Safe Manipulation aka Safe Cracking

schiaparelli

ROOTCON 17

Part 1

Understanding how a Group 2 lock works

Hollywood

i. Methods of Entry

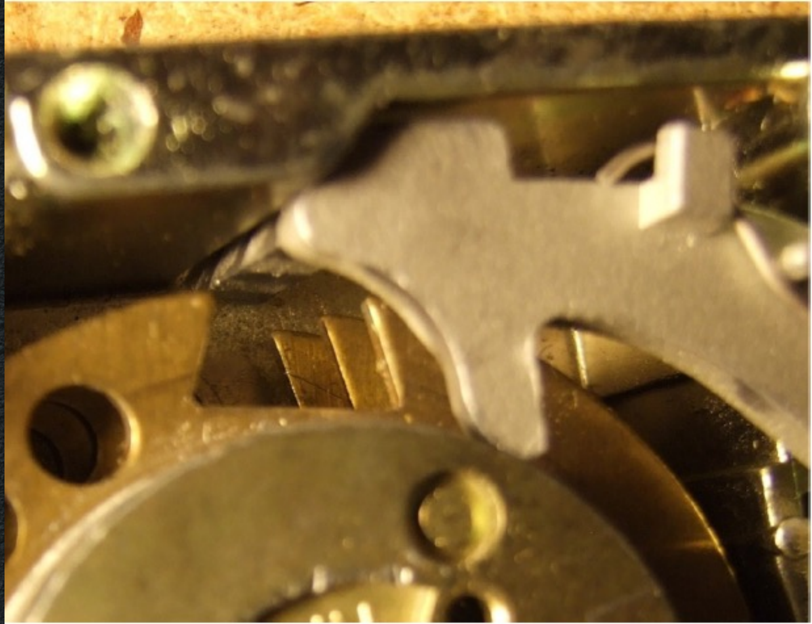
ii. How to dial in a combination?

