Next thing to do is to know what this information can do for you. When the nose is deeper in the drop in area, there's less side to side play. This means the contact points will be closer together. But how does the nose go deeper in without all the gates being lined up?? Look at this next picture very closely; you've seen it before:

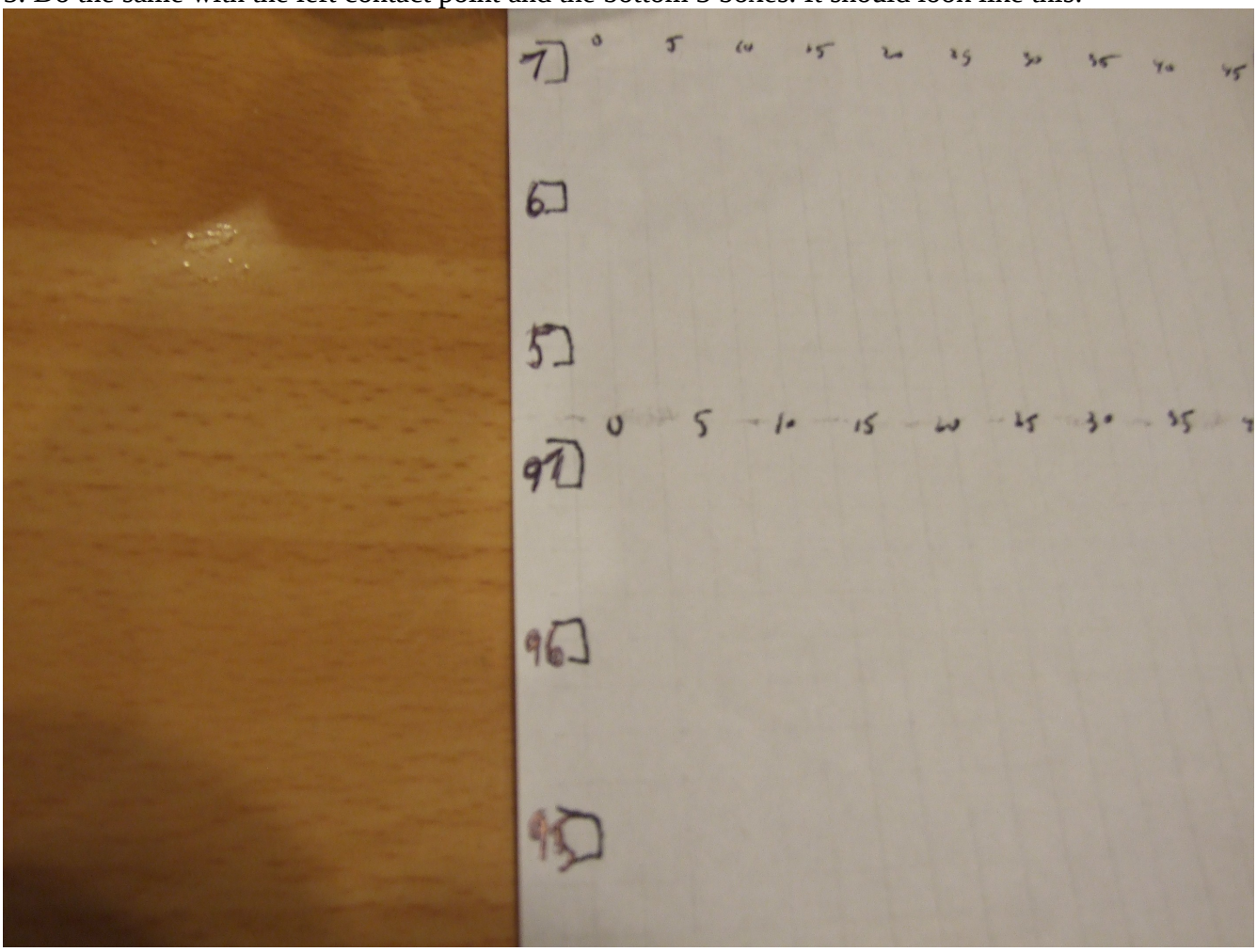
If you look at where the fence is on the wheels, you can just barely make out that it's only touching ONE wheel. The second one. The third one is slightly below and the first one is even more so lower than the 3rd. Now, imagine if the gate on wheel two was there under the fence. The fence would drop ever so slightly onto the next largest wheel, the 3rd one and the nose would drop further into the drop in area. That means there's less wiggle room. The contact points will be closer together by about a quarter of an increment. That's not a lot, but that's what we measure when we do manipulation. We pick up all the wheels, generally with a left rotation, and put them at 0. Then we spin the dial with right rotation to the contact area and measure the contact points while making sure not to pass 0 or else the wheel positions will be disturbed. We then turn left until we reach 0 again put all the wheels at 2.5 and measure the contact points again. Wash, rinse, and repeat at 5, 7.5, 10, and so on until you get to 97.5. That's 40 positions around the dial. We go 2.5 increments because these locks don't open on just that one combination, there is some error so 2.5 increments is sufficient. So basically since one wheel is bigger than the rest, we are graphing just the biggest wheel, not all of them. This flaw is unavoidable. The imperfections of machines make this happen. The third wheel usually is the wheel that the fence rests on. This is not just because of wheel size, but because the spring pushing the lever down is only pushing on the lever, on the side closest to the thirds wheel. It unbalances it and the side of the fence where the nose is, is pushed down further than the back of it. ONTO THE GRAPHING!

