Keys to the Kingdom

Deviant Ollam
Who am i?
Who am i?
Who am i ?

THE CORE GROUP

The Open Organisation Of Lockpickers
Who am i?

THE CORE GROUP

auditing
assessments
research
trainings

workshops
public
lectures
lockpick
village
contests &
games

The Open Organisation Of Lockpickers
The Open Organisation Of Lockpickers
The Open Organisation Of Lockpickers
Lockpicking is Fun, Fun, Fun!
First, a word about rules...

Yes, we have rules. 😊

1. Do not pick locks which you do not own.

2. Do not pick locks which you rely on.
Doorknobs...
Padlocks...
Deadbolts...
...The Mechanism Itself Is All The Same
How It Looks Inside
Attempt Without a Key
Operating With a Key
Pin Stacks
Using a Key
Using Lockpicks
Master-Keyed Systems
Master-Keyed Systems
Master-Keyed Systems
Master-Keyed Systems
Master-Keyed Systems
Master-Keyed Systems
Master-Keyed Systems

ALICE

BOB
Master-Keyed Systems
Master-Keyed Systems
Master-Keyed Systems
Master-Keyed Systems
Master-Keyed Systems
Master-Keyed Systems
Master-Keyed Systems

---

[Image of key with different colored pins and numbers 4 7 3 3 4]
Master-Keyed Systems
Attacking Master-Keyed Systems

“Master-Keyed Lock Vulnerability”
by Matt Blaze
2003-01-27

http://www.cryptoc.com/masterkey.html
Consider Alice's key... for a lock.
Change Key Bitting Depths

3 6 2 3 5
Obviously, it Works in the Lock...
Obviously, it Works in the Lock…
So, What Can We Infer About the Inside of the Lock?
Pins Must Be At the Edge of the...
... They Could Simply be Solid Key...
... But the Specific Details are...
... And these Unknowns are Hidden
... And these Unknowns are Hidden.

So What to Do
Prepare Exploratory Key Number
Prepare Exploratory Key Number

Zero

Cut

0
Prepare Exploratory Key Number

Zero Cut

Bitting Depths
Already Known From Change Key

0 6 2 3 5
This Key Will be Used to Sweep
Beware That MACS Issues Can...
File Position One Down a Bit
File Position One Down a Bit
File Position One Down a Bit
We're Still Encountering MACS
But Let’s Try the Key Anyway…
But Let’s Try the Key Anyway… the Lock Fails to Open
Remove the Key
File Position One Down to the Next Bitting Point
Although They Look Different, These Are Both #2 Cut Depths
MACS is No Longer Being Violated
So, Let’s Try the Key Again…
So, Let’s Try the Key Again… the lock fails to open.
Remove the Key
File Down Position One Again
Let’s Try The Key Again…
Let’s Try The Key Again...OPEN!
Of Course, That Was Expected
Remember the Change Key?
We’ve Duplicated That
We Have Learned Something, ...
We Don’t Know About These
3 6 2 3 5
But Now We Know That This Key...
Of Course, There Could Still Be
So, There is More Exploring to be...
Try They Key...
Try They Key... And Find It Does Not Work
Remove the Key
File Down Position One to the Next Bitting
Try the Key...
Try the Key... and Find it Does Not Work
Remove the Key
File Position One Down another Depth
Try the Key in the Lock...
Try the Key in the Lock... OPEN!
So What Has Been Learned Now?
All Drivers Must Be Raised
Properly Right Now
Given What We Know From Before, this is the Current Picture...
We Still Haven’t Explored These Chambers…
We Know This Key Pin
We Know This Mastering Pin
There’s a Chance of More Shear
Remove the Key
File Position One Down a bit
Try the Key...
Try the key... and find it does not work.
You Can Continue For The Rest of the Bitting Range...
(If There is More to the Bitting...
If There is More to the Bitting

Kwikset Depths

Don't Go Past 7

etc etc etc 6 2 3 5
Prepare Another Key, for Exploring Position Two...
Prepare Another Key, for

Discover ed
Master Depth

6
Prepare Another Key, for

- Zero
- Cut

- Master
- Depth

- Discover
- ed

6 0
Prepare Another Key, for Exploring Position Two…

- Zero Cut
- Depths Known From Change Key
- Master Depth
- Discover Depth

6 0 2 3 5
NOTE - The Zero Depth is Almost Never Used
So, Save Time by Starting
Position Two at the #1 Depth…
MACS is Being Violated Here
But Let’s Try the Key Anyway…
But Let’s Try the Key Anyway… The Lock Doesn’t Work.
Remove the Key
File Down Position Two by a Bitting Depth
MACS is OK now, BTW
Try the Key in the Lock...
Try the Key in the Lock... The Lock Doesn't Open...
Remove the Key
File Position Two Down by a Bitting Depth

6 3 2 3 5
Try the Key...
Try the Key... the Lock Doesn't
Remove the Key
File Position Two Down by a Biting Point
Try the Key...
So What Have We Learned Now?
The Drivers Must be at the Plug’s Edge…
And Now We Know the Following...
We’ve Learned This Earlier
We Don’t Know About These
But Now Our Exploring Here is Kind of Done
There is a Shear Line Here
There is a Shear Line Here, We Know From Our Change Key...
There is a Shear Line Here, We Know From Our Change Key…
So We’re Basically Done with
So We’re Basically Done with Position Two… How Come?
Single Depth Mastering Pins are Rare and Bad…
So, a Five Depth is Highly Unlikely
If We Wanted, We Could Take Our Key...
And File Down to the 6th Bitting Depth...
Try the Key...
Try the Key... It Surely Should
After All...
After All… Depth b was Known in Position Two
Further Exploring Is Not Really Necessary Here...
A Depth of Seven?
A Depth of Seven Would Mean Another Single Depth Pin…
... And Kwikset Locks Don’t Go

6 7 2 3 5
So... Now Three Chambers Remain
Let's Prepare a Third Exploring
What Cut Will be in Position?
A #6 Depth, The Mastering Depth
(By the Way... Is This a Valid Key...?)
(By the Way... Is This a Valid Key?)