1. L4 – R3 – L2
2. Check code
3. Turn dial

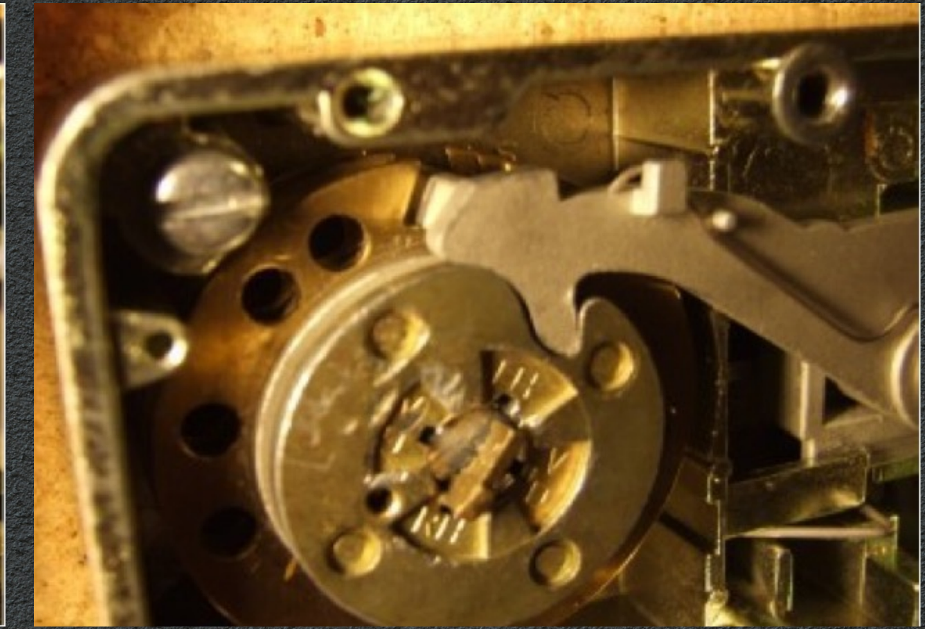
Identity Authentication

1. Code Entry
2. Verify Code
3. Grant Access

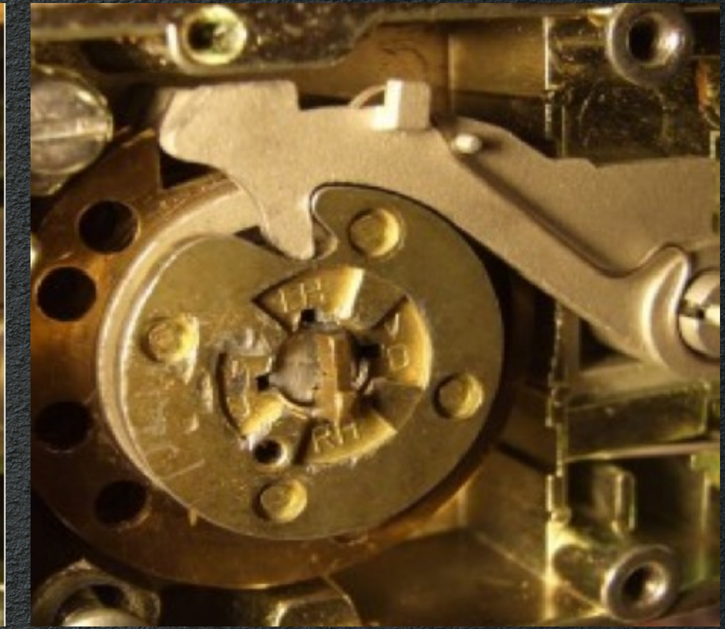
Code entry