Here's a graph paper you can use, copy it, print out as many as you want, do whatever :)


0 5 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80 85 90 95
0 5 10 15 20 25 30 35 40 45 50 55 60 65 70 75 80 85 90 95

Graph 1

So the first thing to do is to label your graph. Write Graph #1 AWL and then your lock model at the top. AWL means all wheels left. That's how we're going to be starting. This is important so that you can come back and know where you left off. Safe cracking doesn't have to be all at once, you can stop any time and come back later. In the 2nd to the top boxes on the left side of the paper you put the right contact point. You want the closest whole number. Let's say you have a contact point of 6 ¼ or 5 ¾, then put 6. If it's 6 ½ you can put 6 or 7, doesn't matter. Then in the box above it, put 7. The box below, 5. Do the same with the left contact point and the bottom 3 boxes. It should look like this:



Now, pick up all the wheels with left rotation (spin left at least 3 or 4 times.You can feel the wheels being picked up) and park all wheels on 0. That means stop on 0, or put all the wheels there. Parking is the same thing as leaving a wheel on that number. When you dial a combination to open a safe lock, you are parking the 1st wheel on the 1st # and the 2nd wheel on the 2nd #.

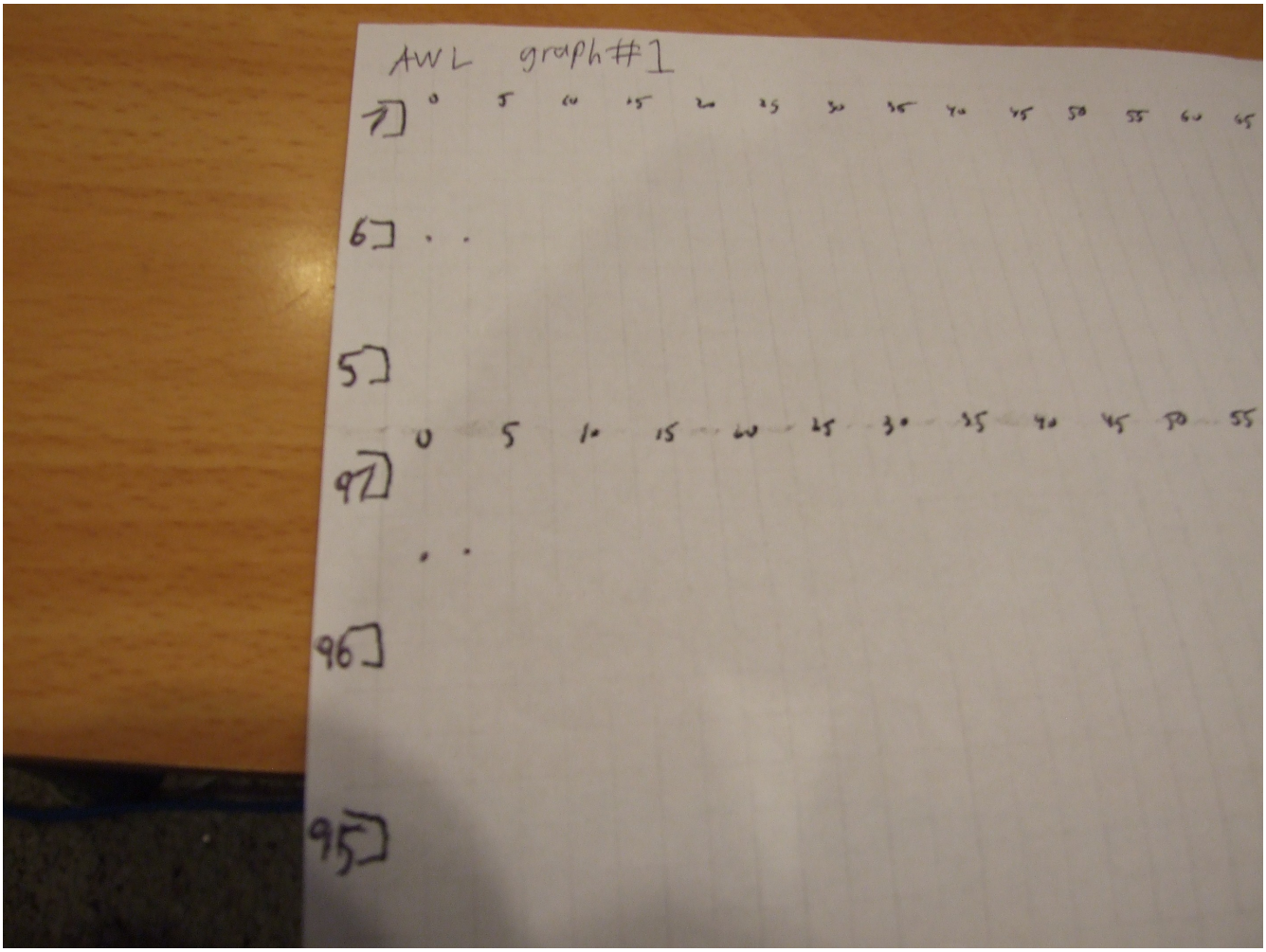
The way you graph the number where the contact point is, is simple. The way the graph is divided, the horizontal lines stand for ¼ of an increment. You want to be able to consistantly read the dial and see if it's on 6 ¼, 6 3/8, 6 ½, 6 5/8, etc. Going by 8th's is the best. An eighth is in between each horizontal

line. So if the right contact point reads 6 ¼ for all wheels on 0, you would go down from 0 (on top of the paper) to one line above the 6. Put a dot there. Same procedure for the left contact point.

