Exploiting Keyspace Vulnerabilities in Locks

Bill Graydon

@access_ctrl
b.graydon@ggrsecurity.com
github.com/bgraydon

Take a look at your keyring...

Outline

- How locks & keys work
- Intro to the tools I’m releasing
- Brute forcing all possible keys
- Reading the pins in a lock
- Impressioning with extra information
- Keyed alike systems & lock disassembly in nonmastered systems
- Information theory and entropy
- How master keying works
- Deriving a master key from multiple low-level keys
- Rights amplification in mastered systems
- Special cases: construction keying, IC cores, Medeco, Mul-T-Lock
- Remediation

Software Analysis Tools

Try it yourself!

https://ggrsecurity.com/personal/~bgraydon/keyspace

Or:

https://tinyurl.com/key-space

Source:

https://github.com/bgraydon/lockview
https://github.com/bgraydon/keyspace

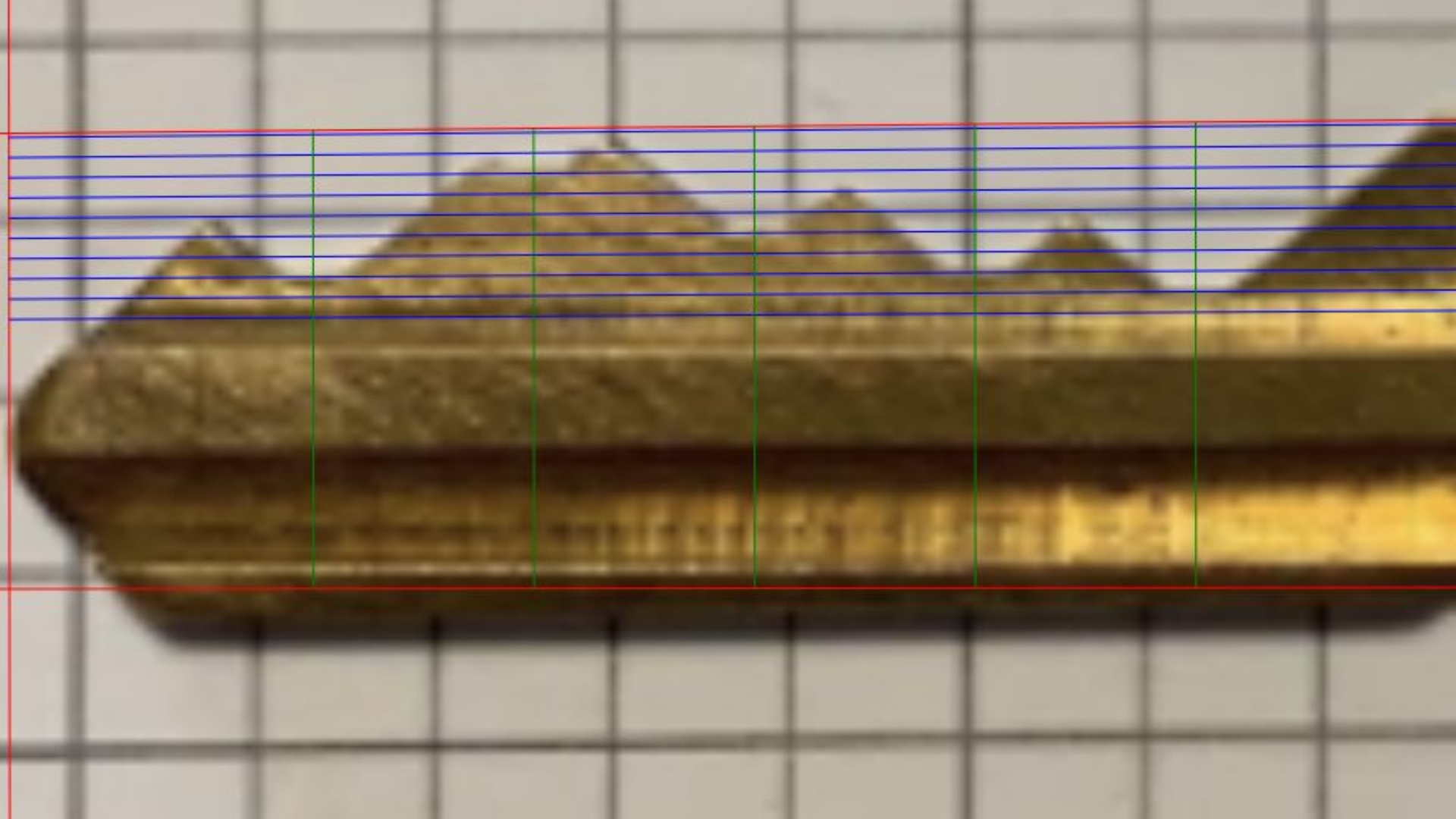
How Locks Work

Demo →

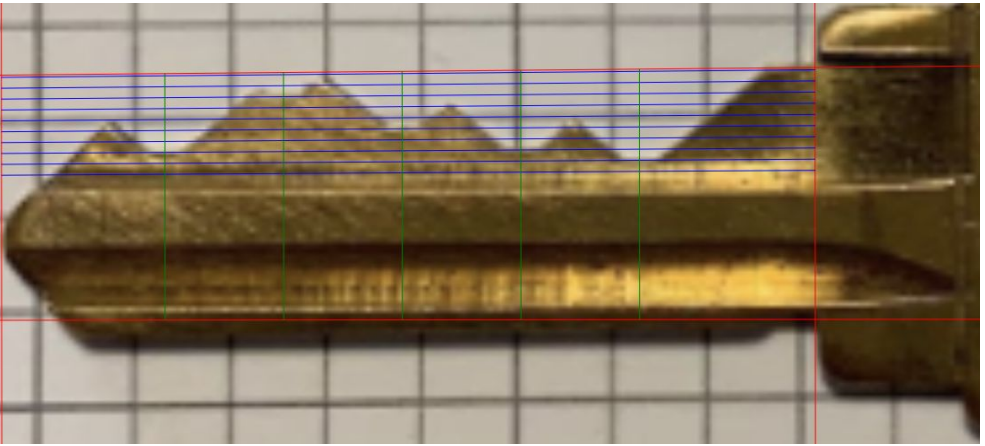
What is a key?

Mechanically encoded information.

Background | Key Codes



Background | Key Codes | Bitting



87527

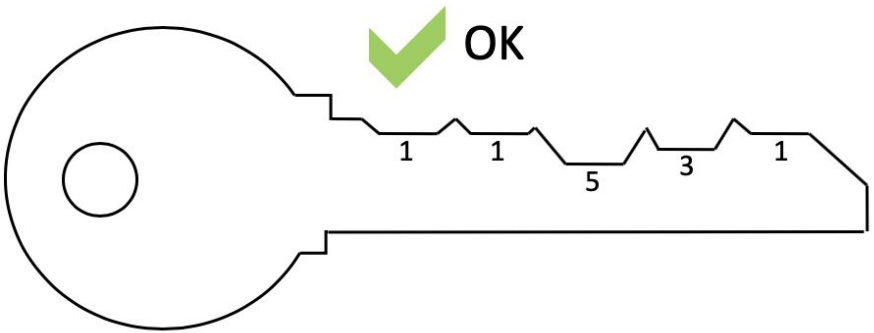
#	INCH	MM
0	0.335	8.51
1	0.320	8.13
2	0.305	7.75
3	0.290	7.37
4	0.275	6.99
5	0.260	6.60
6	0.245	6.22
7	0.230	5.84
8	0.215	5.46
9	0.200	5.08

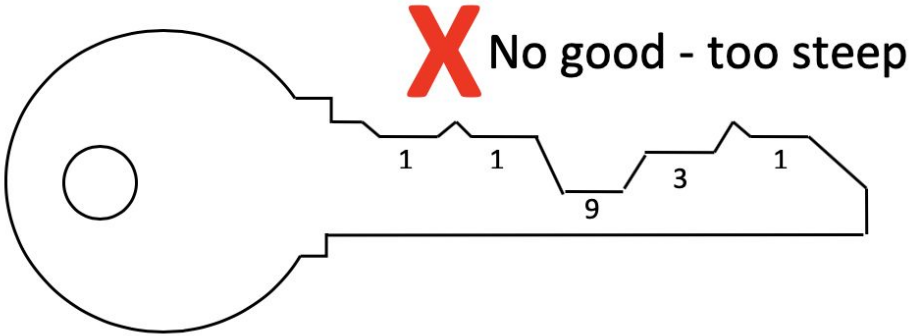
Background | Key Codes

87527

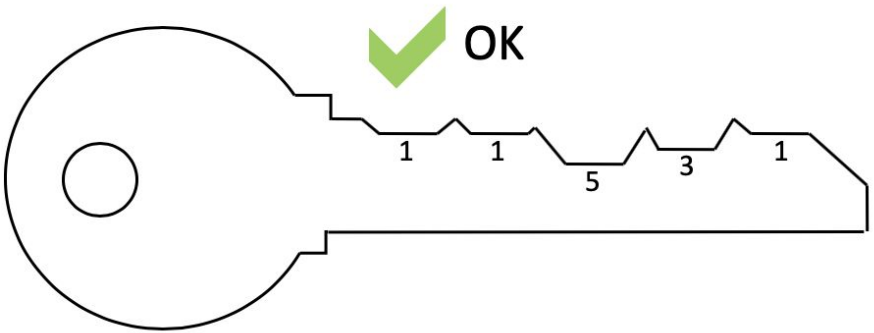
52864

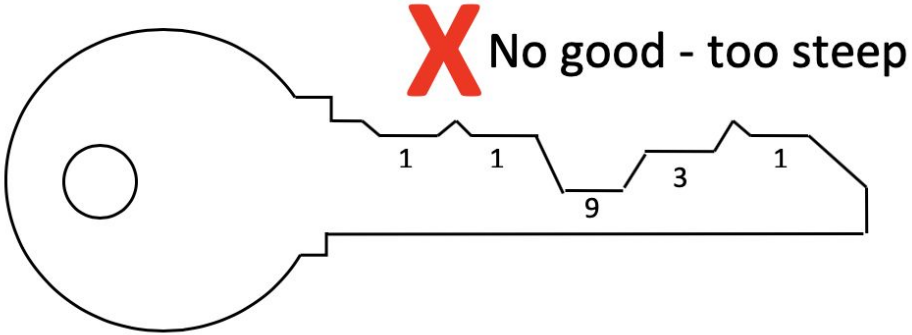
MACS - Maximum Adjacent Cut Specification





MACS - Maximum Adjacent Cut Specification





Demo →

MACS = Maximum Adjacent Cut Specification

Key Type	MACS
Schlage	7
Kwikset	4
Sargent	7
Yale	7
Weiser	7
Medeco	2,3,4

Keyspaces

Demo →

In theory -

Number of depths to the power of the number of spaces

E.g. -

Schlage - 10 depths, to the power of 5 or 6 spaces - 100,000 or 1,000,000 possible combinations

Medeco - 6 depths, to the power of 5 or 6 spaces - 7000 or 46000 combinations

There are further limitations imposed by physical constraints!

