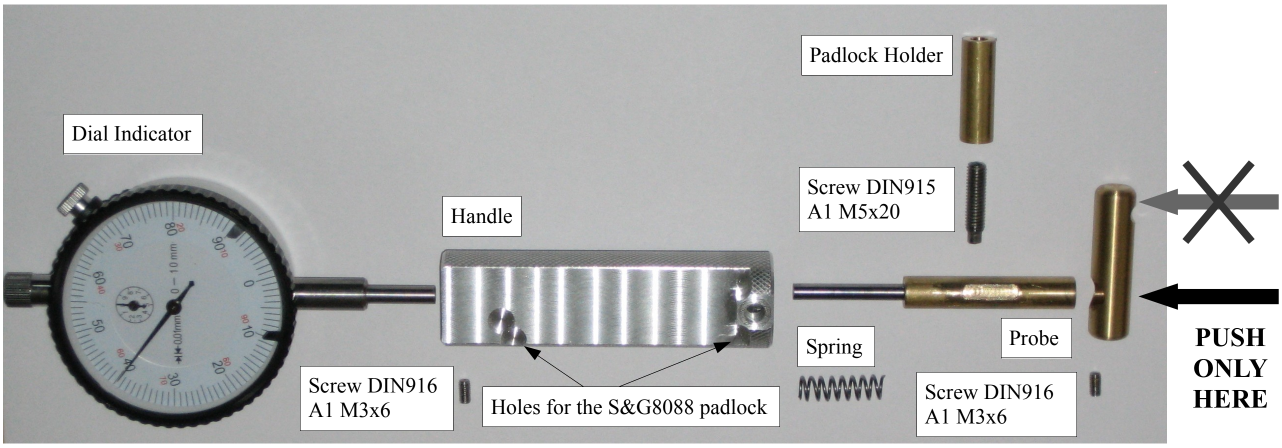
# Welcome to your new **mhPadlockDecoder**,<br>a precision tool that can help you to decode combination padlocks.

This tool consists of five custom parts that have been manufactured using manually controlled precision machinery in a process that takes more than two hours, an off-the-shelf dial indicator, and three screws. Please handle the tool carefully, do not drop it onto hard surfaces, and be **careful how you apply pressure to the probe: only push it down on the short end. Do not try to turn the probe.** Pushing down on the long end (the end that interfaces with the padlock shackle) can lead to torque which would damage the probe[1].

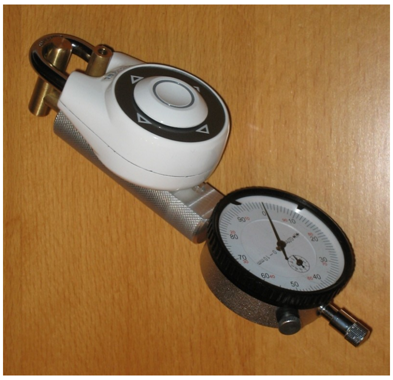


*Picture 1: What's inside.*

While this decoder can be used for different padlocks, the following description covers a specific padlock that works on directional movements ([Up], [Down], [Left], [Right]) of a knob.

## How to use the tool.

Hold the aluminum handle in your hand and push the probe into the tool, then glue the padlock to the handle using double sided adhesive tape[2]. The 8mm brass padlock holder should touch the padlock body, and the probe will now push against the shackle.



*Picture 2: Padlock attached.*

Whenever you intend to reset the padlock by pushing the shackle into the padlock body, or when you plan to dial a combination quickly and reliably, first push the probe into the decoder handle with your thumb.
However, if you need to measure the feedback from the lock while moving the knob, you can let the decoder's internal spring push against the shackle for you.

[1] If the probe has been damaged in this way, the probe will not move easily inside the aluminum handle any more, and you will need to take the tool apart and use a file to remove the deformation on the probe.

[2] The tape that comes with the decoder will allow for easy removal of the padlock later, by simply pulling hard on one edge of the lock.

Just note that sometimes a combination cannot be reliably dialed while pushing against the shackle. Also, under some circumstances the built-in spring is not strong enough, and you need to pull on the shackle yourself to get a correct reading.
Sometimes pulling on the bottom probe part of the dial indicator and then releasing it – so that it hits against the probe part of the tool – helps to get a more consistent reading.

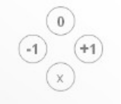
**The decoding process.**

At this time, you should be familiar with the lock design (otherwise read the paper that's located at the bottom of the http://toool.nl/ main page) and you should have the mhVisualizer application (located at the same web page) running on a computer in front of you.

The decoding process works -as usual- because of mechanical tolerances: Pulling on the **shackle** will try to turn the lock's **locking cross** into the four disks. The locking cross can only turn if the disks have been turned to the correct angle, so that the four tips of locking cross can move into the **gates**. However, the disks block in a certain order, so that you can set the disks one after another and do not need to try all states.

The tool can read the status of the locking cross: fully closed or partially open, and it can distinguish between "more open" and "less open" when you try out different states of the disks. The **indicator on the dial will turn counterclockwise when more disks are set correctly** (i.e. when the shackle can be pulled out further). You can expect around 1/100mm..5/100mm of shackle movement for each gate that you found. Hint: If you forget the direction, you can always find out by pushing the shackle in, and you will see that the indicator will turn clockwise.
To compare different states, turn the scale on the dial indicator so that it reads zero, then try a different state and simply check whether the indicator now reads more or less than zero. To turn the scale, you might first need to release a little thumbscrew on the side of the dial indicator.