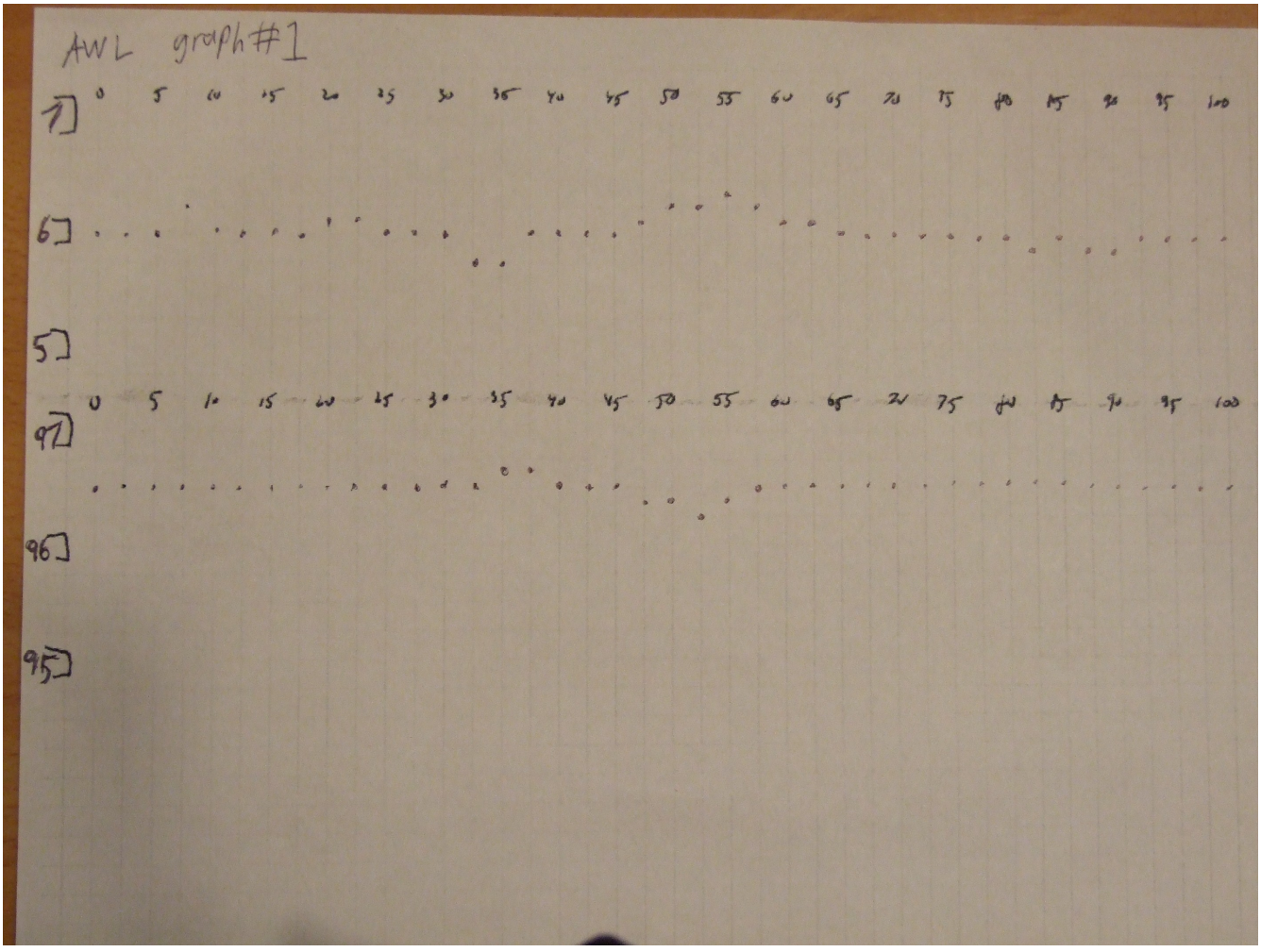
Remember when I said that the contact points have to be felt from the inside out? If 0 is in between the two contact points for you, turn right to feel the left contact point (this is for all wheels left. Because if you have all wheels right, turning right even more would mess them up). Lightly move the dial until you encounter resistance. You should be moving the dial with enough force to move it, but light enough that the contact point stops the dial and your hand keeps moving on the surface of the dial but doesn't move the dial itself. It takes practice. Being able to take accurate contact readings is KEY TO EVERYTING! Graph the number it stopped on. To read the right contact point, spin right rotation to the other side of 0 (because going the short way and spinning left will mess up the wheels on 0) and go slightly past the right contact point. Lightly turn left and read the right point. Then graph it.

If 0 is to the left of both contact points, just spin right and read both contact points that way, making sure not to pass 0 and mess up the wheel positions. If 0 is to the right of both contact points, spin left and do the same thing.

After you've graphed the two contact points for 0, spin the dial left and pick up all the wheels again at 0. Turn to 2.5 and repeat the same procedure. It should look something like this:



This has two points on 6 and two points on 96.5. You want to repeat this process all the way around at every 2.5 increments. If you have a contact point on 5 ¼ or somewhere close to a number you're testing, you have to be careful not to disturb it when you take contact reading. Let's say you have 5 ¼ and 14 ¾ and your contact points. AWL to 5, right rotation just BARELY pass 5 ¼, try not to go completely to 5. It's not too bad if you do though, just don't go past it! Spinning right, the wheels will pick up not quite where you left them with left rotation. The wheels will pick up a bit under 5 so you have some extra room to move between where the wheels are and the contact point. Now, lightly feel the right contact point. You can spin the dial back and re-feel as many times as you want, just be careful not to disturb the wheels at 5. You can feel where the wheels are and where they pick up so you can get a sense of how far you can go before you disturb them. Now, when you test 15, put all wheels left rotation to 15 and turn the dial a couple increments right, past 14 ¾. When taking the contact point reading here, just make sure to do so lightly and not have the nose ride up on the drive cam. Turn too far and the wheels at 15 will be messed up. So graph the whole wheel pack and you'll get something like:



This!