Keys vs. Passwords

Trait	Password	Key
Cost to try one	$0.00000000001	$0.30-$10.00
Detectability of brute force	Possible	Challenging
Length	Unlimited	Severely Limited
Complexity	Unlimited	Limited
Ease of changing	Easy	Costly and time-consuming
Privilege levels	Unlimited schemes	Limited to hierarchical*

The Economics of Brute-Force Attacks

Brute force = trying all possible keys

If we have n key codes to try, we need at most n blanks, possibly fewer

- Blanks cost between $0.13 and $3.00 - the common ones are cheap
- If you have access to a code cutting machine, the marginal cost of a new key cut is the blank + your time
- If you do not, locksmiths will cut keys to code for $3.00-$10.00 each

E.g. - if you can reduce the keyspace of a given lock to 1000 possible keys, the cost might be $450 (you own a code machine, blanks are $0.45 each) or $4000 (you need to use a locksmith, cost per cut key is $4.00)

Demo →

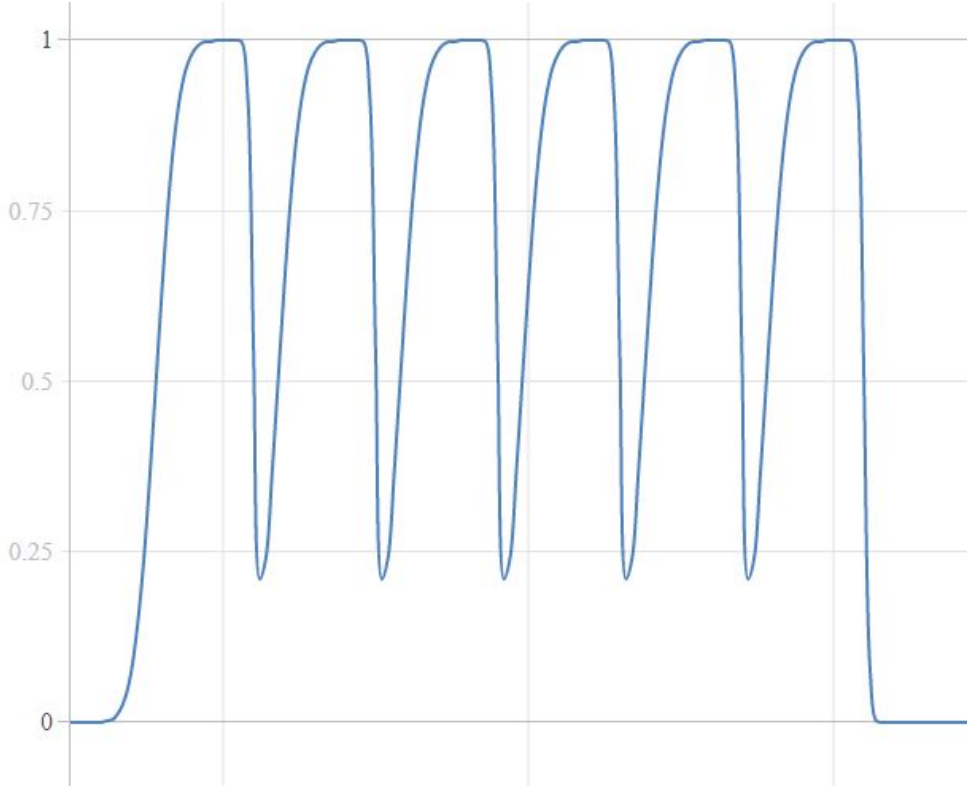
Try-Out Key Set for "Smart" Type Locks that use the KW1 Key 256 Set

Try-Out Key Set for "Smart" Type Locks that use the KW1 Key 256 Set

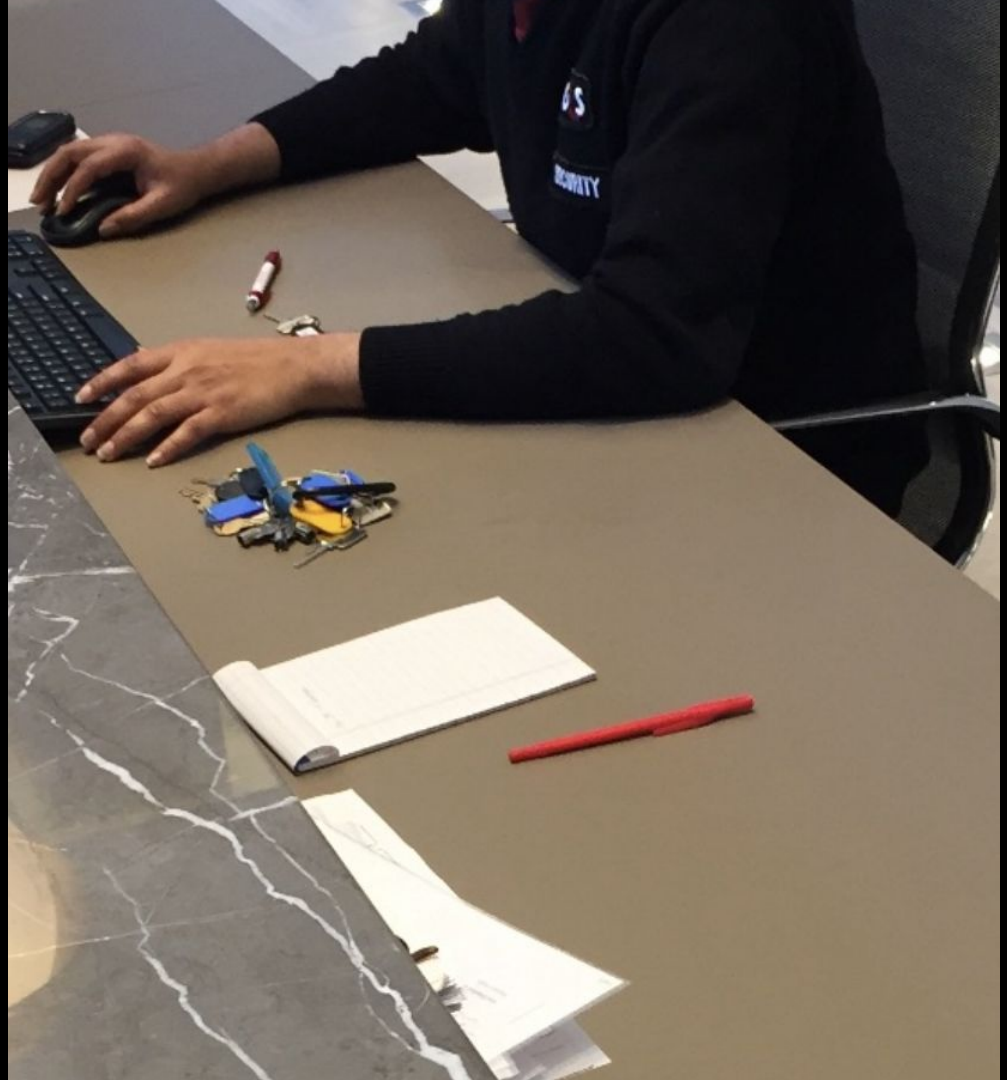
Your Price: $394.90

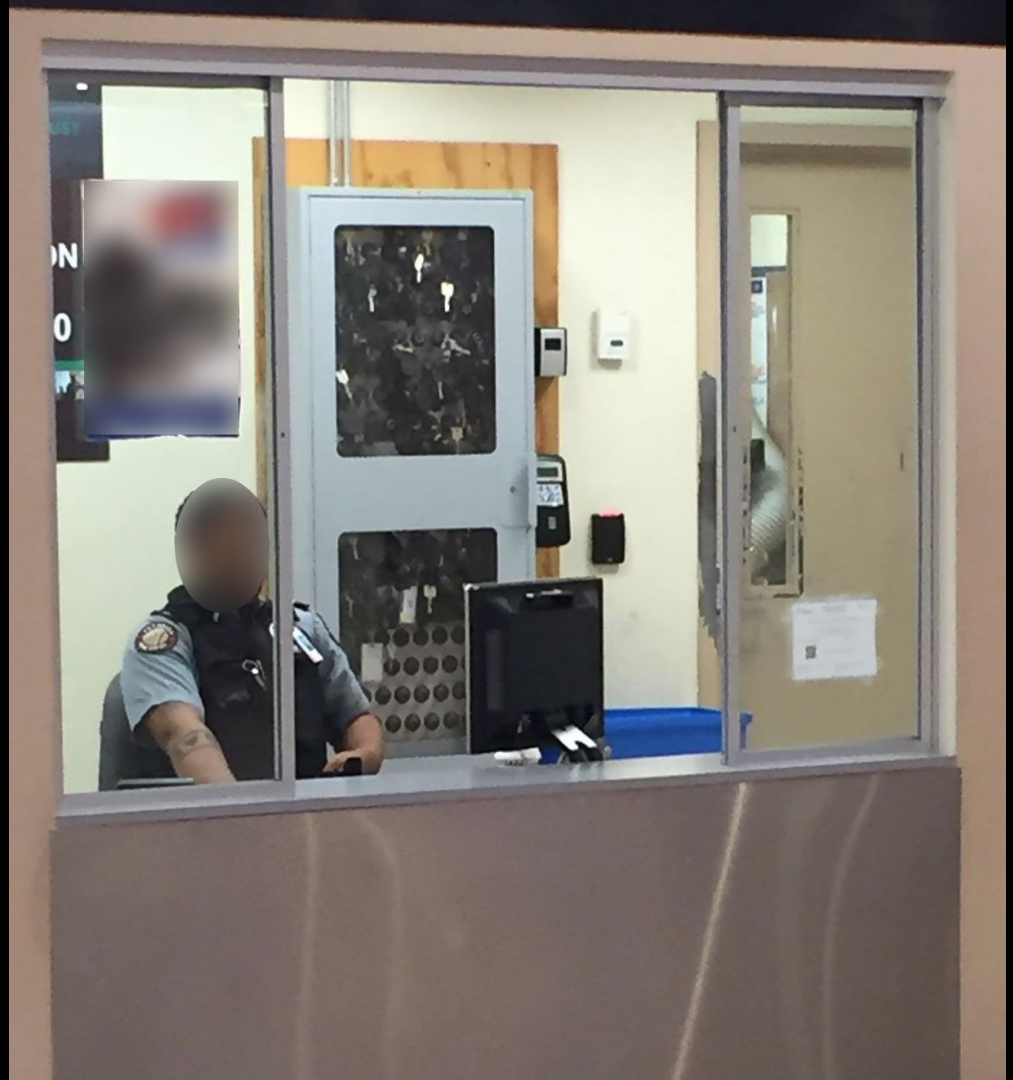
This Tryout set has 256 keys in it, expect to have 98% success with all "smart key" type locks that use the KW1

