

## Re: Master Key crack

**Source:** <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-07/2110.html>

---

**From:** Richard Herring (*junk\_at\_[127.0.0.1]*)

**Date:** 07/30/03

Date: Wed, 30 Jul 2003 09:55:31 +0100

In message <3f26c2b3\$1\_2@news.vic.com>, John E. Hadstate  
<nospam@null.nil> writes

>

> *"Richard Herring" <junk@[127.0.0.1]> wrote in message  
> news:KO4eUTtVapJ\$EwcG@baesystems.com...*

>> *In message <3f2677e9\$1\_2@news.vic.com>, John E. Hadstate*

>> *<nospam@null.nil> writes*

>>>

>>> *"Stuart Green" <greens80@hotmail.com> wrote in message*

>>> *news:1761049f.0307290239.28dd7f11@posting.google.com...*

>>>> *I remeber reading an article about a guy who utilised a master key*

>>>> *hack, known to locksmiths, to identify pin placements on a key and*

>>>> *grind them down progressively to build a masterkey for a lock.*

>>>

>>> *[...]*

>>>

>>>> *In a simple system producing one Master and one Owner key for each lock,*

>>>> *each pin position in the lock has two short pins inserted. The length of*

>>>> *the first pins in each pin position establish the cut heights for the*

>>>> *Owner*

>>>> *keys. The sum of the lengths of the first and second pins in each*

>>>> *position*

>>>> *establish the cut heights for the Master key. The pins come in standard*

>>>> *lengths, and there are constraints on the maximum height differences*

>>>> *between*

>>>> *adjacent pins. Typical locks come with 4, 5, or 6 pin positions.*

>>>>

>>>> *There are a finite number of combinations of pins that make up each*

>>>> *Master*

>>>> *series. Thus, one might enumerate all the possible pin placements for*

>>>> *owner*

>>>> *keys for each Master series. Then, given a few owner keys known to be*

>>>> *part*

>>>> *of one Master series, one might search the entire tree of pin*

>>>> *combinations*

>>>> *until one established which Master series included all the given owner*

>>>> *keys.*

>>>> *This would establish the cut lengths for the Master key for that series.*

sci.crypt: Re: Master Key crack

>> >  
>> >*I suspect that for any decent system, you would need a lot more than 4  
>owner  
>> >keys to establish which Master series they belong to (although there are  
>> >some Master series for 4-pin tumblers that produce a very small number of  
>> >usable owner keys).*  
>> >  
>> >*I think the "master key hack" mentioned by the OP is the one where one  
>> sequentially varies the height of a single pin on one known Owner key to  
>> determine the Master height at that pin. In principle, given one Owner  
>> key and access to the keyhole, that will yield the complete Master  
>> heights using as many blanks as there are pin positions, plus a lot of  
>> filing.*  
> s  
> s  
> s  
> s  
>gggpggggg  
> p  
> 1  
> 1  
> 1  
> 2  
> 2  
> k  
> k  
> k  
>  
>*To make this Owner key work, "k" has to push p up by 1 unit (so it aligns  
>with "g").*  
>  
>*To make the Master key work, "k" has to push p up by 4 units (so the lowest  
>"1" aligns with "g").*  
>  
>*Thus, the Owner key has to be cut more deeply at each pin position than the  
>Master key.*  
>  
>*So, other than showing a maximum cutting depth for each pin position, how  
>does the Owner key reveal the Master key?*

(Not just the Owner key, the Owner key plus access to the keyhole with a set of test blanks:)

1. By indicating which of the two possible depths of each pin is `_not_` that of the Master.

2 By providing a known working depth for all the other pins.

--  
Richard Herring