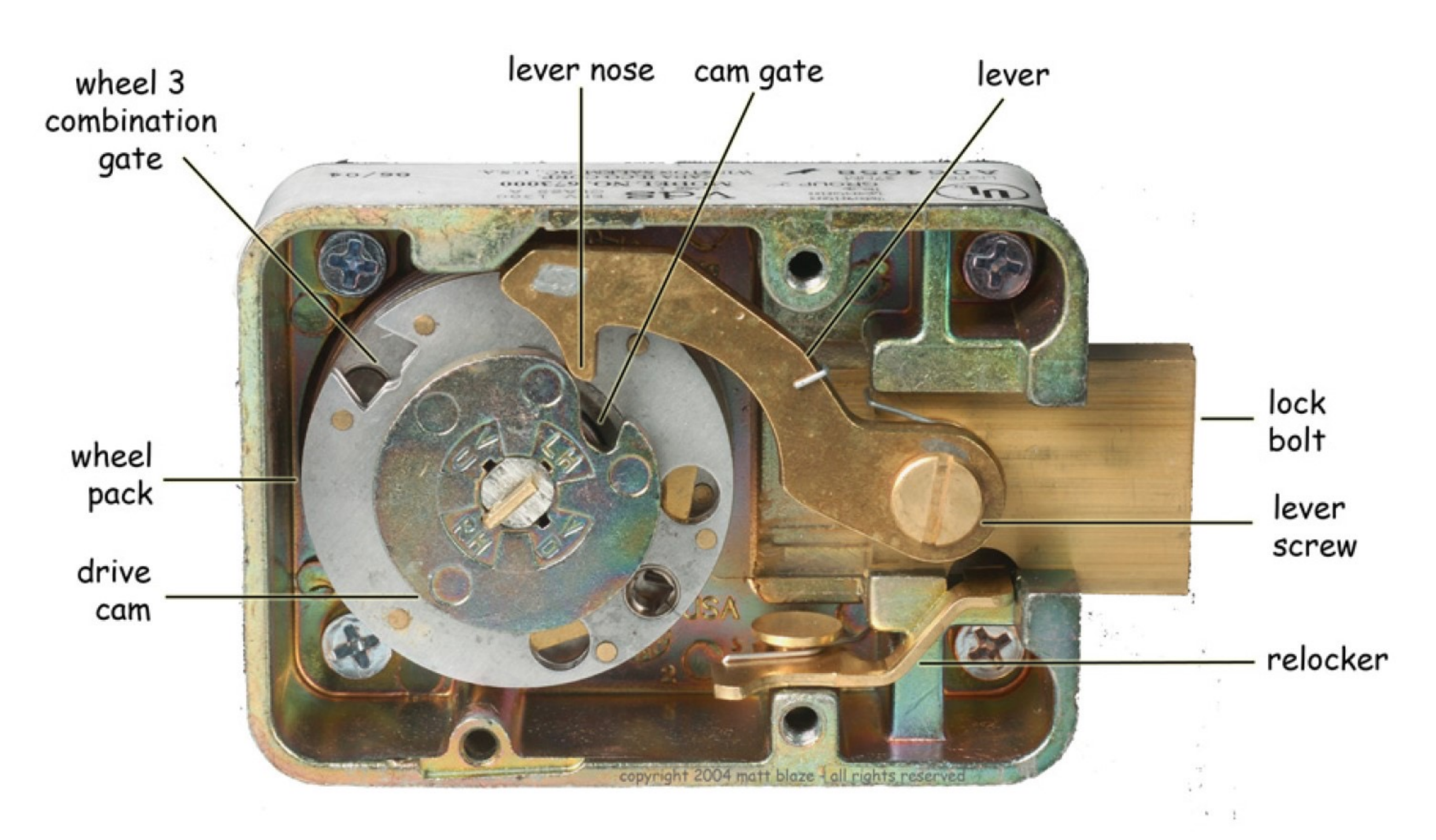
Verify Code



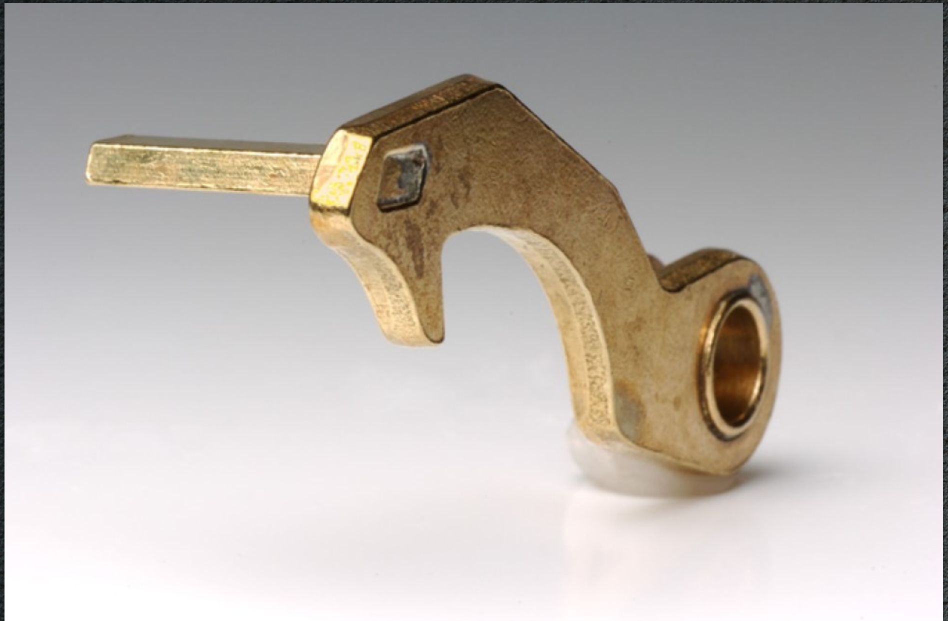
Grant Access



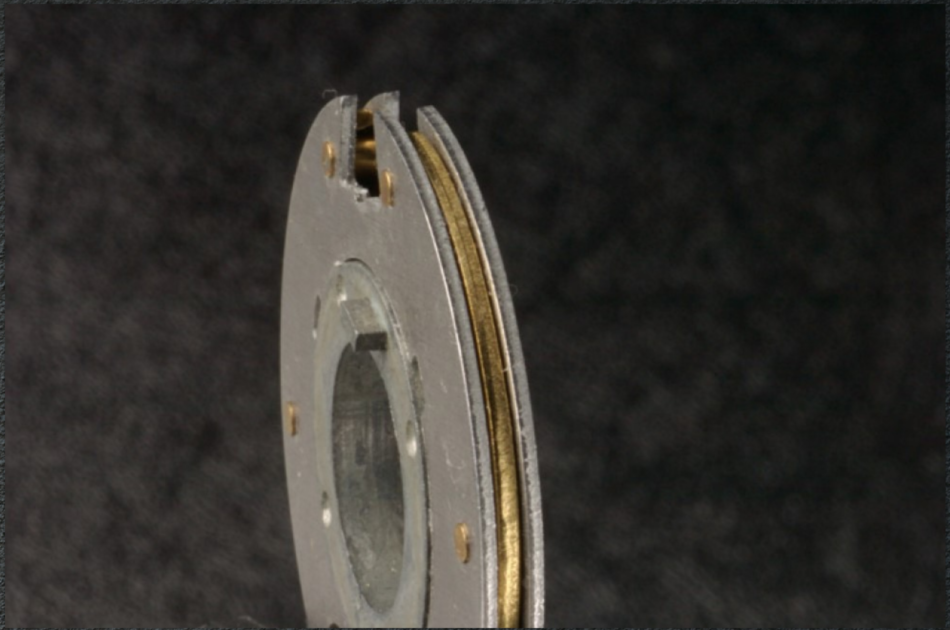
iii. Parts of a 3-wheel safe lock



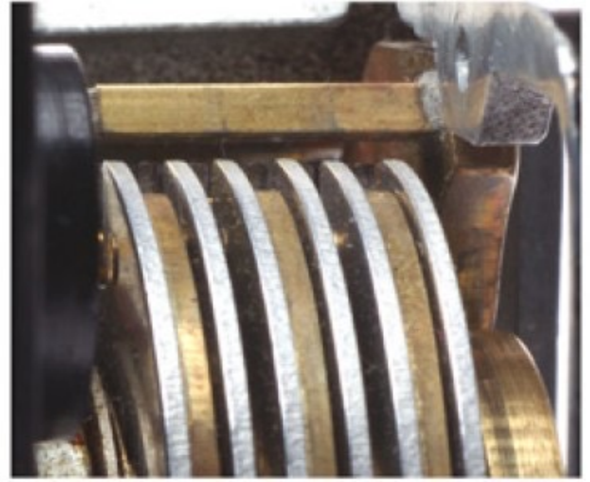
Source: Safecracking for the computer scientist, Matt Blaze



Fence / nose



Wheel



Fence and wheel

Source: Safecracking for the computer scientist, Matt Blaze

ROOTCON 17

iv. Vulnerabilities

100 x 100 x 100 ?