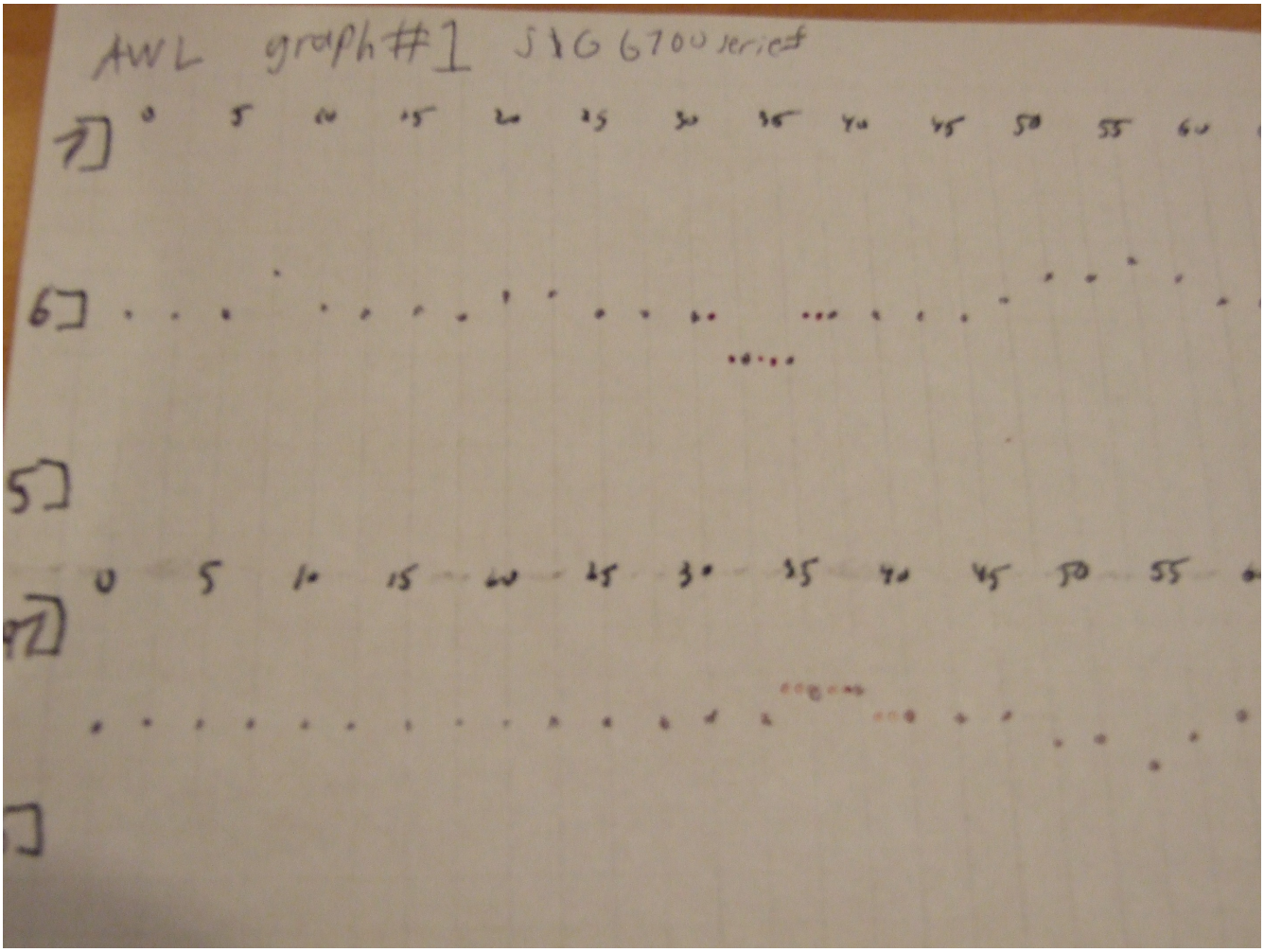
This graph is how you find the gates. So you'd understand how it's kind of important. Taking the correct contact point readings means an accurate graph! So make sure when you take contact point readings, it always consistant! It's best to use a light touch and make sure that the point you take is right where the nose touches the drive cam. But if you use the SAME EXACT amount of force each time (even if the nose does ride up on the drive cam a little) then you should still be fine. Not everyone will have the exact same points because everyone feels with differing amounts of force, but relatively,

the graphs should show the same thing.

Ok, so now it's time to see if you've done your homework! At the very beginning, in the introduction (gasp! That stuff is useful??? Who reads that?!?!) I gave you a site that describes how a gate will indicate it's position on the graph. When the fence is resting on the wheel pack and the gate of the largest wheel is under it, it will be lower right? Yup. And then when it's moved off, it will be higher right? Yup again! Now think hard and you'll remember the right side of the drop in area is sloped. This will give a greater change in contact point that the other side. The left contact point reading will be less dramatic but will help confirm a gate on that number.

So it dips down for a couple numbers and then back up (with the right contact point. With the left, it'll go up and then back down. Think about it, when the two contact points get closer, the left one increases in number). Where in this graph do you see a dip in the contact point and a corroboratory rise in the left contact point? Si! It drops at around 35 for the RCP (right contact point) and up at 37.5 for the LCP. It can sometimes be in the same spot but it can also be a little off like it is here.

Now you want to do something called amplification. Remember how we went every 2.5 increments? Go every 1 increment from 31-39 and graph that in a different color.
You'll get something like this:



This is to find the center of the gate. Going every 2.5 increments isn't precise but it lets us find the gate. Now we need to know the exact number it's on. So for the RCP's it's 32-35. Find the middle of that. It's 33.5. Now do the same for the LCP's. It's 35.25. Then find the middle of these two numbers; it's 34.375. Congratulations!!! That's one of the numbers! You don't really have to dial in 34.375, you can dial 34.5 or 34 ¼. Never go off by more than ¼ increment! Now to find out which number in the combination it is :P Is this seeming like a long process yet? It should, but with practice you can get your time to 5-10min for an s&g 6700 series.

