物联网安全课程实验报告

**实验五**

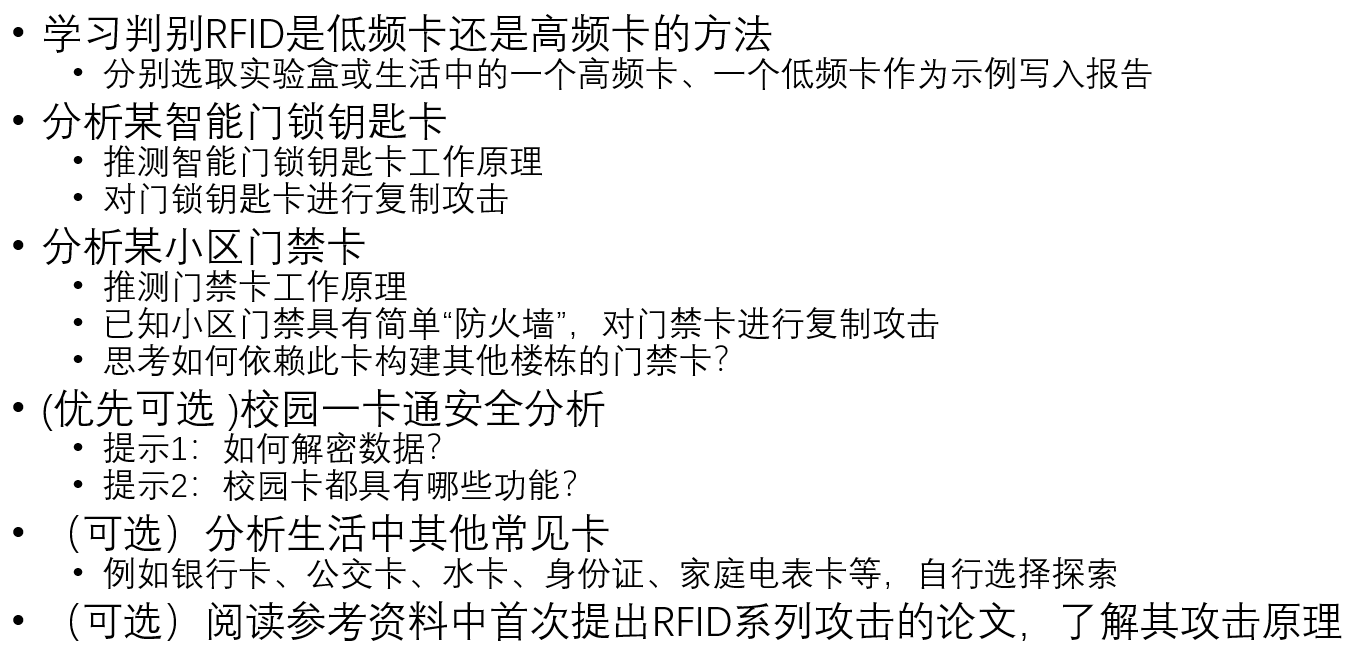


|  |  |  |
| --- | --- | --- |
| **实验名称** | ： | RFID安全实验 |
| **姓名** | ： | 辛杰 |
| **小组** | ： | 田博仁-王梓骁-辛杰 |
| **学号** | ： | 2213034 |
| **专业** | ： | 物联网工程 |
| **提交日期** | ： | 2024年12月13日 |