Keyspace = 1,000,000

+/- 0.75

67 x 67 x 67 = 300,763

+/- 1.25

40 x 40 x 40 = 64,000

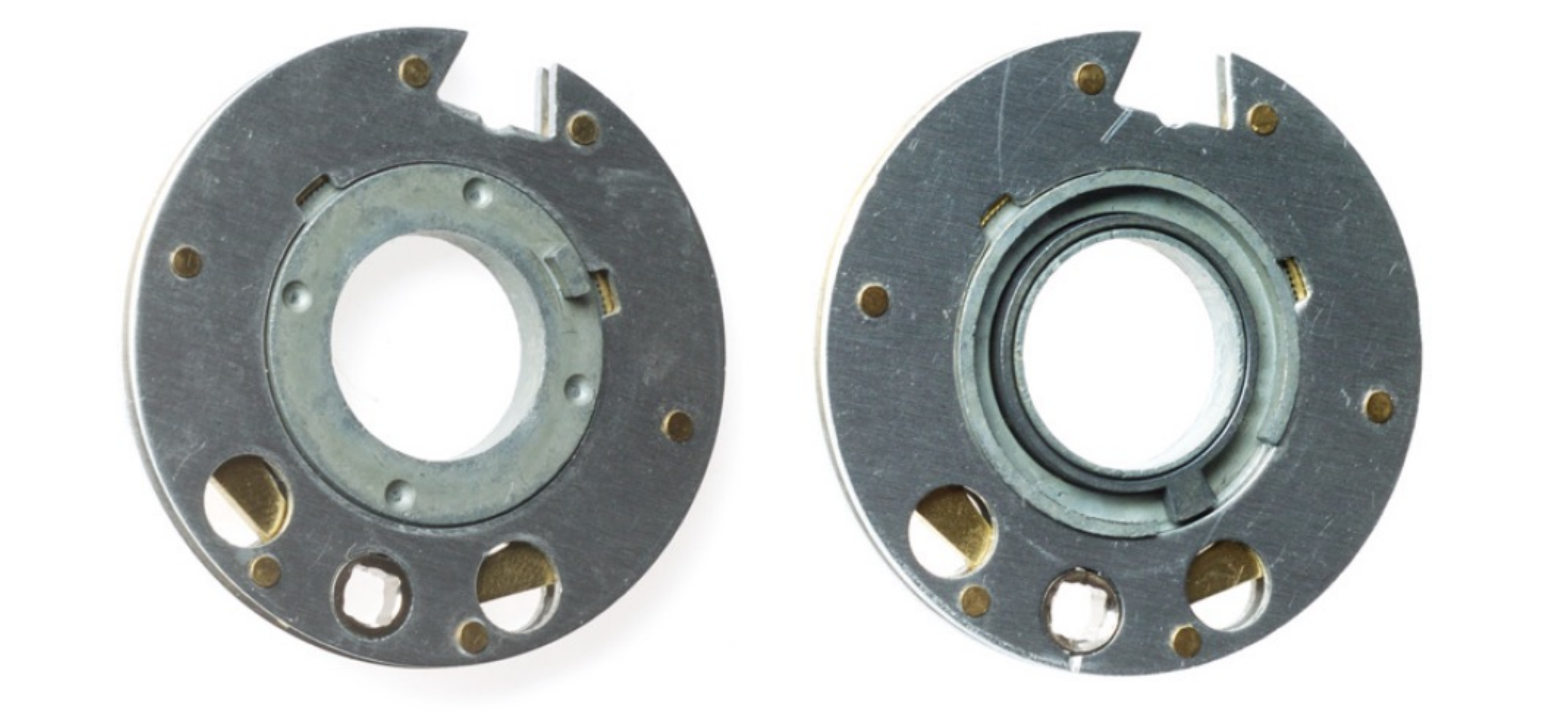
Forbidden Zone on W3

~10 numbers

242,406 combinations