Lock Tolerances



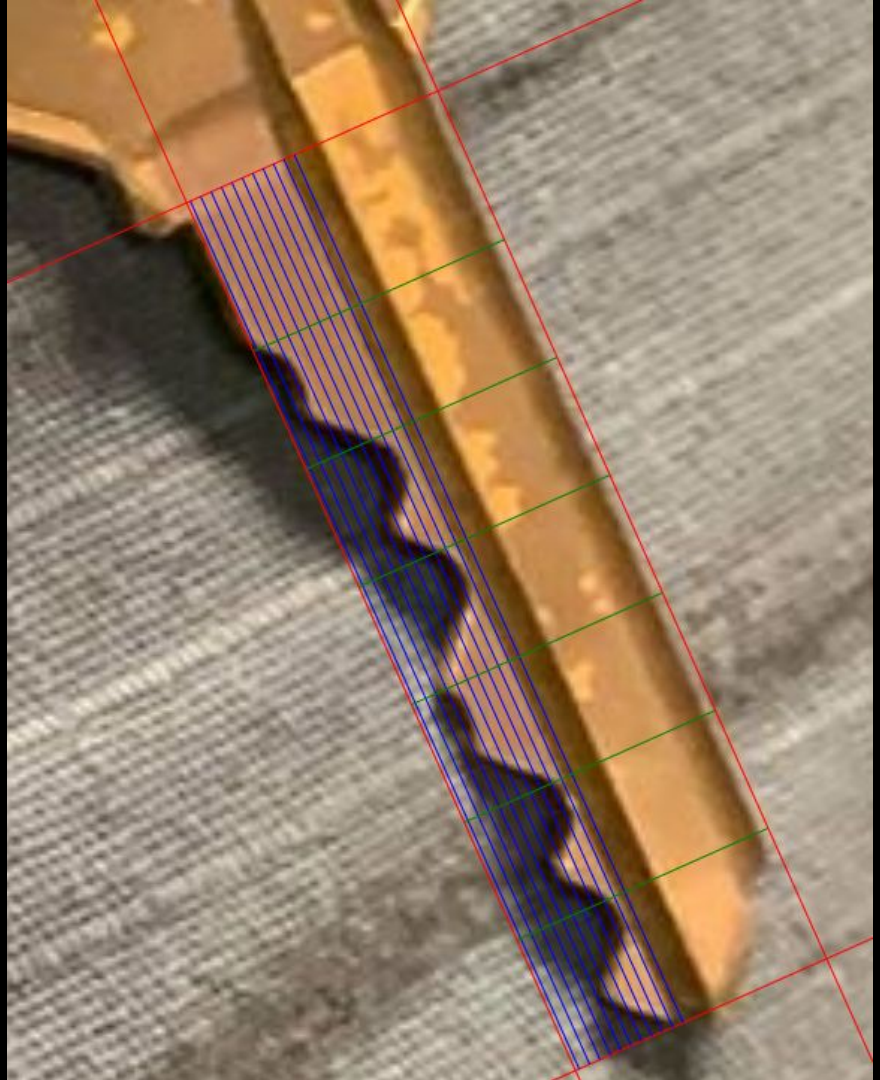
Demo →






MM
AA


KW1
HUCO




X1S10

GM Try Out Key Set

Part Number: GMPK

Your Price: $85.95

LOWEST PRICE GUARANTEE

click here for more info

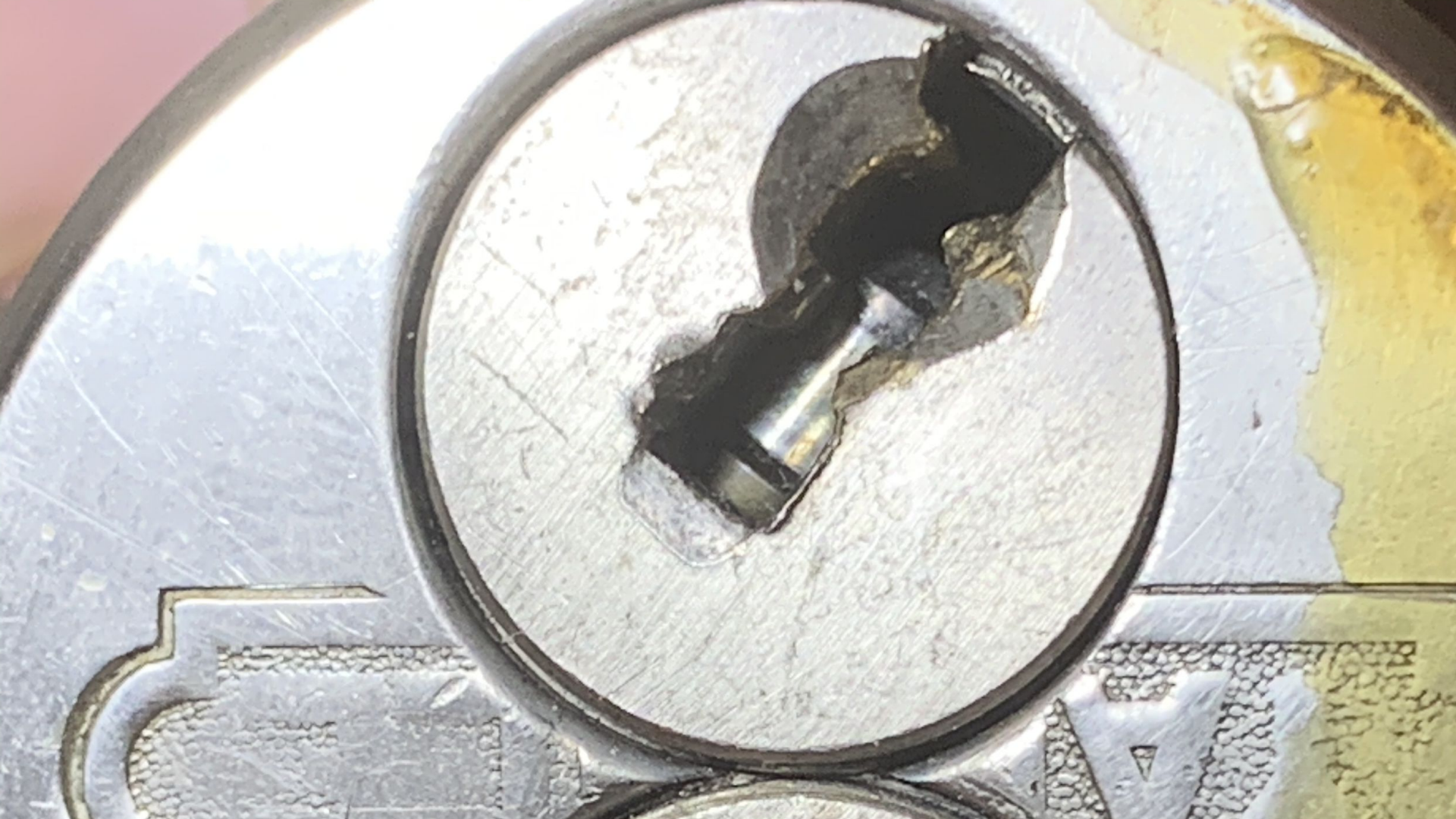
Be the first to review this product

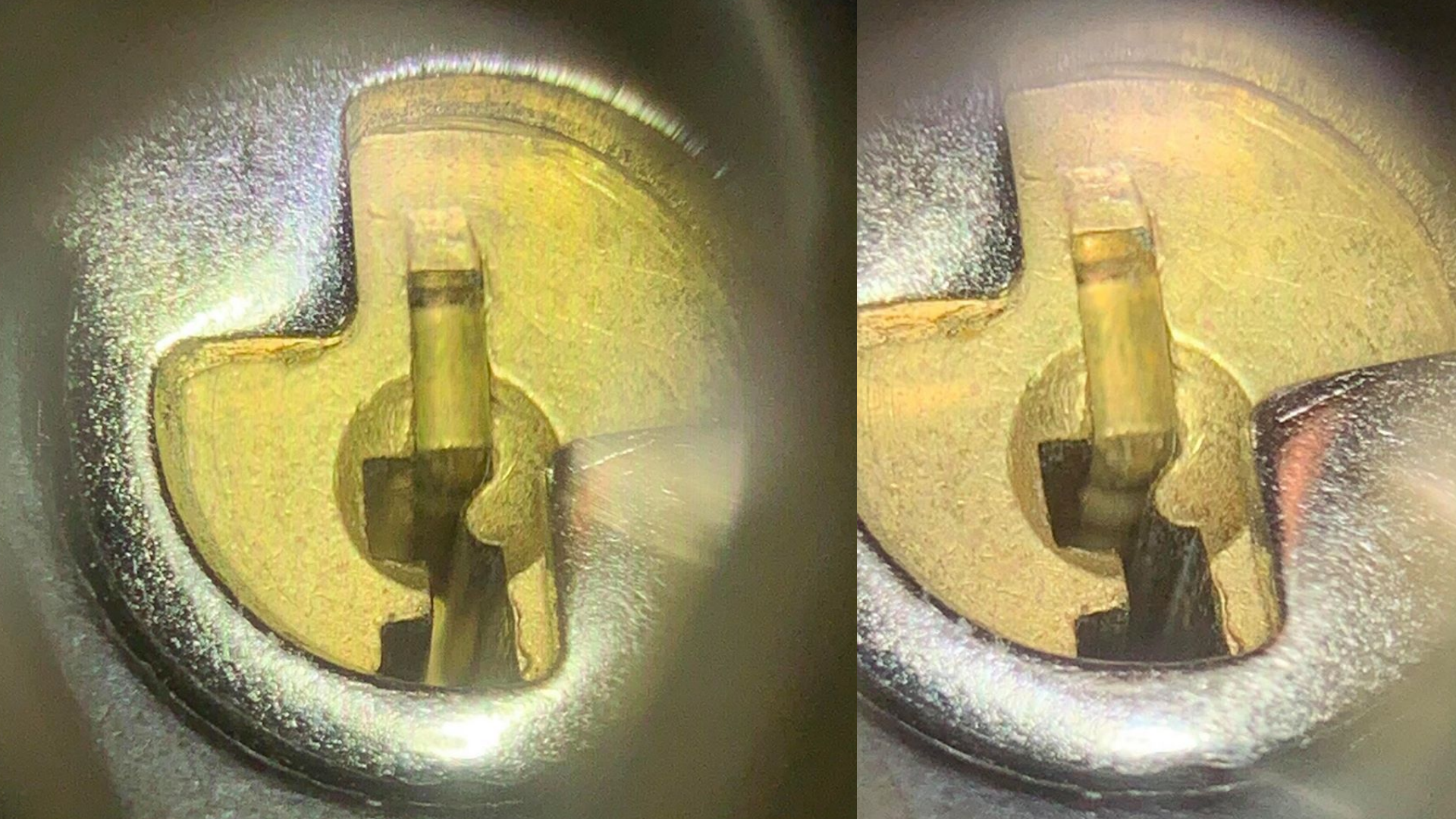
GM Try Out Key Set
62 key set

Description | Additional Info | Reviews | Tags

Try out keys are used in many cases as a first try. The success rate with this set is about 80%. (for GM's from 1967 - 1987 models) Set works on doors, trunks, and ignition for all single sided keyways A-K.

Decoding Locks






.156B.C.
159B.C.
.162B.C.
.219B.C.
.222B.C.
.225B.C.
.282B.C.
.285B.C.
.288B.C.
.342B.C.
.345B.C.
.348B.C.