High low testing

The way you can determine which wheel the number belongs to is something called high low testing. Recall that the nose drops lower when the gate is under the fence. The contact area will be narrower. Now, when the wrong number is entered, the contact area will be wider. So we want to put the number we found on two of the wheels and throw the other wheel off. And do this with each wheel. So that in two of the tests, the gate will be under the fence and in the other it won't. So in one of those tests, we should have a contact area that I significantly wider since the gate will not be under the fence for one of the tests. We start with the first wheel being thrown off by 10 increments under. This is a low test. It doesn't have to be 10, it should be at least 10 though. This is just so it has more isolation.
For example: We find 34.375 (we'll make it easy and say 34.5)

Low testing:
R24.5 L34.5 L34.5 (This is right 4 times to 24.5 and left 3 times (this picks up wheels 1&2) to 34.5)
L34.5 R24.5 L34.5 (This is putting only 2nd wheel on 24.5)
L34.5 L34.5 R24.5 (This is left 4 times to 34.5 and right 2 times (this picks up only 1 wheel) to 24.5)

Each of these times you want to measure both contact points and write them down. Then find the space in between them. That's the size of the contact area. Now, this is where a thorough understanding of how safes work come into play. So let's say these 3 test show this:

LCP 97 RCP 6 Contact area 9
LCP 97 RCP 6 1/4 Contact area 9 1/8
LCP 96 3/4 RCP 6 1/4 Contact area 9 2/4

The most likely wheel to have 34.5 as a the combination is wheel 3. But we need to do High testing as well (it's not required if the indications from low testing is good enough. It just helps support it):

High test:
R44.5 L34.5 L34.5 (This is right 4 times to 44.5 and left 3 times (this picks up 2 wheels) to 34.5)
L34.5 R44.5 L34.5 (This is putting only 2nd wheel on 44.5)
L34.5 L34.5 R44.5 (This is left 4 times to 34.5 and right 2 times (this picks up only 1 wheel) to 44.5)

and say we get:

LCP 97 RCP 6 Contact area 9
LCP 97 RCP 6 Contact area 9
LCP 96 7/8 RCP 6 1/8 Contact area 9 1/4

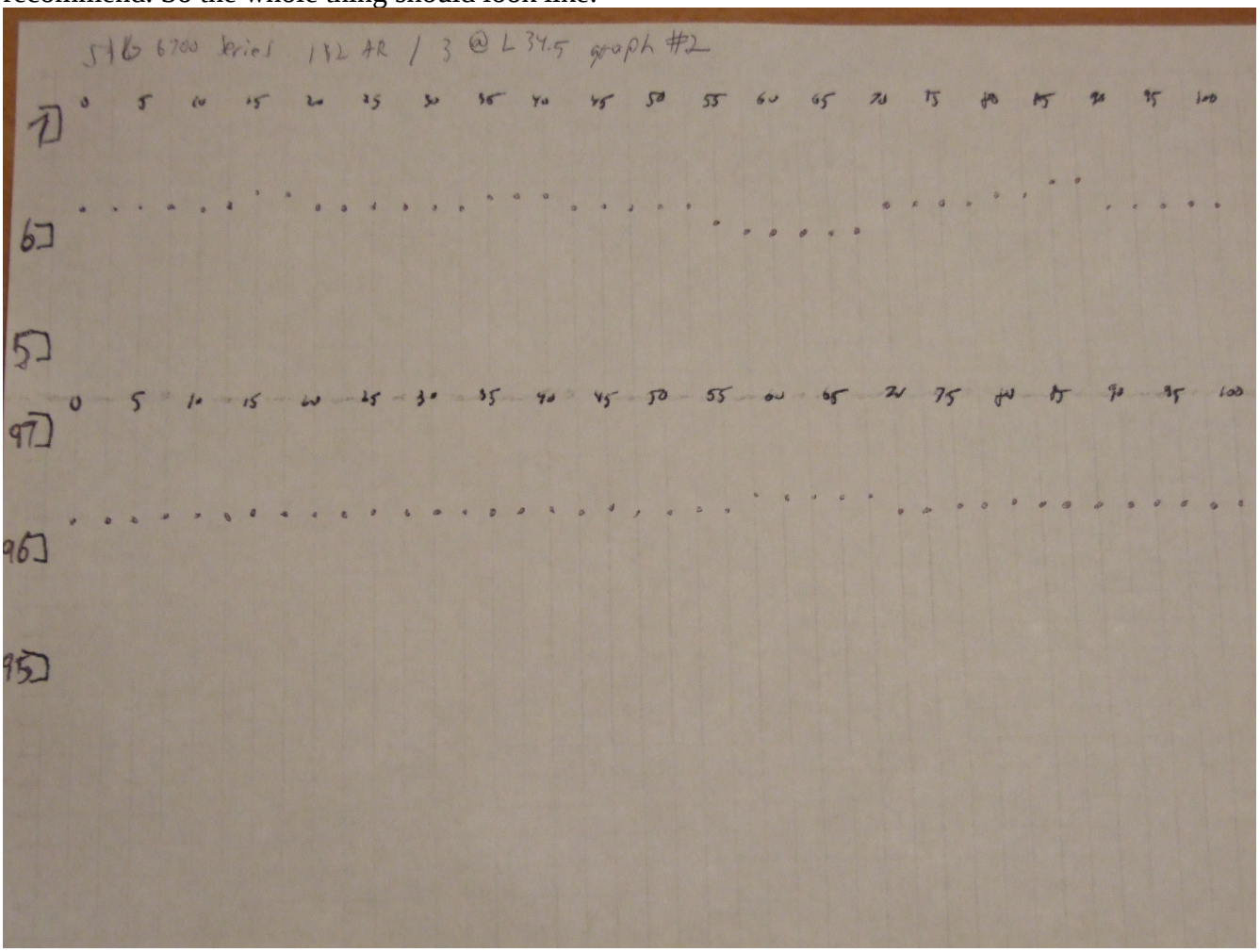
Now both test show wheel 3 to indicate. So we know so far the combination is ?-?-34.5. This is why an understanding of how wheel pick up is needed. You need to know how to put each wheel at a specific number and know which wheel is at what number. IT IS CRUCIAL!!!