51,200 combinations

ROOTCON 17

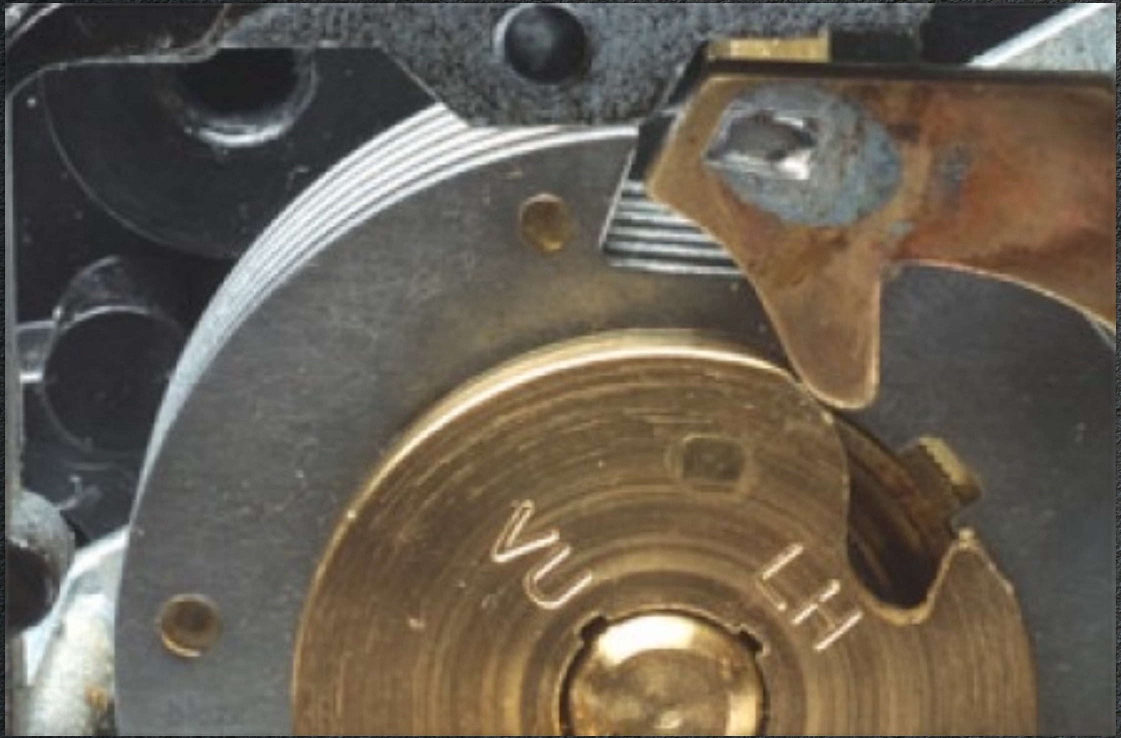


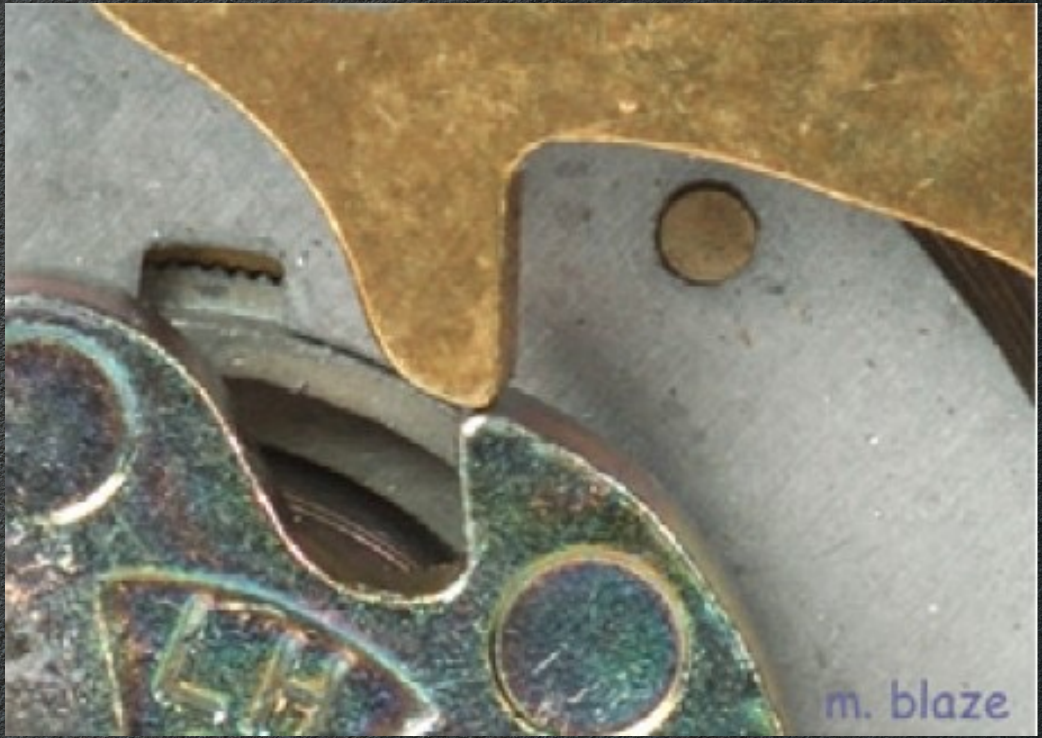
Source: Safecracking for the computer scientist, Matt Blaze