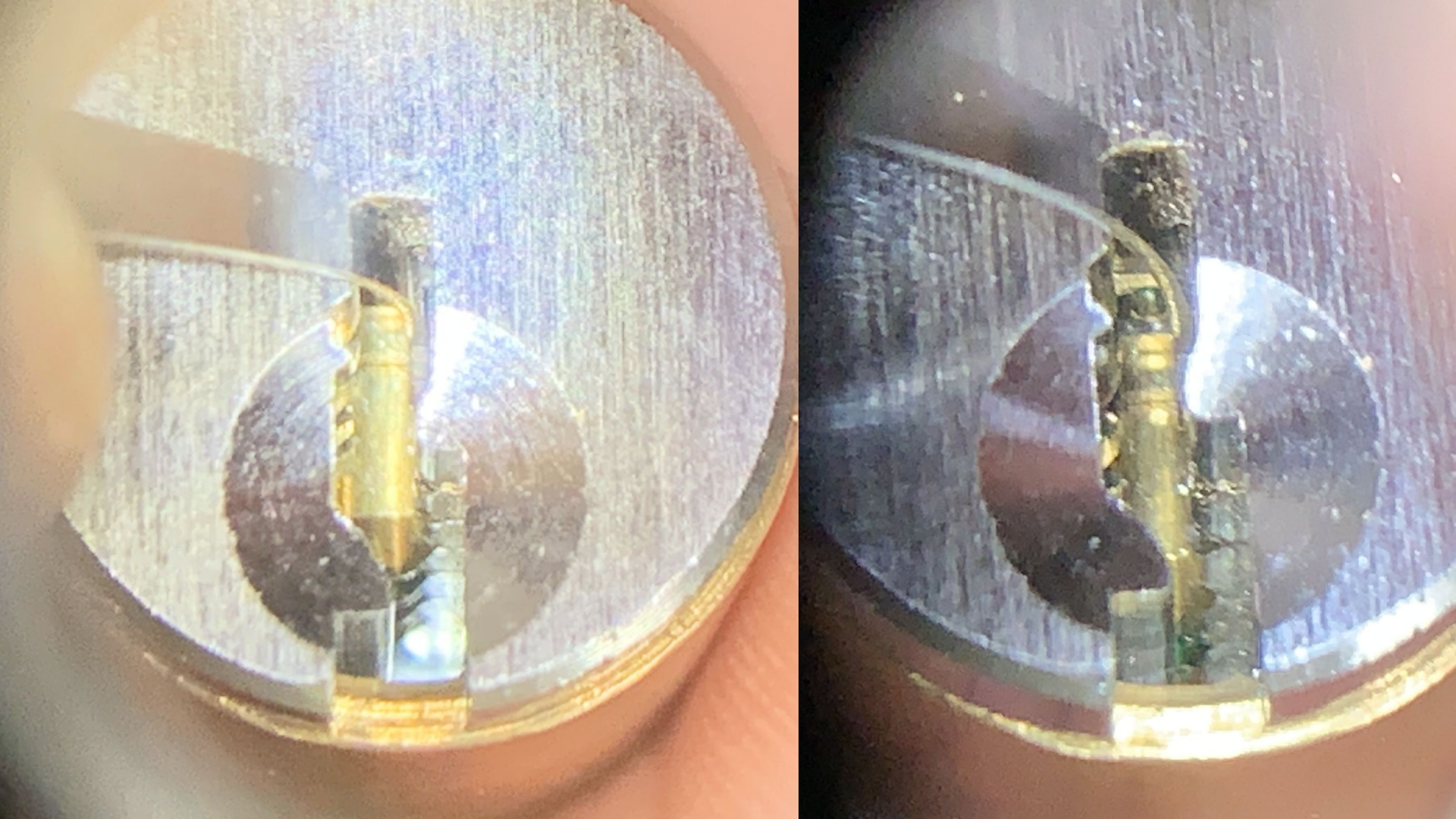

E-2402
Re-Key
A LOCK
Re-Keying Set for Up to Six Locks
Ensamble para cambiar hasta seis cerraduras para puertas.
Trousse pour modifier jusqu'à six serrures de portes.
Takes only minutes • THREE keys included
No locksmith needed • Lock not included
SCHLAGE
"C" TYPE LOCKS
All you'll need is a screwdriver!
PRIME-LINE
E-2402
you'll need is a screwdriver!
PRIME-LINE


SARGENT .020

Depth of Cut	Bitting No.	Bottom Pin	Master Pin	Top Pin
.330	1	.171	—	
.310	2	.189	.039	*.219
.290	3	.210	.060	
.270	4	.231	.081	
.250	5	.249	.099	.180
.230	6	.270	.120	
.210	7	.291	.141	
.190	8	.309	.160	.145
.170	9	.330	.180	
.150	0	.351	—	

EPD = .498 TFC = .216 BCC = .156 MACS = 7

* INVERT .219 BOTTOM PIN USE AS TOP PIN



Password Re-Use

- Is bad

Key Re-Use

- Is called “keyed alike” and is a common and accepted arrangement

In a keyed-alike system, the key space is 1!

Keyed Alike - When Your Keyspace is 1

- Elevators
- Most alarms (i.e. Detex)
- Enterphone systems
- Most controller boxes
- Golf carts
- Heavy equipment
- Police cars
- Traffic light controllers
- Telecom boxes
- Almost all other utilities
- New York City
- HVAC / Building automation systems
- Many city’s fire safety boxes
- Many regional Knox boxes
- Vending machines
- Postal keys
- Luggage - TSA keys
- Handcuffs

HOPE XI: Howard Payne & Deviant Ollam, This Key is Your Key, This Key is My Key

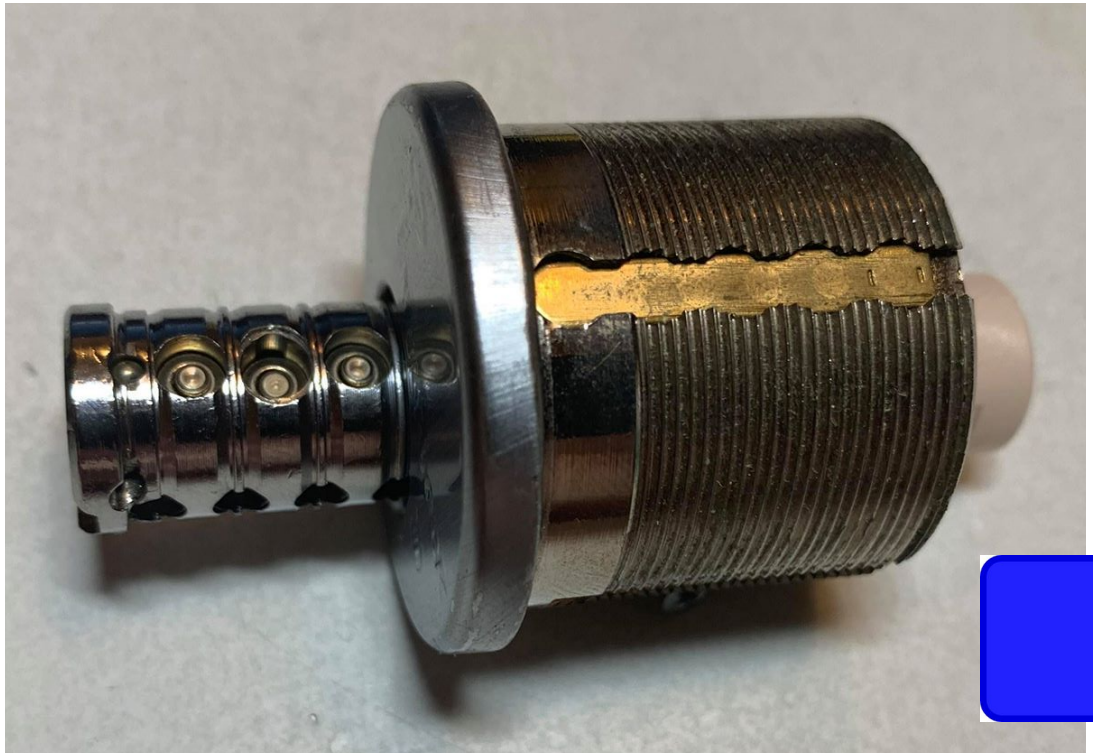

THE BO


Mircom
WIPE YOUR FEET
UPON ENTRY


POSTAL
LOCK BOX
MADE BY DOORKING INGLEWOOD, CALIF.

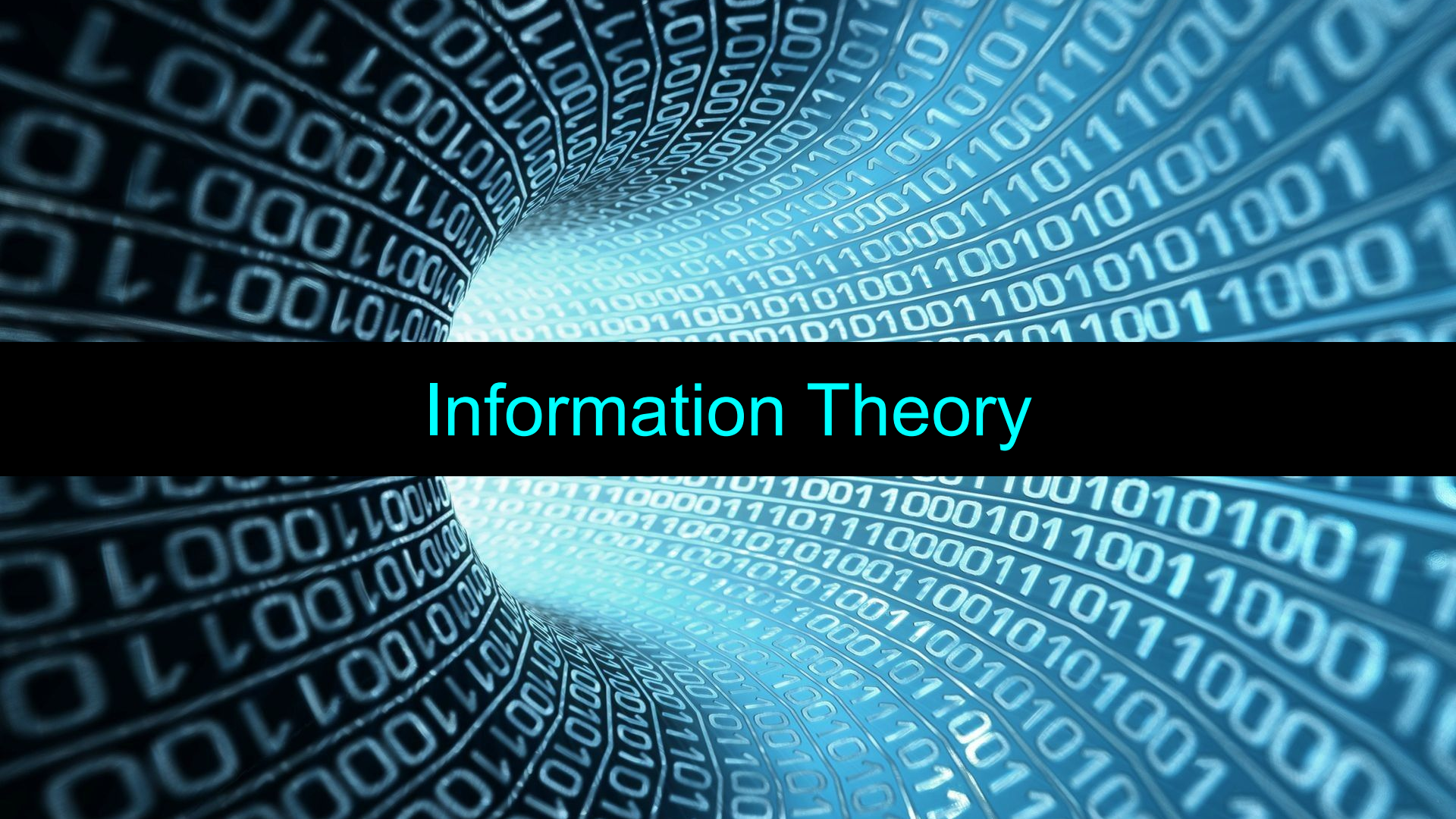

FORT LOCK
CHICAGO, ILLINOIS

Lock Disassembly



Demo →

DEF CON 26 - m010ch - Please Do Not Duplicate Attacking the Knox Box



Information Theory

Shannon Entropy

Information = stuff we know.