## 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



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：

#### 学习判别RFID是低频卡还是高频卡的方法

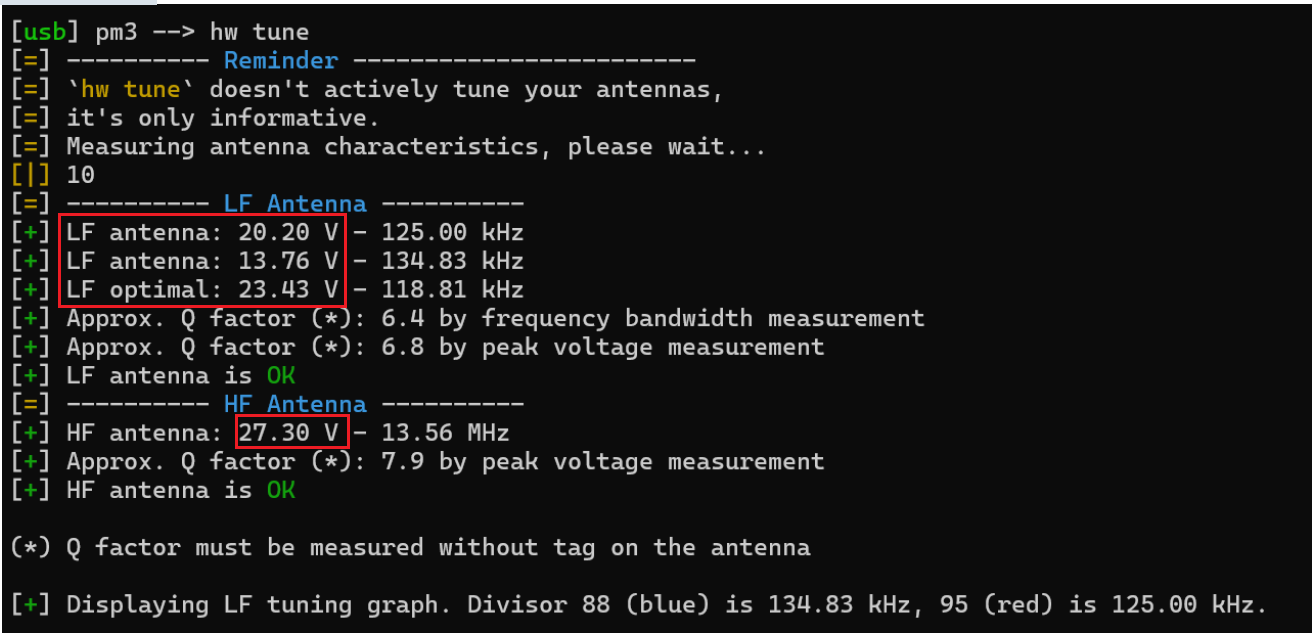
#### 对门锁钥匙卡进行复制攻击

#### 对门禁卡进行复制攻击