Source: Safecracking for the computer scientist, Matt Blaze

v. Exploitation

The Contact Points



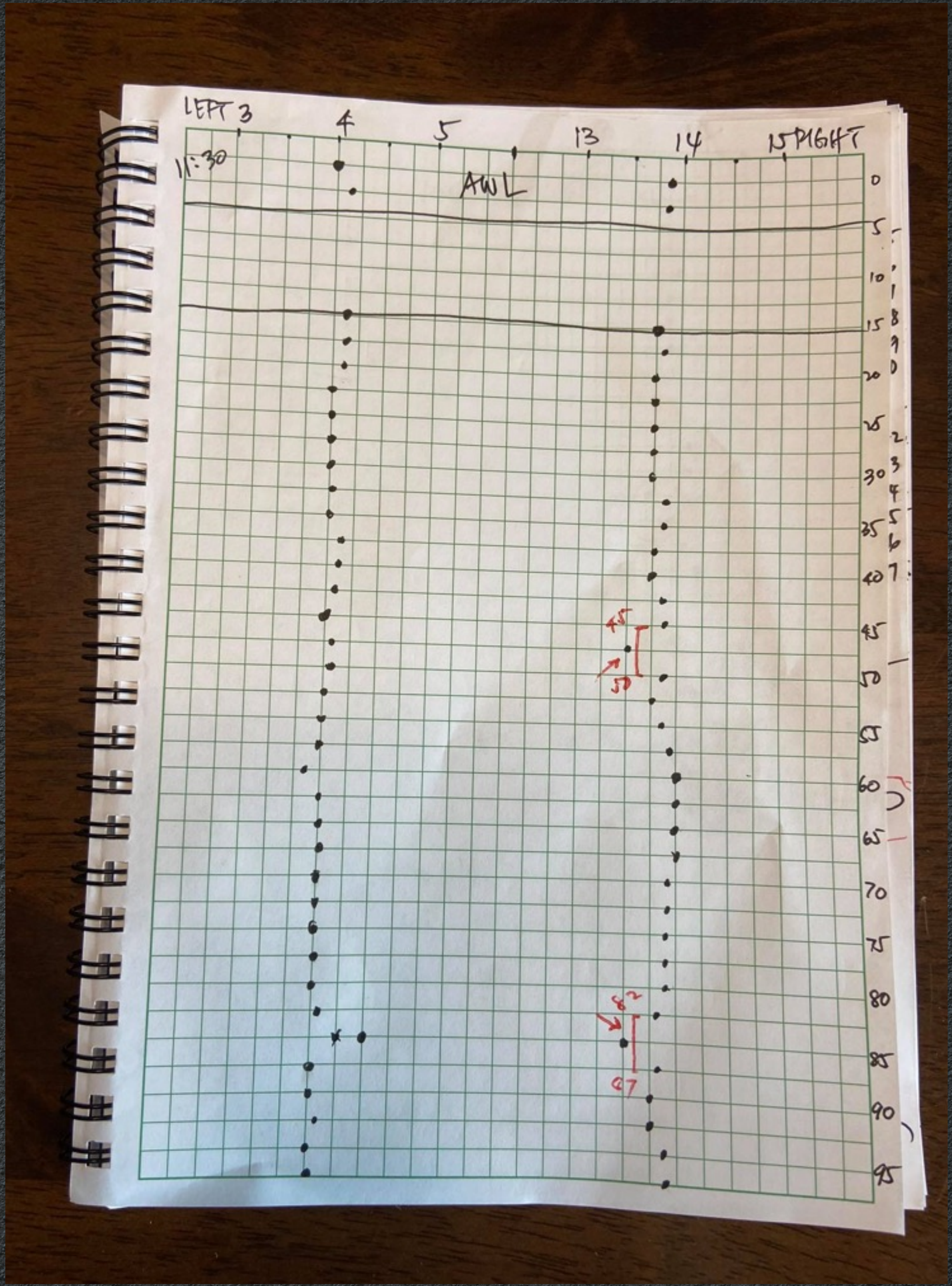


Source: Safecracking for the computer scientist, Matt Blaze

The First Algorithm

1. AWL – All Wheels Left
2. Dial to 0 / 2.5 / 5 / 7.5 / ….
3. Take Contact reading
4. Graph
5. Rinse and Repeat

Graph


LEFT 3
4
5
13
14
15 RIGHT
11:30
AWL
0
5
10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
85
90
95
45
50
82
87