Entropy = stuff we don't know.

We know whether a stop light is red or green. The colour of a stop light is **information**.

We don't know the outcome of a random variable, such as a coin flip or a dice roll. A coin flip and or dice roll has **entropy**. A key or password has entropy.

Measuring Entropy

Once we *do know* the information, how many bits on a hard drive will it take to write it down (on average)?

A coin flip → **one bit**

A random number 0..255 → **8 bits**

A random number 1..10 → 3.32 **bits**

3 random numbers 1..10 can be encoded in a number $0..10^3$.
We can use 10 bits to encode 0..1023. So 10 bits will encode 0..999.
10 bits / 3 random numbers 1..10 ≈ 3.33 ≈ **3.32** bits / random number

Measuring Entropy

Number of bits it takes to write down a number 0..x
→ $\log_2(x)$

Number of bits of entropy (H) for a random variable with n outcomes:
→ $H = \log_2(n)$

E.g:

A fair coin flip, 2 outcomes: $\log_2(2)$ = **2 bits**
A random number 0..255: $\log_2(256)$ = **8 bits**
A random number 1..10: $\log_2(10)$ = **3.322 bits**

Key Entropy Examples

Number of bits in a piece of information (e.g. key, password) -

- 8-character ASCII password - 8*8=256 bits of entropy
- 10-digit passcode, 3 characters long - 1000 combinations or 9.97 bits
- EVVA MCS key, 4 rotors with 8 positions each - 8^4=4096 or 12.00 bits of entropy
- Schlage 5-pin system - 5^10 or 100000 combinations (16.6 bits)

If there are N possibilities, and all possibilities are equiprobable, then entropy (H) is given by:

$$H = \log_2(n)$$

If some possibilities are more likely than others, entropy goes down. E.g., dictionary-based passwords; avoidance of deep cut keys; key coding to deter picking

Entropy: 2 Possibilities, Unequal Probability

Master key decoded to 14767 or 94767…

When 50/50 chance…

$$H = -p_1 \log_2(p_1) - p_2 \log_2(p_2)$$
$$H = -0.5 \log_2(0.5) - 0.5 \log_2(0.5) = -\log_2(0.5) = \log_2(2) = 1 \textbf{ bit}.$$

Are these equiprobable?

$$H = 0.95 \log_2(0.95) + 0.05 \log_2(0.05) = 0.286 \textbf{ bits}$$

In the extreme, if one option is certain, that's 0 bits!

In general… $H = -\Sigma\, p \log_2(p)$

Joint+Conditional Entropy, Mutual Information

Demo →

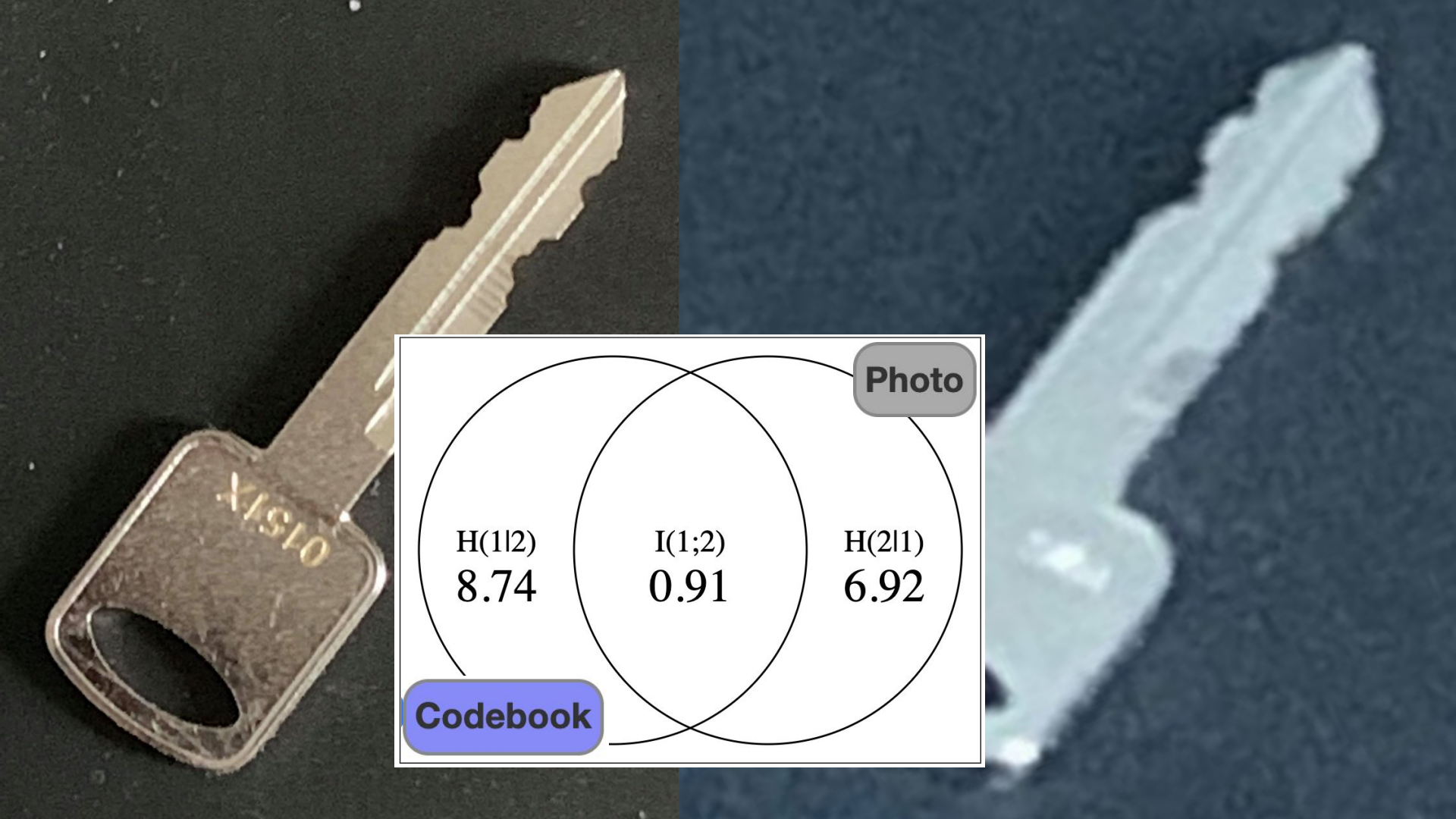
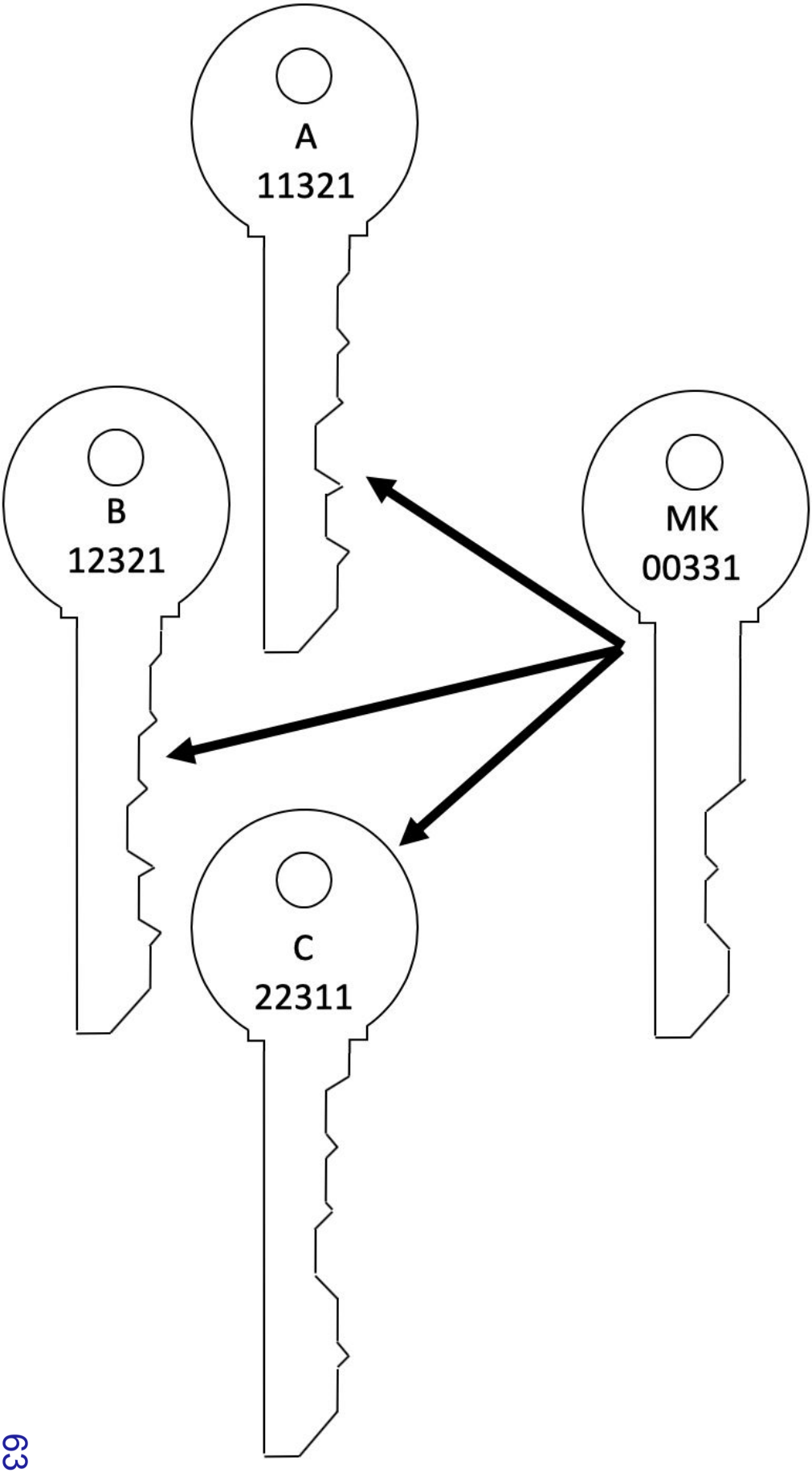