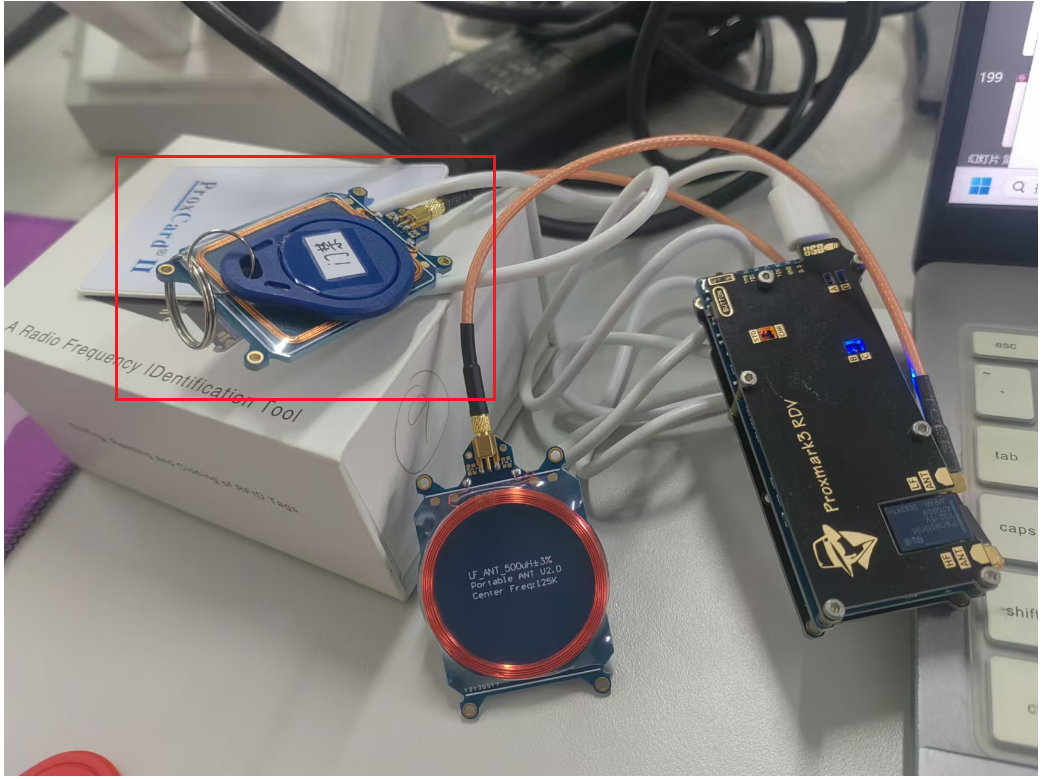
#### 实验步骤：

##### 判断RFID是低频卡还是高频卡

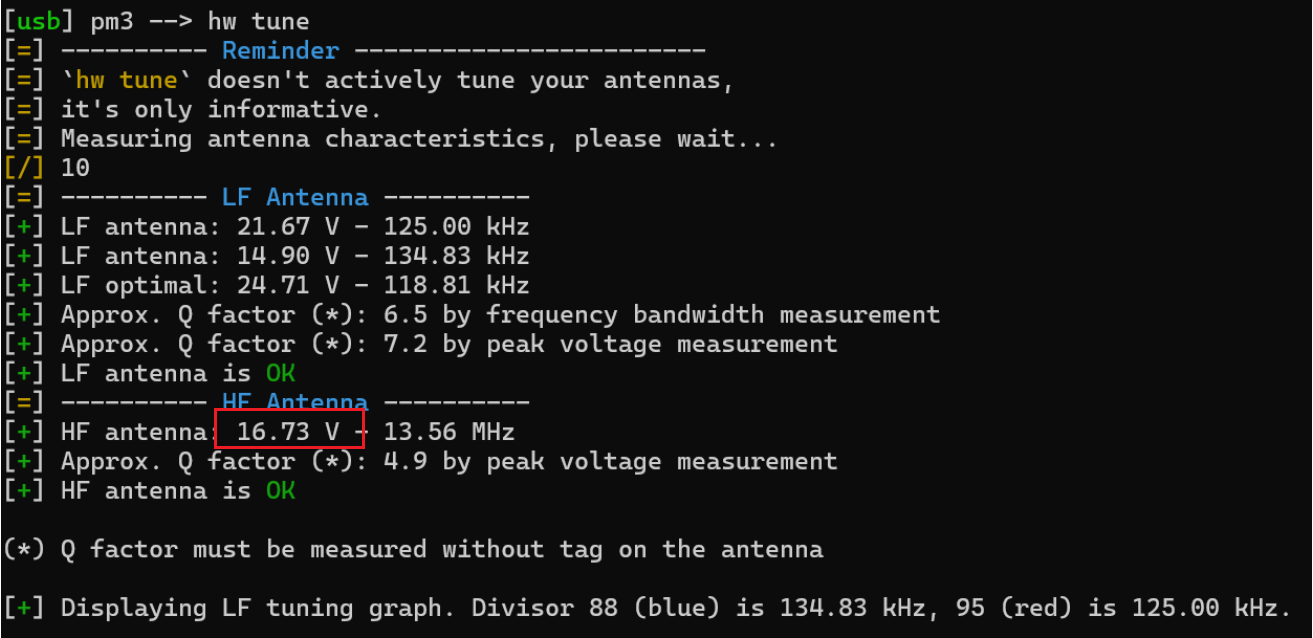
空置状态运行hw tune命令测量电压，可以看到高频和低频初始的电压



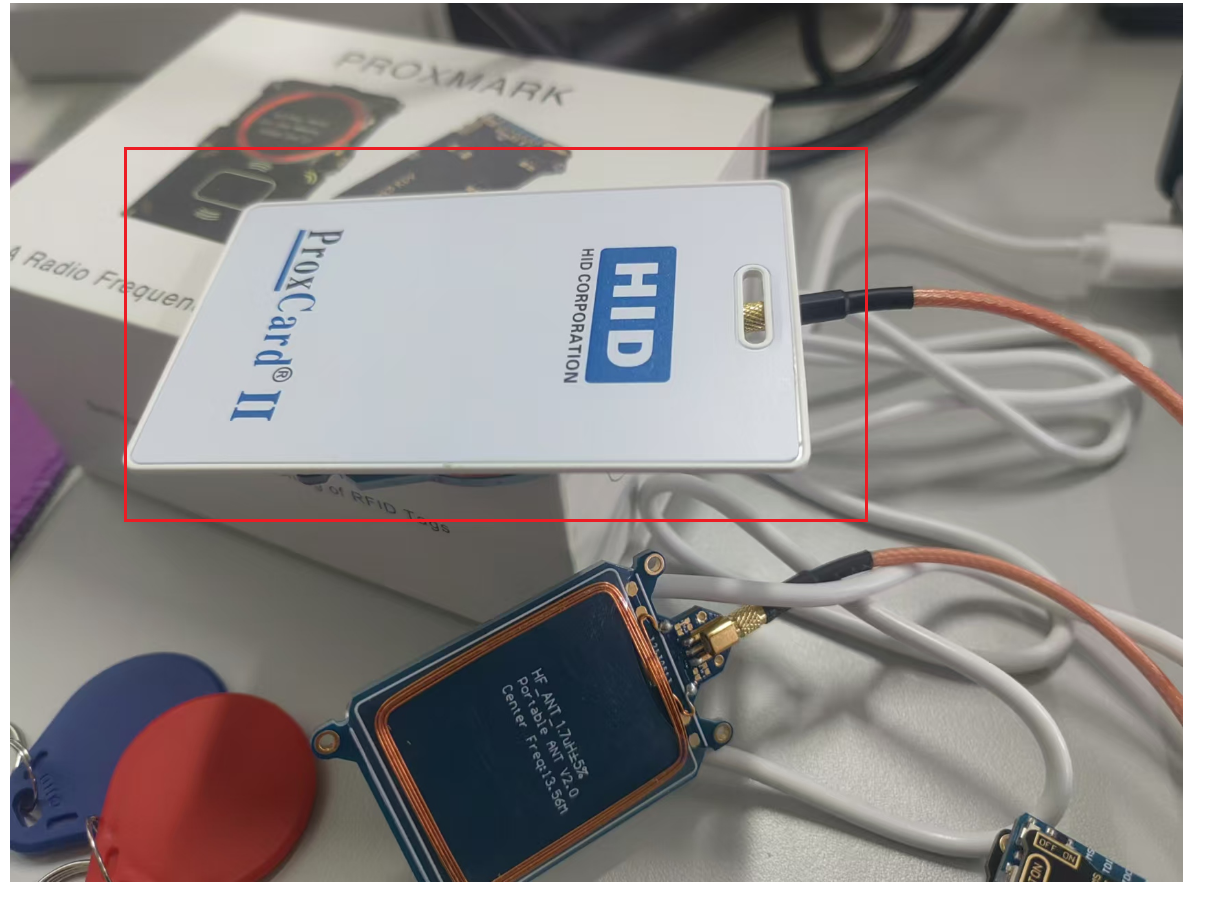
放置一张在高频线圈放置一张高频卡（提前不知道）