VERY IMPORTANT NOTE
Notice how we found 34.5 with AWL rotation. In all the high low tests every time we put a wheel on 34.5 is is with LEFT rotation. This is important. Parking with right rotation will put the wheel slightly off. The width of the fly and drive pin on each wheel makes it so that when you approach each wheel from the opposite direction, it will pick up in a slightly different spot than how you left it. Compensating for this will be covered later.

Graph #2

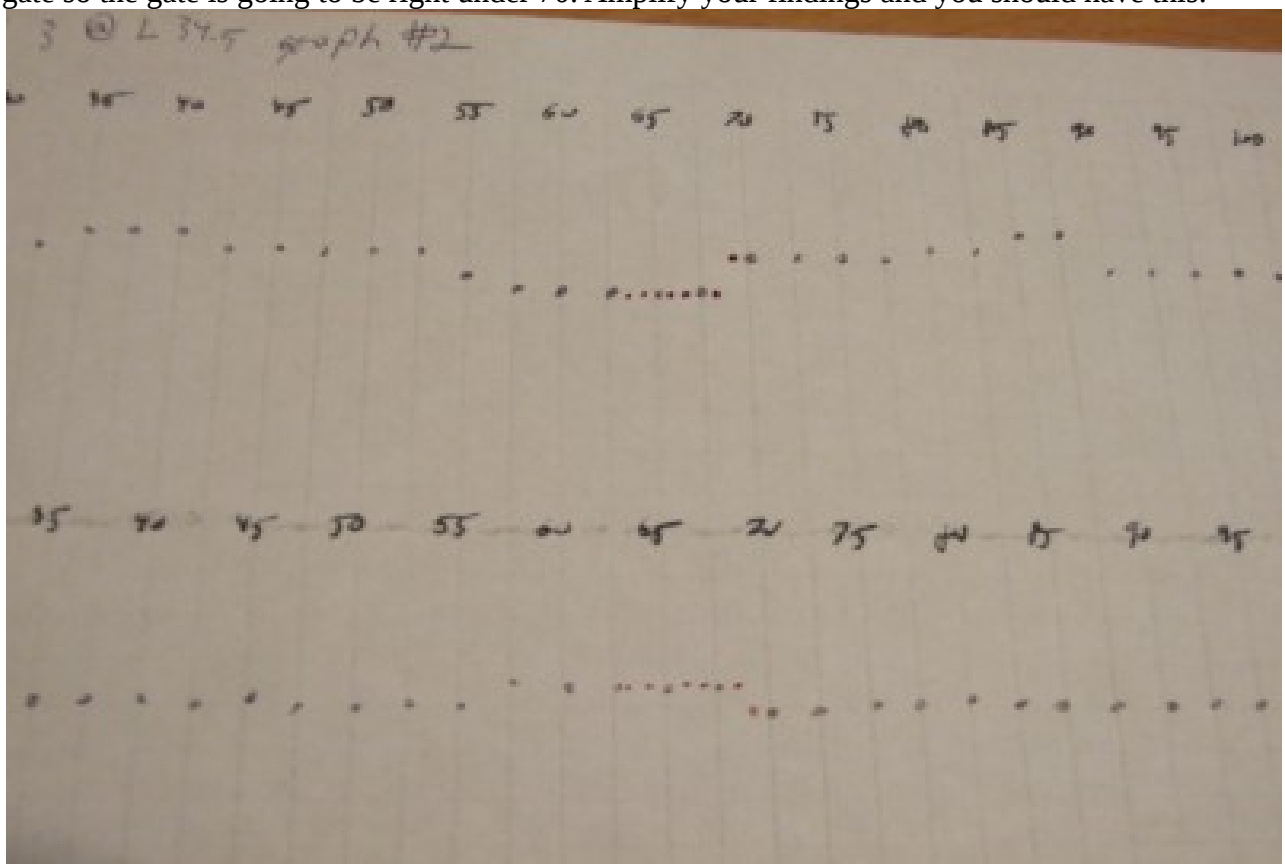
So start graph number two like you did number one with all the titles and all. But since you have wheel 3 going left you will have the other two wheels going right. It would be titled with LOCK TYPE Graph #2 1&2 AR / 3 @ L34.5. This means you are graphing wheels 1&2 with right rotation and wheel 3 is parked at 34.5 with left rotation when you take contact readings. AR means around right.

To graph this you pick up all wheels with right rotation and stop at 0. Then you turn left and pick up wheel 3 from 0 and stop at 34.5. Then you graph your contact points. Next turn right and pick up the wheel from 34.5 and the other 2 wheels at 0 and turn to 97.5. The 1st and second wheel will pick up at the same time so no need to to an extra rotation. You'll get better at is as you go. Then repeat the whole process, turning left to pick up wheel 3, park it at 34.5 and read contact points. Just be careful when you pass by 34.5 and you try to read 32.5. You're going to mess up the wheels so you'll have to reset the first wheel. You can just start at 32.5 instead of 0 to avoid this problem. That is what I recommend. So the whole thing should look like:



Now: There's not an indication like there was in the last graph. There could be, but here's there's not because I'm illustrating a principle to you. Things don't always work as perfectly as they did in the first graph I showed you. Since you are graphing the wheels with RIGHT rotation, you read the graph from right to left. The first graph was AWL so you read it left to right. Gate signatures can vary and can also be directional, as in only read as a gate from one direction. A down and up signature is the most

common type you'll get. The next one is where it drops and doesn't rise back up within a reading or two. It can rise back up, but not immediately after. That's the case in this graph. We see after 70, it drops and takes a while to come back up. That is a gate signature. The whole thing is way to wide to be a gate so the gate is going to be right under 70. Amplify your findings and you should have this:



Since gates are usually about 3 increments wide I would choose 67.5 as the gate center not 68. Now do high low test again and find which wheel is indicating. Since we already know 34.5 is the 3rd wheel we only need to do high low tests for 2 wheels not all 3.