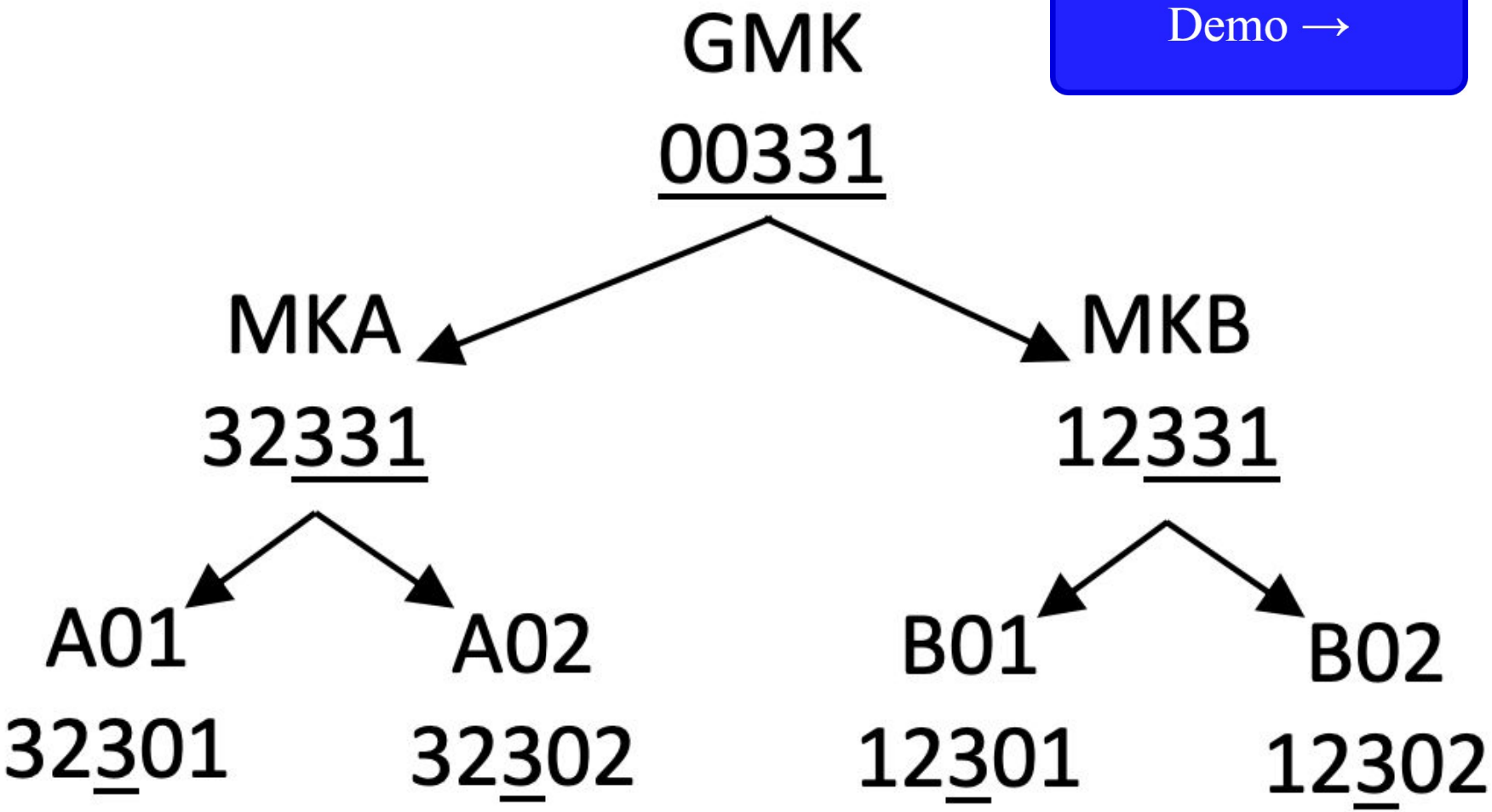
Photo
H(1|2)
8.74
I(1;2)
0.91
H(2|1)
6.92
Codebook

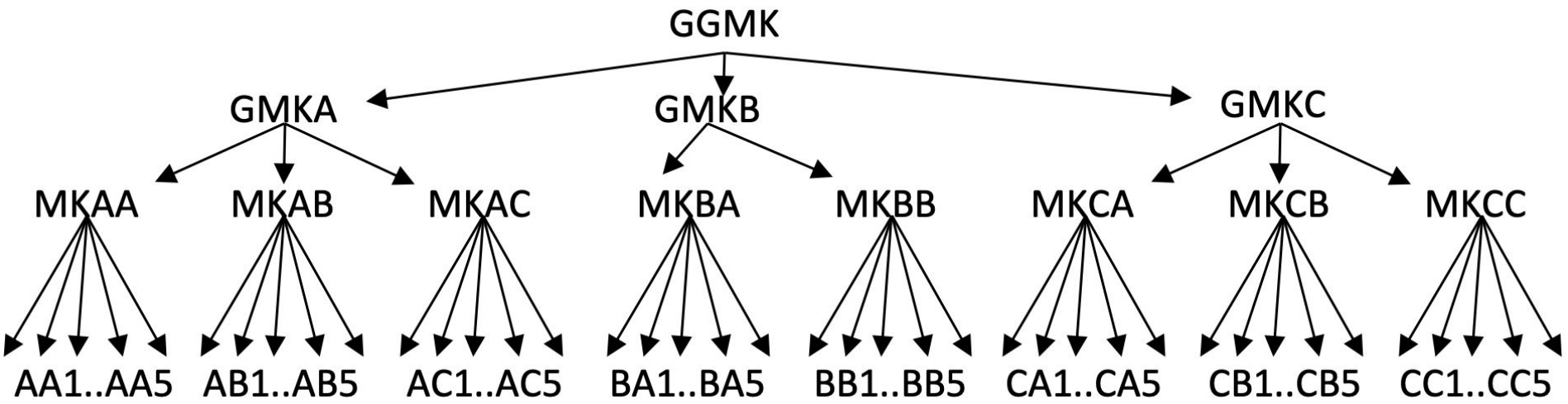
Master Keying

Demo →


A
11321
B
12321
MK
00331
C
22311

Demo →


GMK
00331
MKA
32331
MKB
12331
A01
32301
A02
32302
B01
12301
B02
12302


GGMK
GMKA
GMKB
GMKC
MKAA
MKAB
MKAC
MKBA
MKBB
MKCA
MKCB
MKCC
AA1..AA5
AB1..AB5
AC1..AC5
BA1..BA5
BB1..BB5
CA1..CA5
CB1..CB5
CC1..CC5

SARGENT .020

Depth of Cut	Bitting No.	Bottom Pin	Master Pin	Top Pin
.330	1	.171	—	
.310	2	.189	.039	*.219
.290	3	.210	.060	
.270	4	.231	.081	
.250	5	.249	.099	.180
.230	6	.270	.120	
.210	7	.291	.141	
.190	8	.309	.160	.145
.170	9	.330	.180	
.150	0	.351	—	

EPD = .498 TFC = .216 BCC = .156 MACS = 7

* INVERT .219 BOTTOM PIN USE AS TOP PIN

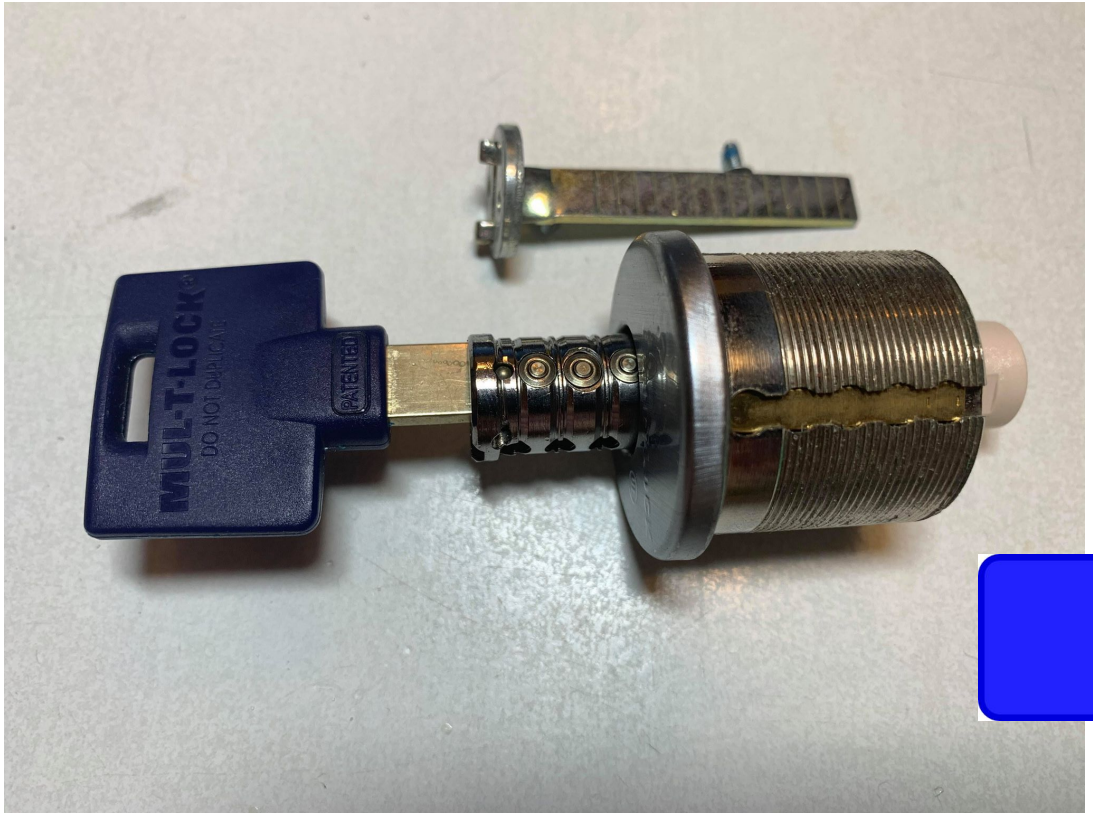
SARGENT .020

Depth of Cut	Bitting No.	Bottom Pin	Master Pin	Top Pin
.330	1	.171	—	
.310	2	.189	.039	*.219
.290	3	.210	.060	
.270	4	.231	.081	
.250	5	.249	.099	.180
.230	6	.270	.120	
.210	7	.291	.141	
.190	8	.309	.160	.145
.170	9	.330	.180	
.150	0	.351	—	

EPD = .498 TFC = .216 BCC = .156 MACS = 7

* INVERT .219 BOTTOM PIN USE AS TOP PIN

Master Keyed Lock Disassembly



Demo →

Deducing the Master from Multiple Change Keys

Demo →

LA
LOCKED

Rights Amplification

Demo →

Construction Core Systems

Demo →

Interchangeable Core Systems

Demo →


SCHLAGE
CONTROL


Yale


SCHLAGE


RESTRICTED
NOT DUPLICATE
mobiado

159 Possible Medeco TMKs If…

Intelligence: large facility

Intelligence: IC System

Demo →

Reduce further with change keys and other information.