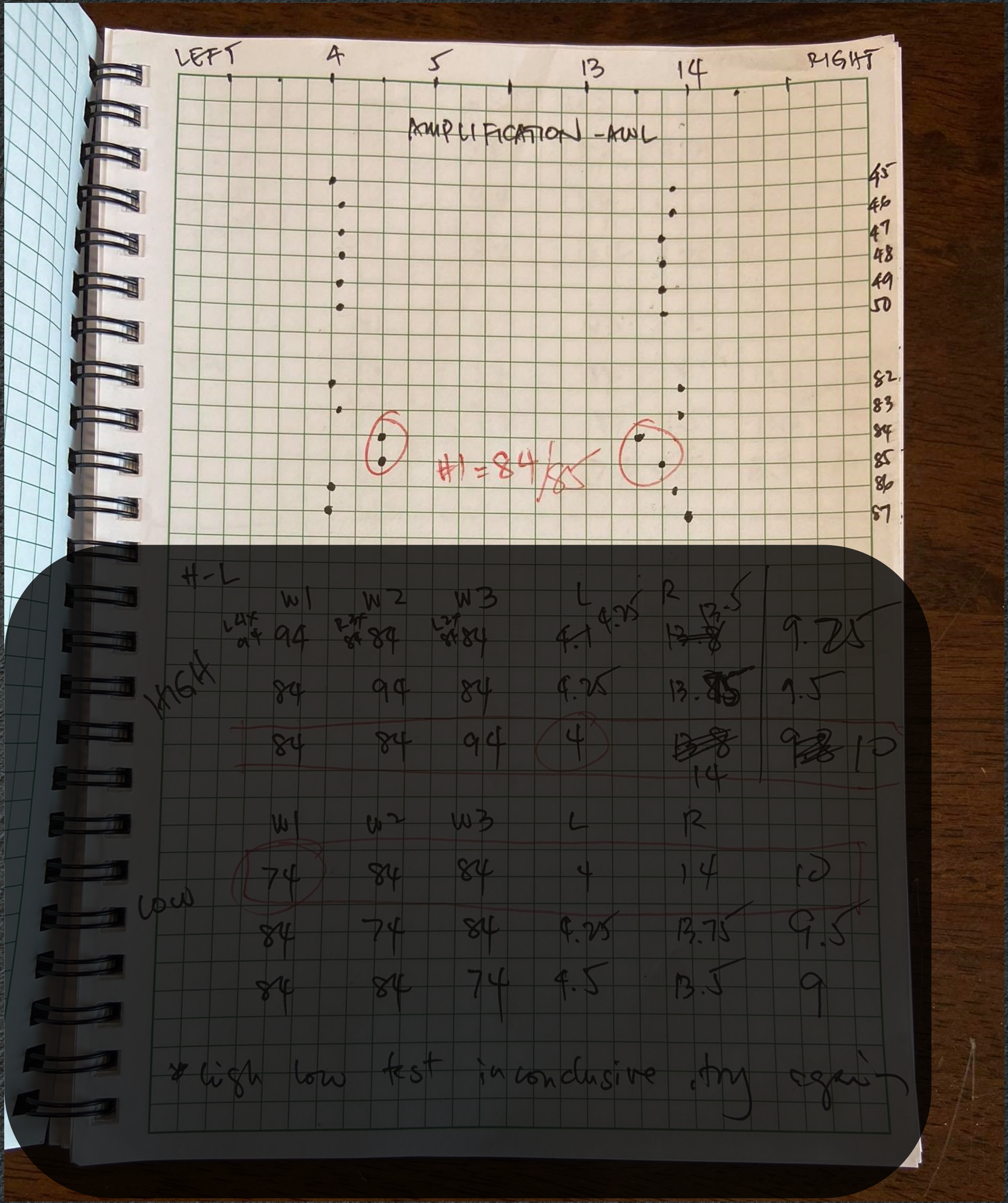
If there’s time, Part 2

The logic behind safe cracking

i. The other Algorithms

- Amplification
- High Low Test
- Graph 2nd number
- Brute Forcing the 3rd number

Amplification


LEFT
4
5
13
14
RIGHT
AMPLIFICATION -AWL
45
46
47
48
49
50
82
83
84
85
86
87
#1=84/85

H-L

	W1	W2	W3	L	R	
HIGH	L4x 94 94	R3x 84 84	L2x 84 84	~~4.1~~ 4.25	~~13.8~~ 13.5	9.25
	84	94	84	4.25	13.85	9.5
	84	84	94	4	~~13.8~~ 14	~~9.8~~ 10
	W1	W2	W3	L	R	
LOW	74	84	84	4	14	10
	84	74	84	4.25	13.75	9.5
	84	84	74	4.5	13.5	9

* high low test inconclusive .try again

High Low Test

*AWL indicate at 84

W1	W2	W3	Left Contact	Right Contact	Right - Left
94	84	84	79	91.5	12.5
84	94	84	79.75	91.25	11.5
84	84	94	79.25	91.5	12.25

Test indicate W1 @84

Graphing the 2nd Number

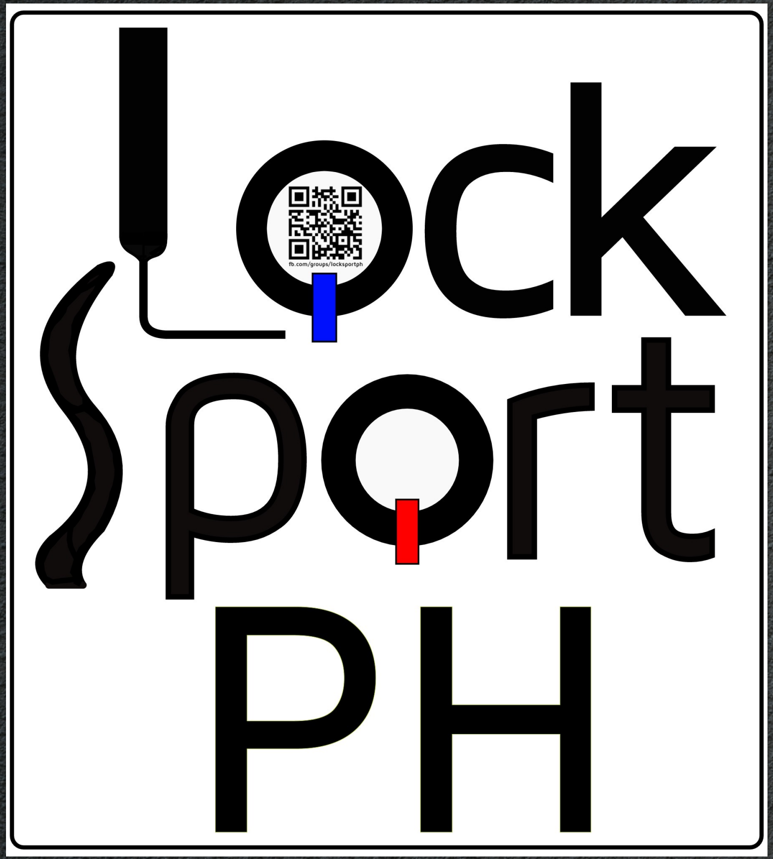
- Depends on which wheel indicated first.
- To be discussed in the village…

ii. Other Exploits

- Radiographic (X-Ray)
- Drilling (Destructive) + Borescope
- Robot Autodialer
- Explosives (Destructive)
- Thermic Lance (Destructive)

iii. Remediation

- Group 1 locks
- Group 2M locks
- Delrin Wheels
- Kaba-Mas X-10


Lock
Sport
PH
fb.com/groups/locksportph