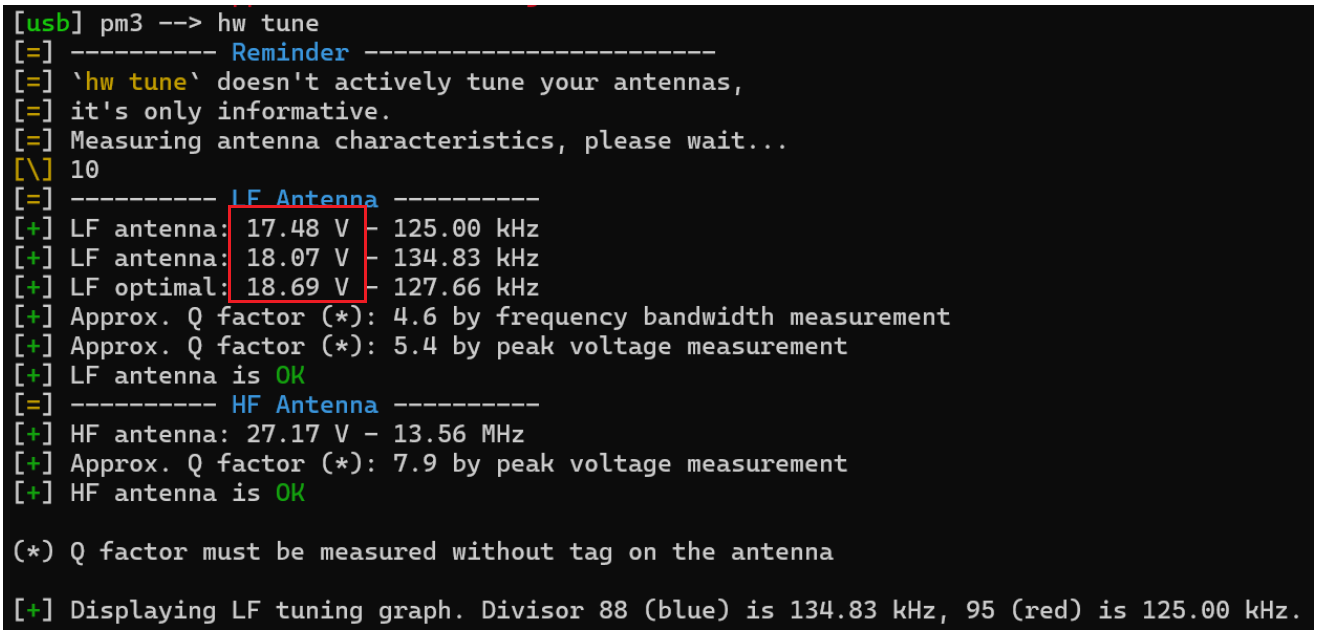


再次测量电压，高频电压明显下降，这是由于互感的原因，所以可以判断它是高频卡



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

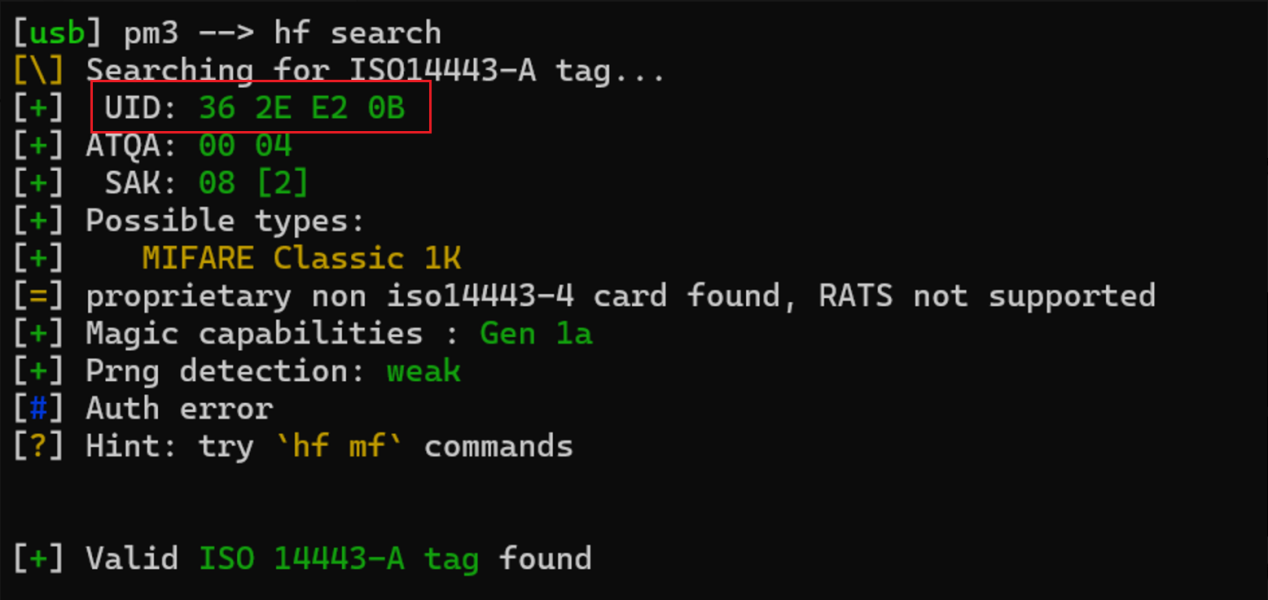




##### 对门锁进行复制攻击

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