Answer - No. This would violate MACS since we're dealing with a Kwikset lock.
What Cut Will be in Position

6
A #4 Depth Will be There... The
Master Cut Discovered Earlier

6 4
What Will We Do in Position

6 4
Leave Position Three Blank For

6 4 0
And For the Rest of the Key?
Finish Off with Depths Known

Executing the Change...
So, Now it’s Time to Explore…
So, Now it’s Time to Explore... Or
Remember the Change Key’s Known Depth...
So What About #1 and #3 Depths?
A #1 Depth Would be Unwise
A #3 Depth Would be Unwise, Too
And #2 Depth Was Already Known, So Skip It...
Thus, #4 Depth is an Ideal Starting Point.
This is a Much More Efficient Exploring Range,
Key 3 is Prepared
Key 3 is Tried...
Key 3 is Tried... It Doesn't Turn
Remove the Key
File Down by One Cut Depth
Try the Key...
Try the Key... OPEN!
This Tells Us Quite a Lot
So, Let’s Discuss What We Know
Mastering in Position Three
But Otherwise, Position Three Seems Pretty Dialed...
Would We Need to Explore a "6"?
Would We Need to Explore a #6 Pin?

I wouldn’t. That would mean there’s a single-depth mastering pin in there. Most professional locksmiths would know better than to use one when building a system.
How About a #7 Depth?
How About a #7 Depth?

While it's possible to have multi-mastered pin stacks, this is rare. Personally, I'd skip it and just make a note to myself saying, "Come back later if I get stuck."
Let’s Prepare a Fourth Exploring
Start Out with Mastering We’ve Discovered Thus Far
Leave Position Four Blank
Exploring Key Number Four, Fully-
Keep in Mind, This Violates MACS
We Could Sweep This Exploring…

6 4 5 0 5
But Remember This is the Change
New Bitting...
More Efficient: Only Explore
Key Four, First Attempt...
Key Four, First Attempt... No Go.
Remove the Key

![Key Diagram]

6 4 5 1 5

http://tool.us
If Desired, File to the #3 Depth,
Give the Key a Try…
Give the Key a Try... OPEN!
That Was Expected, of Course
Remove the Key
File Down… Skipping a Depth, to

6 4 5 5 5 5
Try the Key...
Try the Key... No Luck.
Remove the Key
File Down by Another Depth
Try the Key...
Try the Key... No Joy.
Remove the Key
File Down to the Last Depth
Try the Key...
Try the Key... Nope.
So, WTF?
Maybe You Question Yourself
In This Case... Position Four is Not Mastered
The Master Key We’ve Decoded Thus Far
Let’s Prepare a Fifth (and Hopefully Final) Exploring Key …
Code-Cut the Mastering We’ve Discovered So Far...
Leaving the Fifth Position Free
Attempt Either at the Blank
Try the Key... OPEN!
That’s a Heaping Bowl of Awesomesauce
There's a Very Real Chance We Know it All Now...
The Mastering Might be Fully Decoded
True, There *Could* be Another Cut...
There Could Even be Other Cuts
But Personally, I'd Just Start
Of Course, Your Key Will Likely Look Like This…
Of Course, Your Key Will Likely Look Like This

(Since most likely you will be hand-filing all cuts, not working with a code-cutter to set up your exploring keys.)
Speaking of Hand-Filed Keys…

Beware of Canyoning!
The Internals of our Original Door Lock...
These Marks Represent the Mastering Depths
Here's a Hypothetical Alternate...
A Winnar is You!
Mitigating Against This Attack?

- Restricted Keyway / Restricted Blanks
- Secondary Monitoring Systems
- Audit Trails / Access Control Scheduling
- Use Entirely Separate Zone Arrangements
- Move Away From Tumbler System
Other Badass Lock Designs
High Security Locks - Side Bar
High Security Locks - Pin-Based Side Bar
High Security Locks - Pin-Based Side Bar
Pin-Based Side Bar - Schlage Primus
High Security Locks - Side Bar Only Design
Rotating Discs
Rotating Discs
Rotating Discs
Rotating Discs
Rotating Discs
Rotating Discs
Rotating Discs
Rotating Discs
Rotating Discs
Rotating Discs
Rotating Discs
Rotating Discs
Rotating Discs
Rotating Discs
Magnetic Locks
Magnetic Locks
Magnetic Locks
Magnetic Locks
Magnetic Locks
Magnetic Locks

photo courtesy of Eric Schmiedl
Magnetic Locks

photo courtesy of Eric Schmiedl

http://tooll.us
A New Contest At HOPE
Master-Key Escalation Contest
Master-Key Escalation Contest
Master-Key Escalation Contest
Master-Key Escalation Contest
Master-Key Escalation Contest
Master-Key Escalation Contest

Will j00 be teh winnar?!?
Master-Key Escalation Contest

SATURDAY

ESCALATOR Action

SUNDAY

SATURDAY
Thank You Very Much!

http://tool.us

info@tool.us

This presentation is CopyLeft by Deviant Ollam. You are free to reuse any or all of this material as long as it is attributed and freedom for others to do the same is maintained.