

Proxmark3 Cheat Sheet

This cheat sheet contains many useful commands to help you get started with Proxmark3.

Big thanks to Alex Dib, Philippe Teuwen and Iceman over on the RfidResearchGroup GitHub for their cheat sheet!

iClass

Reverse hf iclass permute r
Permute 3F90EBF0910F7B6F
Master
Key

Simulate hf iclass reader
Reader

Dump hf iclass dump k
AFA785A7DAB33378

Read hf iclass readblk b 7 k
Block AFA785A7DAB33378

Write to hf iclass writeblk b 07
Block d 6ce099fe7e614fd0 k
AFA785A7DAB33378

Print hf iclass managekeys p
Keystore

Add Key hf iclass managekeys n
to 0 k AFA785A7DAB33378
Keystore
[0-7]

Encrypt hf iclass encryptblk
Block 0000000f2aa3dba8

Load hf iclass eload f
Dump iclass_tagdump-filename.bin

iClass (cont)

Simulate hf iclass sim 3

Simulation notes:

0 <CSN> simulate the given CSN

1 simulate default CSN

3 Full simulation using emulator memory

Simulate iClass Sequence

```
pm3 > hf iclass dump k AFA785-  
A7DAB33378
```

```
pm3 > hf iclass eload f iclass-  
_tagdump-db883702f8ff12e0.bin
```

```
pm3 > hf iclass sim 3
```

Clone iClass Legacy Sequence

```
pm3 > hf iclass readblk b 7 k  
AFA785A7DAB33378
```

```
pm3 > hf iclass writeblk b 07 d  
6ce099fe7e614fd0 k AFA785A7DAB3-  
3378
```

iClass lclass attack

Extract custom iClass key (lclass attack)

```
pm3 > hf iclass sim 2
```

```
pm3 > hf iclass lclass f  
iclass_mac_attack.bin
```

```
pm3 > hf iclass dump k <Kcus> e
```

Verify custom iClass key

```
pm3 > hf iclass lookup u 010a0f-  
fff7ff12e0 p fefffffffffffffff m  
66348979153c41b9 f default_icla-  
ss_keys.dic e
```

Generic Commands

High Frequency Search hf
search

Low Frequency Search lf
search

Measure Antenna Character- hw tune
istics

Check Version hw
version

Generic Commands (cont)

Check overall status hw status

Mifare

Check for hf mf chk *1 ? d

Default default_keys.dic
Keys

Dump hf mf dump 1

(0=Mini,
1=1k, 2=2k,
4=4k)

Write to hf mf wrbl 0 A

Block FFFFFFFFFF d3a285-
9f6b880400c8010020-
00000016

Hardnested hf mf hardnested 0 A
Attack FFFFFFFFFF 0 A w

Load Dump hf mf eload 353C2AA6

Simulate hf mf sim u 353c2aa6

Run hf mf autopwn
autopwn

Simulate Mifare Sequence

```
pm3 > hf mf chk *1 ? d defaul-  
t_keys.dic
```

```
pm3 > hf mf dump 1
```

```
pm3 > script run dumptoemul -i  
dump.bin
```

```
pm3 > hf mf eload 353C2AA6
```

```
pm3 > hf mf sim u 353c2aa6
```

Clone Mifare 1K Sequence

```
pm3 > hf mf chk *1 ? d defaul-  
t_keys.dic
```

```
pm3 > hf mf dump
```

```
pm3 > hf mf restore 1 u 4A6CE843  
k hf-mf-A29558E4-key.bin f hf-  
mf-A29558E4-data.bin
```



By **Lewys Martin**
(CountParadox)

cheatography.com/countparadox/
leweys.eu

Published 15th August, 2019.

Last updated 30th September, 2019.

Page 1 of 2.

Sponsored by **CrosswordCheats.com**

Learn to solve cryptic crosswords!

<http://crosswordcheats.com>

Indala

Read	1f indala read
Demodulate	1f indala demod
Simulate	1f indala sim a00000-00c2c436c1
Clone to T55x7	1f indala clone a0000000c2c436c1

Lua Scripts

List Scripts	script list
Convert .bin to .eml	script run dumptoemul -i filename.bin
Format Mifare card	script run formatMifare -k FFFFFFFFFF -n FFFFFFFFFF -x
Options	---
k <key>	: the current six byte key
n <key>	: the new key
a <access>	: the new access bytes
x	: execute the commands

HID Prox

Read	1f hid read
Demodulate	1f hid demod
Simulate	1f hid sim 200670-012d
Clone to T5577	1f hid clone 200670-012d

HID Prox (cont)

Convert Site & Facility code to Wiegand	1f hid wiegand 0 56 150
---	-------------------------

Brute force HID reader

Options	---
a <format>	: 26 33 34 35 37 40 -44 84"
f <FC>	: 8-bit value, facility code"
c <CN>	: (optional) Starting Number, max 65535"
d <delay>	: delay in ms. Default 1000ms"
v	: verbose logging, show all tries"
---	---
pm3 >	1f hid brute a 26 f 224
pm3 >	1f hid brute v a 26 f 21 c 200 d 2000

Raw Data

Get samples	data samples <size>
Save samples	data save <filename>
Load samples	data load <filename>
raw samples	[512-40000]

Hitag

Read Hitag information	1f hitag info
Act as Hitag reader	1f hitag 26
Sniff Hitag traffic	1f hitag sniff
Simulate	1f hitag sim c378181c_a8f7.ht2

Hitag (cont)

Write to Block	1f hitag writer 24 499602D2 1 00000000
Simulate Hitag2 sequence	pm3 > 1f hitag reader 21 56713368 pm3 > 1f hitag sim c378181c_a8f-7.ht2

T55XX

Detect T55XX	1f t55xx detect
Demodulation Config	1f t55xx config FSK
Write to Block	1f t55xx wr b 0 d 00081040
Factory Reset Tag	1f t55xx wipe

Modulation Types

<FSK FSK1 FSK1a FSK2 FSK2a ASK PSK1 PSK2 NRZ BI BIa>	EM is ASK
HID Prox is FSK	Indala is PSK



By **Lewys Martin**
(CountParadox)

cheatography.com/countparadox/lewyns.eu

Published 15th August, 2019.
Last updated 30th September, 2019.
Page 2 of 2.

Sponsored by **CrosswordCheats.com**
Learn to solve cryptic crosswords!
<http://crosswordcheats.com>