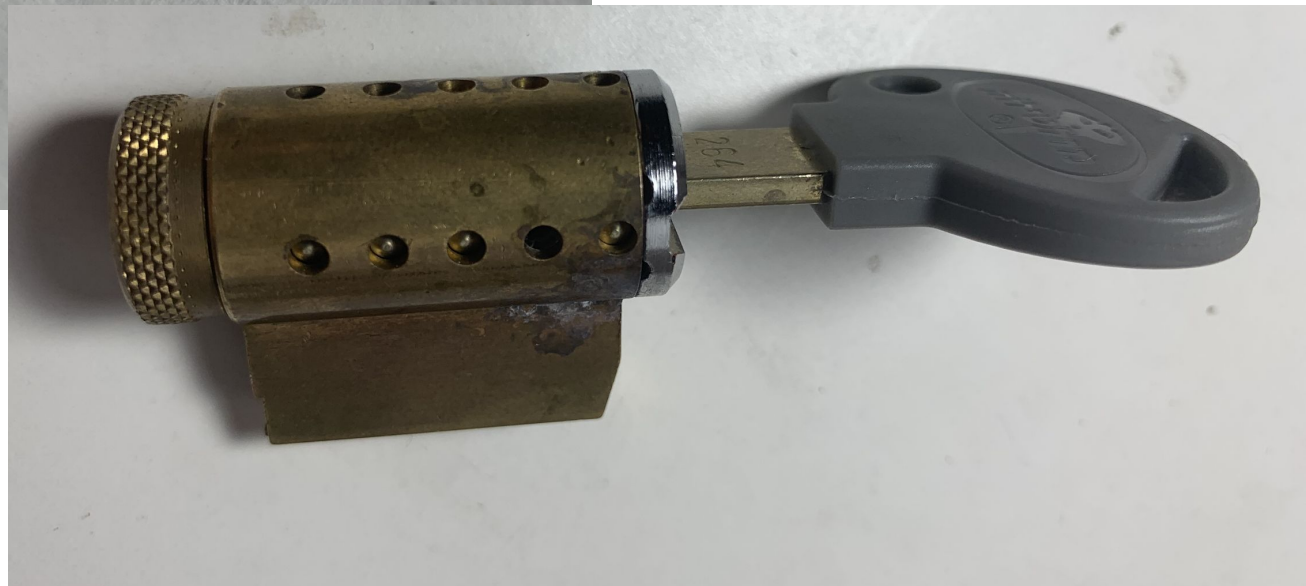

MUL-T-LOCK
UL


MUL-T-LOCK
INTERACTIVE+
DO NOT DUPLICATE
MT5 TM


264

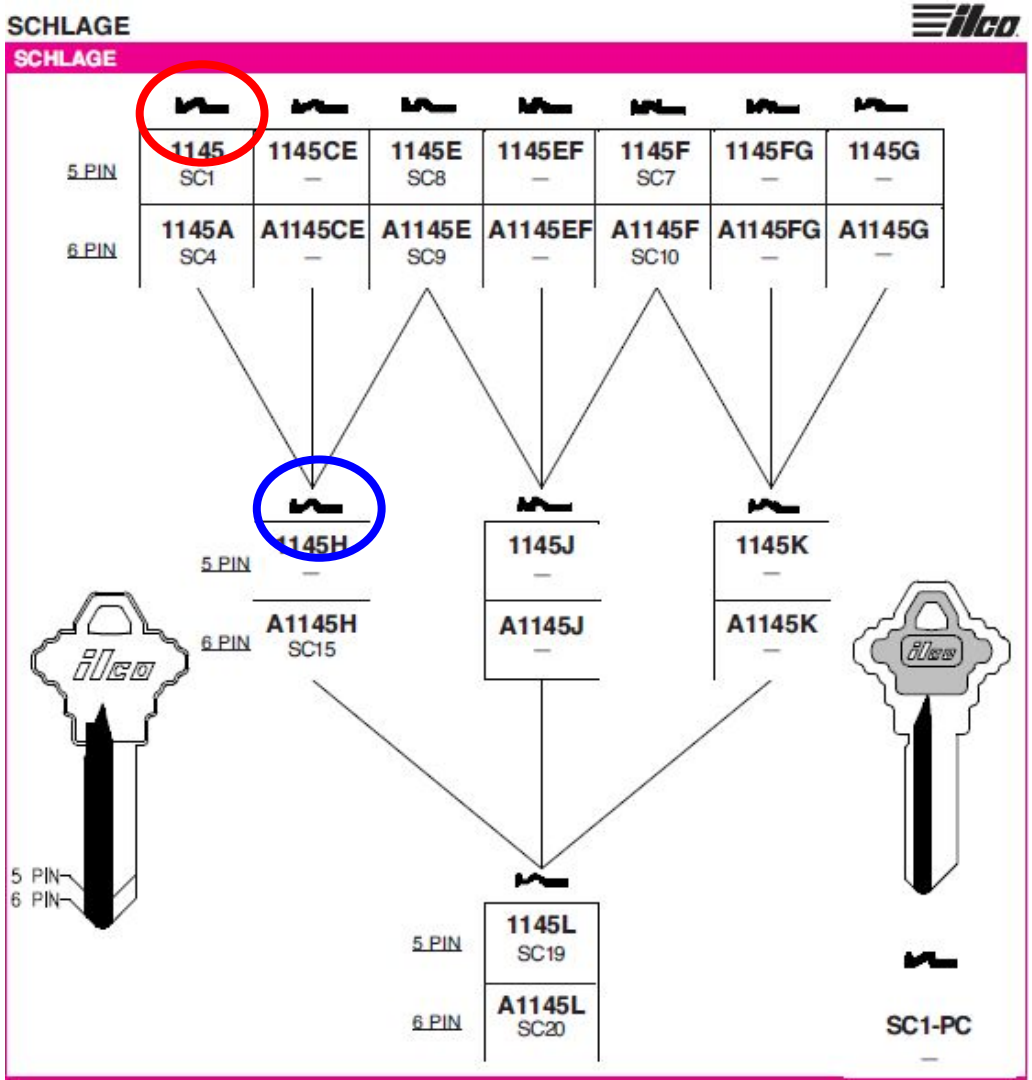
Correct Key:

Incorrect Key:




284


284

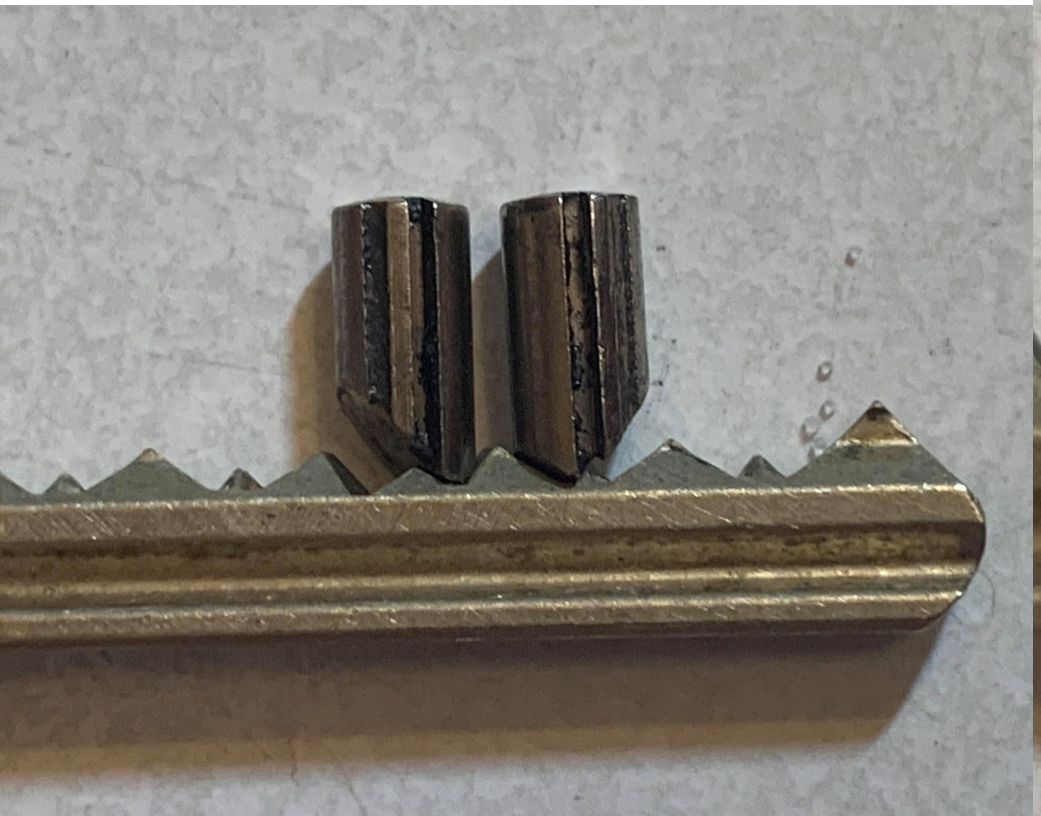

SCHLAGE
5 PIN
6 PIN
1145
SC1
1145CE
—
1145E
SC8
1145EF
—
1145F
SC7
1145FG
—
1145G
—
1145A
SC4
A1145CE
—
A1145E
SC9
A1145EF
—
A1145F
SC10
A1145FG
—
A1145G
—
1145H
—
A1145H
SC15
1145J
—
A1145J
—
1145K
—
A1145K
—
1145L
SC19
A1145L
SC20
SC1-PC
—
5 PIN
6 PIN


medeco
SIS


medeco


medeco
SECURITY LOCKS
PAT. NO. 6,477,875
medeco
SECURITY LOCKS
medeco
SECURITY LOCKS