Pay attention to the rotation direction. It's different than the first high-low tests we did because this number was found with right rotation. So every time we go to 67.5, it needs to be right rotation.
Low test:

L57.5 R67.5 R67.5 RCP: 96.5 LCP: 6 Contact area: 9 ½
R67.5 L57.5 R67.5 RCP: 96.5 LCP: 6 ¼ Contact area: 9 ¾

L57.5 R67.5 R67.5 RCP: 96 ¾ LCP: 6 ¼ Contact area: 9 ¾
R67.5 L57.5 R67.5 RCP: 96 ½ LCP: 6 ½ Contact area: 10 ¼

Let's say wheel two indicates like in the example, so now you know the combo is ?-67.5-34.5. Now, just dial in 0-67.5-34.5, 2.5-67.5-34.5, 5-67.5-34.5 and so on until it opens. You can graph this until it opens just in case the lock does not open you have something extra to refer to but usually it's not needed to graph on the final run. If you read Oldfast's chronicles you know he goes by every 2 increments. This is because it is possible to miss a number every 2.5 increments if it's a lucky s&g 6730. Personally I graph with 2.5 because I know my 6730, even though it has +/- .5 dialing tolerance, it's not that precise and will work with 2.5. With experience, you'll be able to get your own way of doing it.

Let's say in your first graph, the 2nd wheel indicated first and not the 3rd. You would graph the second graph by going all wheels LEFT to 0, right 3 times to 34.5 (actually, not 34.5 but that will be explained later in Rotational Conversion), left twice to 0. Repeat with 97.5 instead of 0. Basically, you're dialing in a combination each time because the first wheel has to be set, the second wheel has to be set in a different place than the 1st, and then the 3rd wheel has to be set different than the 2nd. If the 3rd wheel reads first, the first two wheels are parked in the same place together so there's no extra dialing for the second wheel.

If the 1st wheel reads first, the it's easy! The 2nd and 3rd wheel can be graphed without disturbing the 3rd wheel at all! If you start at 32.5, you won't pass 34.5 and mess up the first wheel there. This doesn't happen often though. The third wheel is the wheel that indicates most of the time.

And there you go!!! You should have just manipulated your first safe lock! Well, it'll take practice so you probably didn't but if you did then you're a natural :)

More “advanced” techniques (Nothing too crazy)

Ch. 3: Alternatives

There are different ways to graph and different ways to tell which wheel is indicating rather than using the hi-low method.

Alternative to hi-low

Since wheel 3 indicates most of the time, you can just park wheels 1&2 in the “forbidden zone” (the contact area. It's called that because you're not supposed to set the 3rd number to a number inside it) and then just move wheel 3 through the area you think there's a gate in. If the contact points indicate a gate, then you know it's wheel 3 because nothing else is moving! If nothing indicates, you can do the same for wheels 1&2 separately. This saves time only when wheel 3 is indicating though.

Alternative if 2nd wheel reads 1st

If the second wheel reads first, basically what you are doing is entering a new combination every time you test a number for the 2nd graph. 0-34.5-0, 2.5-34.5-0, etc. The first wheel has to be moved so you end up taking so much time! An easier way is to just put the 1st and 2nd wheel on the gate for the 2nd wheel and just move wheel 3 around. In the first place, wheel 3 usually reads first, if not, the wheel 3 is most likely going to read 2nd. This is way faster and has a high chance of you finding the second gate so I highly recommend you do this. This is what I do when the 2nd wheel reads first in a lock.

Alternative to AWL

The first obvious answer would be AWR, all wheels right. Yup, you can do that too if the lock isn't indicating any gates with AWL. It's just that 2 numbers in the combo are set with left rotation and the 3rd wheel usually indicates first; and the 3rd wheel is set with left rotation. When you set a wheel at let's say, 50, with left rotation, it will be in a different spot that if you set it at 50 with right rotation. I'll explain how to compensate for this later. You can also graph just one wheel such as the 3rd wheel so that you don't have to do hi-low or isolate wheels to find which wheel is indicating because it's the only wheel moving. But again, this is only faster if the 3rd wheel indicates first.

Make it all go faster

If you want to get fast at manipulation, you have to take some shortcuts. Don't graph. It takes WAY to much time! And only take right contact points, the right ones are enough of an indication by themselves because of the slope of the drive cam. Just go AWL and look for a suitable drop, amplify, hi/low test (just one), then move on to the next wheel. Keep going like this. Or if you're ok with some risk, just run the 3rd wheel around until you find a gate and then amplify. That way, you don't have to do hi/low testing; you know it's on wheel 3! Repeat for wheel 2. You can get 5-10min manipulations this way!

Rotational Conversion

Now if you graph with AWR and the 1st or 3rd wheel indicates or you graph AWL and the second wheel indicates first, then you need to make sure you dial to the right number. If the combo is 30-90-60, it's going to be dialed L-R-L traditionally. If you dial it in R-L-R, and then left to drop in area and right to retract bolt, it won't even drop in. The gates will be just barely off from underneath the fence. That's because with each wheel, the width of the fly and drive pins add up and push each wheel off more. The 3rd wheel will be the least affected because there's only the drive pin of the drive cam. The 3rd wheel has the drive cam, fly on the 2nd and 3rd wheel, and the drive pins on those wheels as well.