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**



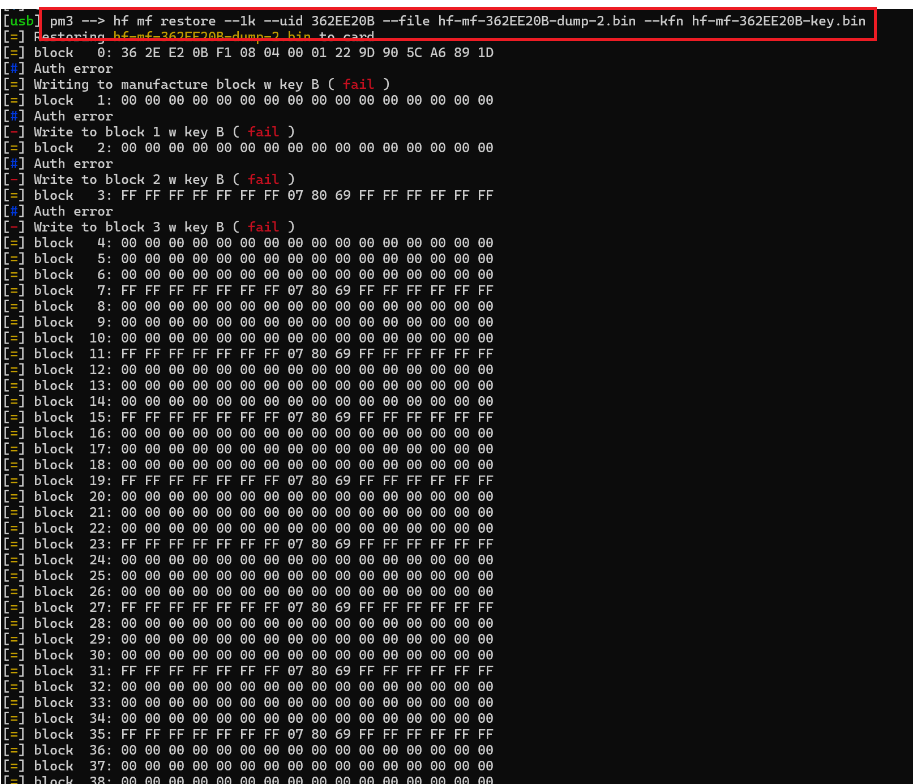
之后进行读卡操作，在读卡之前要通过以下指令删除被写入卡的原数据

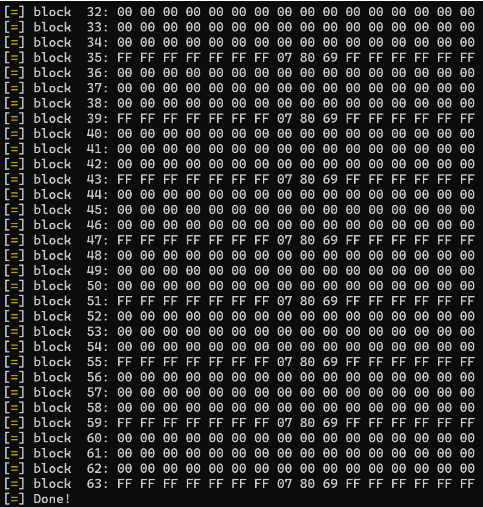
**hf mf autopwn**

**hf mf wipe**

用以下命令进行读卡