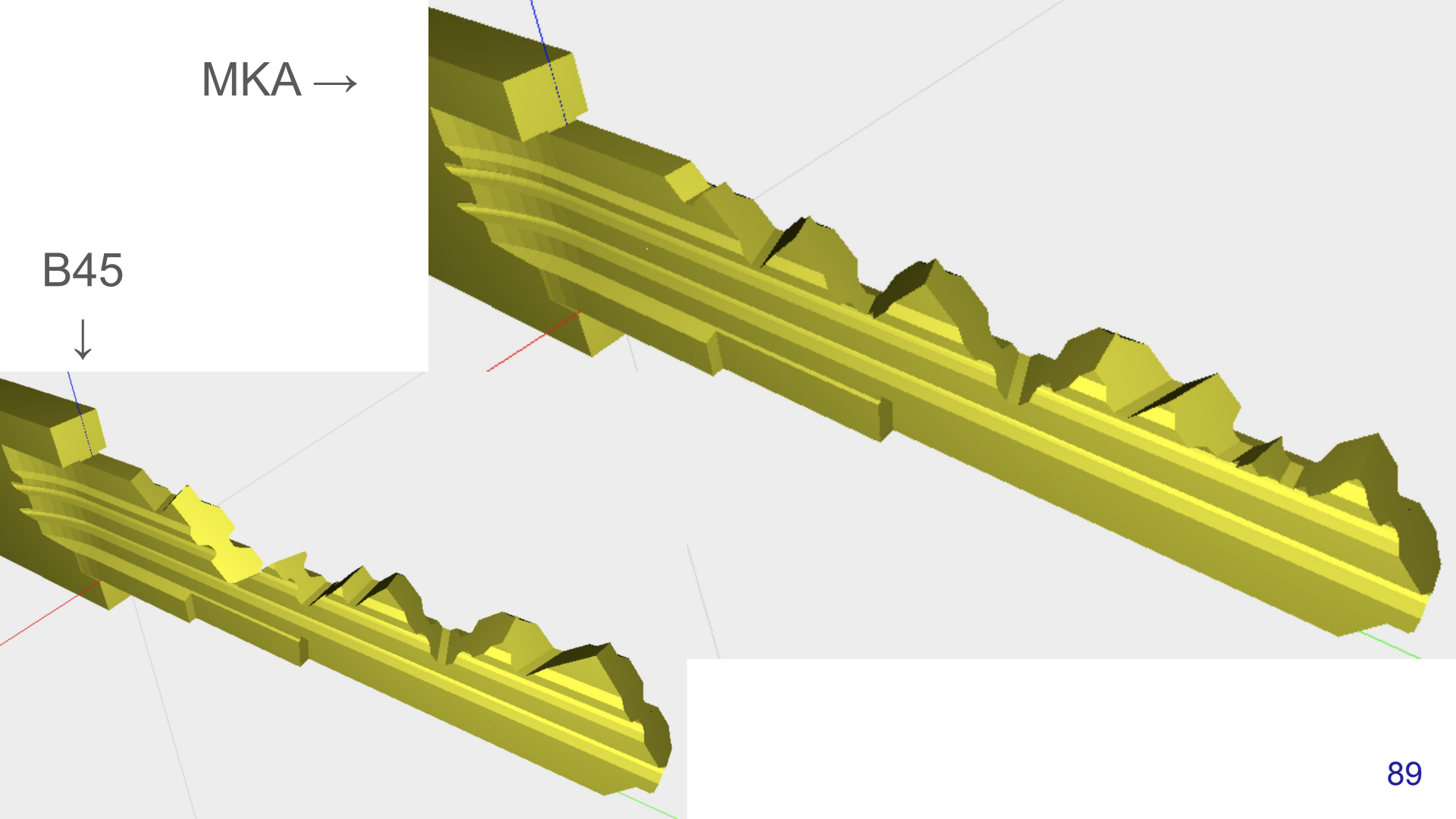
Medeco Biaxial



MKA →

B45

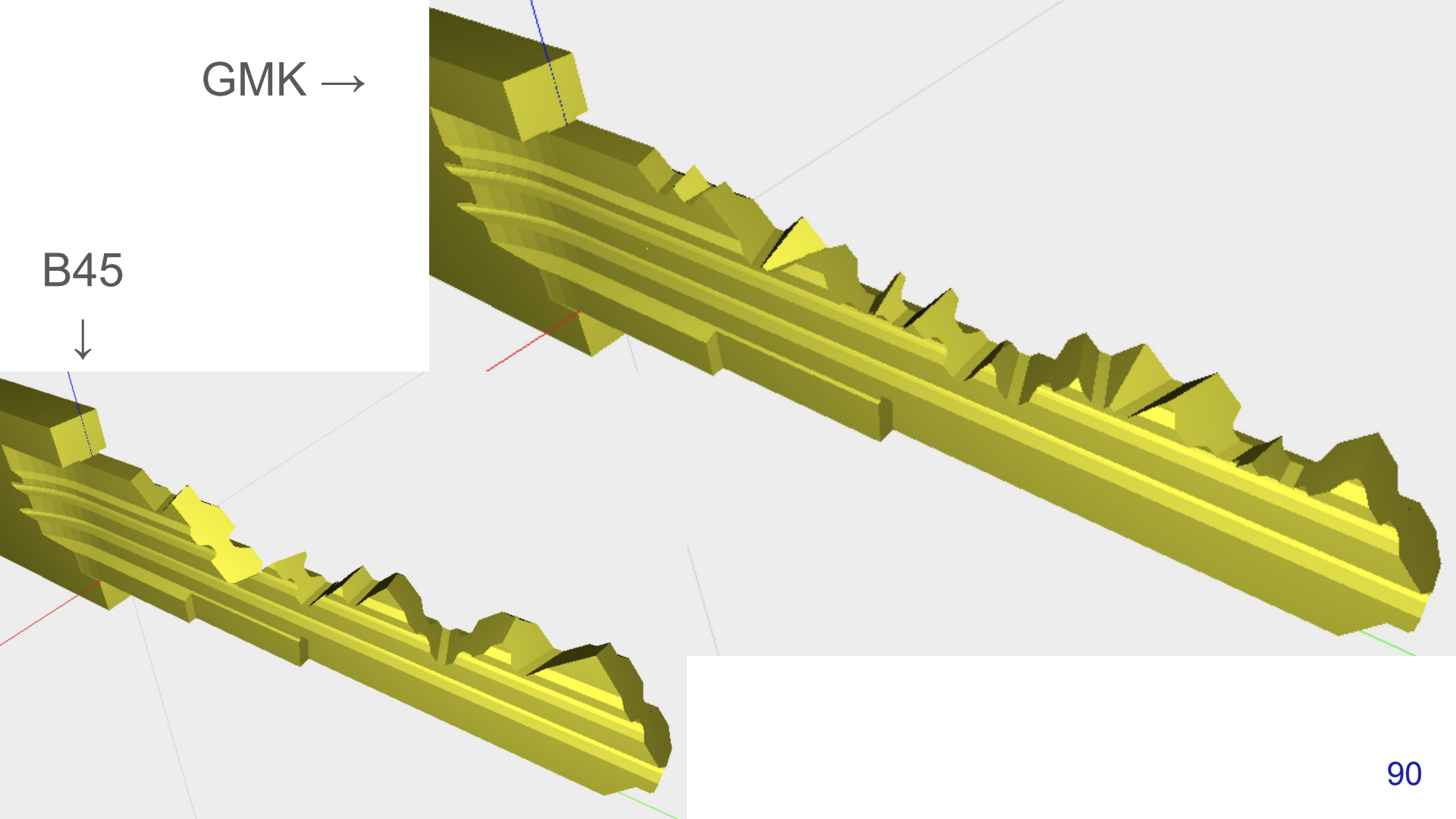
↓



GMK →

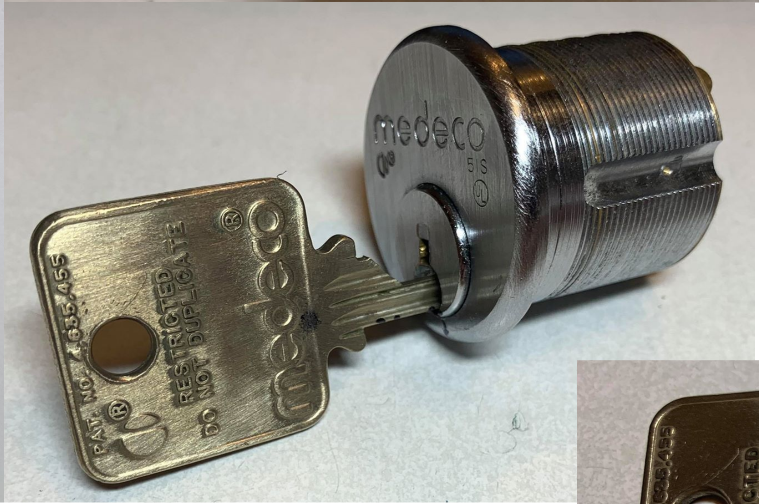
B45

↓



Nonmastered Medeco Locks

Demo →


medeco
51S
PAT. NO. 4,635,455
RESTRICTED
DO NOT DUPLICATE
medeco


PAT. NO.
RESTRICTED
DO NOT DUPLICATE
medeco


RESTRICTED
DO NOT DUPLICATE
medeco

Physical Creation of Keys

Getting a Key Cut

1. Identify the blank
2. Determine the bitting code you want
3. Go to a locksmith (not a hardware store or 7/11)
4. Ask if they can cut you a key by code
5. Give them the blank and code: e.g. “A Schlage SC1 with bitting code 0-4-2-8-5”
6. If they say “that key is restricted, I can’t cut you that”... check out our DEF CON 27 talk on Duplicating Restricted Mechanical Keys or wait a year for our (tentative) DEF CON 29 part II of that talk.

Defenses

- Avoid very large mastering systems
- Don’t master high-security and low-security facilities on one system
  - Very high risk locations should be off-master (current requirement for USA nuclear arsenals)
- A missing lock is as bad as a missing GMK!
- Consider alternatives to the 2-step system
  - Other specific defenses
  - If this is in your threat model
- Use a restricted keying system - it won’t stop a determined attacker, but it can slow them down and drive their costs up
- Your facility should be secure even if an attacker has the GMK
  - All a lock does is keep honest people honest. Add alarms, guards, etc.
- Use IC or electronic components to make rekeying easier

THE WATCHDOGS NEWS CHICAGO

Master keys for O'Hare Airport security acces were lost, costing city in 'five figures'

A set of keys that provides almost total access to O'Hare Airport were lost and never recovered. But there were rare consequences for the employee involved, a Sun-Times investigation found.

By Robert Herguth | Jun 21, 2019, 5:00am CDT

SHARE

A set of keys like these belonging to the Chicago Department of Aviation and allowing high-level security access to O'Hare Airport were lost. | Photo illustration by Ashlee Rezin & Brian Ernst / Sun-Times

It looks like something you'd borrow from the counter of a gas station to get into the

MOST READ

School cops speak out at t about kids out there that h

Cubs trade pitcher Mike M Royals for catcher Martin M

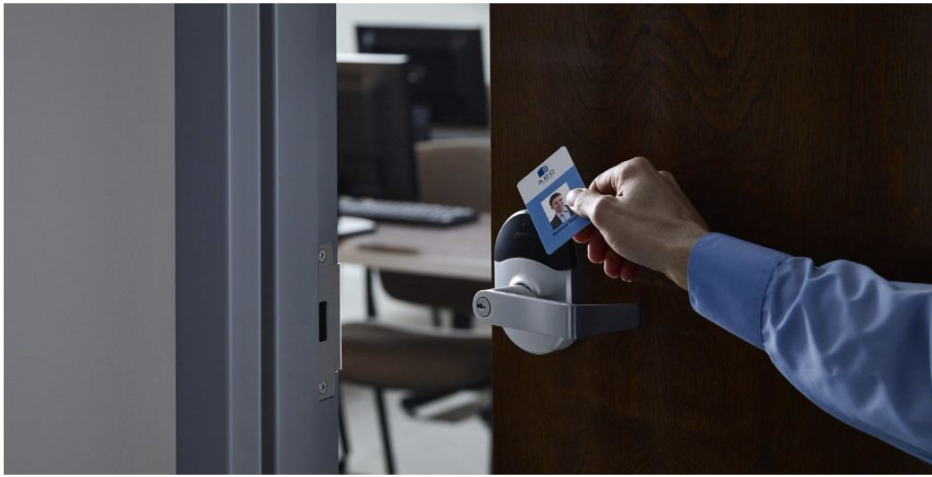
Dach, Nylander, others deb Blackhawks' development

2 men killed in South Chic police

R. Kelly divorce files show battle over money

Breaking News

Subscribe to our breaking n list



NEWS

Lost, stolen campus master keys too expensive to replace

November 27, 2018 0 view

The master keys at UCA have recently been brought into the light due to an investigation involving a lost key.

The investigation began in June after a theft was reported in Assistant Director of Financial Aid fo Scholarships Andrew Linn's office in McCastlain Hall, Jeff Pitchford, vice president of university and government relations, said.

A thief reportedly broke in and stole four pills out of Linn's office. The key used was a grand


Master Lock

Questions?

b.graydon@ggrsecurity.com
@access_ctrl

Go try it!
https://ggrsecurity.com/personal/~bgraydon/keyspace

Or: https://tinyurl.com/key-space

Source:
https://github.com/bgraydon/lockview
https://github.com/bgraydon/keyspace

A huge thank you to Josh Robichaud, Karen Ng and Jenny & Bobby Graydon for their help in preparing this talk.