To fix this, first pick up all wheels and take them to any number. I like 50 because it's far from the contact points and I won't confuse the wheels picking up from the contact points. You can go right or left. In this example I picked up all wheels right. Now start turning left and right before you get to 50, slow down and feel for where the 3rd wheel will pick up. It might be 50 or it might be a bit off. Act like you're feeling for a contact point, be light and gentle. Let's say it picked up at 50.5. So the first wheel is .5 off. Now go around again and feel for the second wheel being picked up. Let's say that's 51.5. So the 2nd wheel is 1.5 off. Now do the same for the 3rd and let's say It picks up at 52.5. So the 3rd wheel is 2.5 off. I like to write them down like this: .5-1.5-2.5 just so I know which wheel is off by what amount. So for the combination of 30-90-60 L-R-L converting to R-L-R, we start by dialing 30 with right rotation. But we go PAST by .5 to 29.5. This puts the gate centered under the fence. For 90, we go left to 90 and PAST by 1.5 to 91.5. Same thing with the 3rd wheel. Go right rotation PAST 60 by 2.5 to 57.5. Then left until you feel the nose drop in to the drive cam and the turn right to retract the bolt!

Great job! You can now successfully manipulate a safe lock! If you still haven't got it, read on! There's a troubleshooting page :) And keep at it, this takes time and you will get out what you put into it!

Additional info: The reason I had said not to start with a LaGard 3330 is because it has more oval shaped wheels. I don't know if it's intentional or just how they're made, but the ovals all block the gates on the other wheels so you won't get any good or consistent indications from them. There's more on how to get past this in the next chapter ;)

Ch. 4: Troubleshooting

So the main purpose I wrote all this was to help people with no knowledge of safe cracking. When I started out I had many problems I had that I wasn't sure about and this section is to address those issues for others that might have those problems. If the lock doesn't open:

- High-Low tests: Make sure you are getting the high/low tests right. Put the right wheels on the right numbers and in the correct rotation. Remember: Wheel 1 is the first number in the combination so it is the wheel that's closest to the dial and gets picked up last. Wheel 3 is the last number and gets picked up first. Don't forget that or to use correct rotation.

- Dial accurately: Dial within 1/8 of an increment of where you are trying to park a wheel. It's best if you get EXACTLY on that number. If your contact point feels really faint, here's a technique Datagram taught me. Get close to the contact point and then turn the dial by lightly running your thumb along the dial with just enough friction to turn the dial. When it hits the contact point, it should stop exactly on it. Make sure you DO NOT increase the force otherwise the nose will ride up on the drive cam and you'll get a false reading. This takes practice. Try having the back of the lock open as you do this and look at it/have someone else look for you/or record it so you know just how much force to put on the dial with your thumb. If you have too light of force, you'll randomly stop and think the contact point is there.

- Read correctly: Make sure you are consistent with your readings. This is a big thing. If the increments on the dial are really wide and it's hard to pinpoint exactly where the dial is, tape a needle to the index mark you dial to and a piece of tape tapered to a point on each contact point. This helps greatly with readings since you need to be consistent down to the 1/8 increment. What you see to be 3/8 could be what I see to be 2/4 or vice versa. That doesn't matter as long as you are consistent with all your readings. Another problem is you have to make sure that you are viewing the dial from the same angle! Looking at it from different angles can give you varied readings. You can also tape paper on. This little setup was done in 30 sec and it works well enough to tell that in the picture it's on 8 3/8 not 8 1/2 or 81/4.

-Feel consistantly: Like I said before: It’s best to use a light touch and make sure that the point you take is right where the nose touches the drive cam. As long you use the SAME EXACT amount of force each time though (even if the nose does ride up on the drive cam a little) then you should still be fine. Not everyone will have the exact same points on their graphs because everyone feels with differing amounts of force, but relatively, the graphs should show the same thing. Graph the first graph with the same combination several times without looking at previous graphs until you get the same graph every time! That way, you’ll improve on your touch. It’ll take time but it’s worth it!

Sub-Chapter 4.5: LaGard 3330

I don't have too much information on this so it'll only be a sub-chapter. As explained, the LaGard has a masking effect or wheel shadowing, whatever you want to call it. This means the graphs will look like it has multiple hills/a giant hill or mountain in it. This information comes from a conversation on a site called keypicking.com. Great site to learn about lockpicking, safe cracking, etc!

For graphs with one big major hill in it:

First thing, make a first graph and find the lowest point on the graph. I'm assuming you did AWL or AWR. This means that low point, is a low point for ALL wheels. No wheel has a high point there or else it would not be low. Do something similar to a high-low test now. Put two wheels on that low point and one at the highest point. Do it for each wheel and find contact area. The widest contact area will belong to the wheel that has the big hill. Now put that wheel on the lowest area and graph the other two wheels. Keep doing this to find the highs and lows of each wheel and try to “unmask” the other wheels.

For graphs with multiple, distinct, hills:

Do the same thing as previous but for each hill. Tag each hill to a wheel so you know which wheels to park in which spot to reveal the gates on the other wheels. Put wheels 1&2 on their lowest point and isolate wheel 3 and graph just that wheel. If that doesn't work, try with just wheel 1 or just wheel 2. I prefer to try wheel 3, then 2, then 1. 1 is last because it takes longest to graph that one when isolating it.

Another way!

Take readings every 10 increments and then amplify the lowest point. Do a high-low type test and have two wheels on the highest point and one at a time put a wheel on the lowest point. Find the contact area that is the slimmest, that'll give you whichever wheel has that as a low point. Let's say wheel 3 had that point. Graph a second graph with the same method and have wheel 3 on that low spot. Find another low spot and the wheel it belongs to. Basically, you're acting like that low point is a number in the combination temporarily. Do a third graph with the other two wheels on their low spots. If it doesn't open, put the final wheel on it's low spot. You should now have low spots for all the wheels. Put wheels 1&2 on their low points and graph just wheel 3. They should allow wheel 3 to be graphed. Do this for wheels 1&2 if wheel 3 doesn't show up. After you find a gate for a wheel, put that wheel on it's gate, and pick another wheel to isolate and graph.

Acknowledgements: Thanks to everyone at keypicking.com! Especially Oldfast for large portions of information as well as getting me started in this hobby! And to my girlfriend for the motivation to write this :)