The lock has a number of **known constraints** that help to speed up the process:
(A) The upper disk usually blocks first.
(B) The last move of the combination sequence will leave three disks in a certain relation to each other (-1, 0, +1) – this is shown in the upper right hand corner of the mhVisualizer application for your reference.



(C) Repeating the last move 5 more times will yield the same state you had before the five moves.

The decoding process consists of **two simple steps** that are repeated until the lock opens:
(1) Find a gate on one or more disks.
(2) Verify on which disks you have found gates.

So let's get started.

Dial a sequence of [Up] moves, until you find that the indicator turns counterclockwise a bit, and note how much it turns. According to (C), the same behavior should occur again after five more moves. When the indicator turns counterclockwise, this means that you have probably found the gate on the upper disk.
If this happens at the end of a move, the last move in the correct sequence is either [Up] or [Down]. If it occurs during a move, but at the end of the move the indicator turns clockwise again, the last move in the correct sequence is [Left] or [Right] or [Down]. In that case, try dialing a sequence of

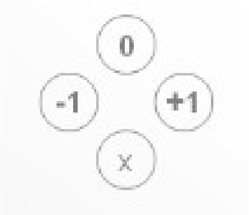
[Left], and / or a sequence of [Right].
When you found the gate on the upper disk, mark it in your mhVisualizer application.

This concludes step (1), you should now go to (2) and verify the gate by turning single disks in the mhVisualizer application and trying the sequences that it suggests to you. The dial indicator should show less shackle movement when the disks have been turned by plus or minus one increment from the assumed gate position.

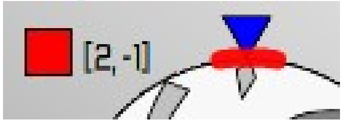
Now we try to find the next gate.

According to (B), you already have some information about the last movement in the correct sequence: it's either [Down], or you can derive it from the gate on the upper disk. Assuming the last movement is not down, it depends on the M index[3] of the upper disk:

| **M index of upper disk** | **Last movement in the correct sequence** |
|---|---|
| +1 | [Left] |
| 0 | [Up] |
| -1 | [Right] |



Example:



Here, the M index -1 indicates that the last movement is [Right]
(or [Down] – [Down] is always an option as well and needs to be tested if the other option doesn't yield good results).

Assuming the last movement is e.g. [*Right*], then you can try all 5 possible positions of the *right* disk (in this example valid positions of the right disk have an M index of 0, cf. (B)),
and check if one of them shows more shackle movement than the others. While doing this, keep the upper disk at the gate that you have already found before.
Once you have found a gate, mark it in your mhVisualizer application.

Then try the same for the lower disk (in this example valid positions of the lower disk have an M index of +1, cf. (B)).

In this example, the left disk is unaffected by the last movement and can therefore have the gate on any of the 15 possible positions; therefore you would need to try out all 15 positions on the left disk.

If you do not get consistent readings and the verification step (2) fails during the process described above, you should at some point in time assume that the last movement is [Down] and try the disk positions accordingly.

At the end of this process, the padlock will open. Usually, you will notice this while you pull on the

[3] The mhVisualizer application displays the [N, M] index of each disk next to the corresponding disk.

shackle manually in order to apply force to the disks; or sometimes the internal spring of the tool is strong enough to open the lock.

Sometimes the lock doesn't open consistently with the tested sequence; this might happen when some of the movements – esp. the last movement – have been executed while pulling on the shackle. In this case, try to reproduce what happened in the mhVisualizer application and turn the disks one by one back and forth, until you find a correct sequence.

While the decoding theory might seem to be simple and straightforward at first glance, it does require some puzzle solving skills, training, proper estimation, concentration, and a little bit of luck; and if you like this type of challenge, the lock and the tool will offer many hours of fun for you.

For your first attempts, knowing the last movement in the sequence might be helpful; later have somebody else set your lock to a new random combination, so that you don't know the last movement.

I hope you will have lots of fun with this tool :)
If you have questions or comments, you can reach me at mh@TheOpenSourceLock.org

[*The Open Source Lock* project (TOSL) aims at designing the perfect lock – thoroughly tested by the world's best lock experts and hackers – that will offer well known and tested security without obscurity. If this project seems interesting to you, let me know.]

**Appendix: mhVisualizer Keyboard Map.**

To select one of the disks – so that you can turn it or to set a marker – use:

```
   u              8
h     j   or   4     6
   n              2
```

Both sets of keys work, the letters are better suited if you do not have a numeric keypad on your laptop computer. Hint: <u> corresponds to the *u*pper disk. Make sure caps lock is off.

**Disclaimer.**

The opinions expressed here are those of the author only; the author is not affiliated with the lock manufacturer in any way; the lock manufacturer or the author’s employers have nothing to do with this document or the tool. All trademarks are the property of their owners. Some of the concepts and techniques mentioned in here are protected by intellectual property rights such as patents. The information might be incomplete and / or contain errors. The tool might not work as intended, fail unexpectedly, and your hands and fingers might hurt after using the tool. Worse things might happen. It's all your own responsibility. **The author gives no warranty and accepts no liability whatsoever concerning this document or the tool.** If for any reason such exclusion is not possible, the author's liability shall be limited to the purchase price of the tool.