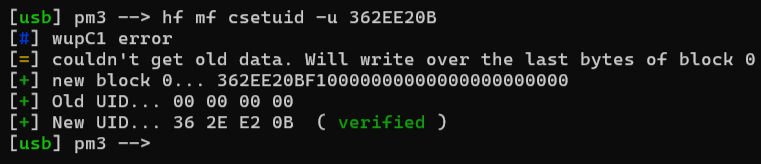
**hf mf restore --1k --uid 362EE20B --file hf-mf-362EE20B-dump-2.bin --kfn hf-mf-362EE20B-key.bin**





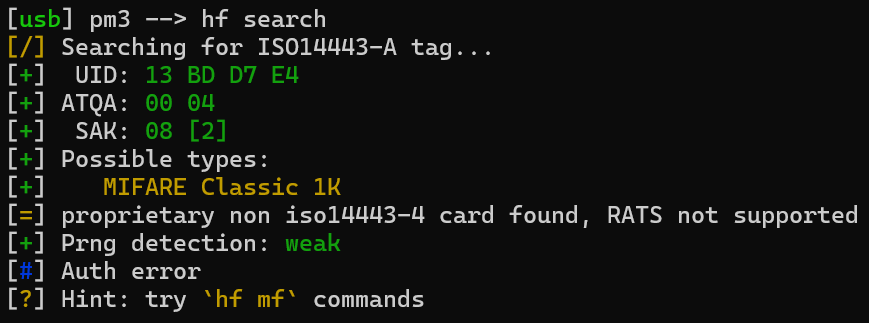
因为红卡是UID卡，不能用restore写UID，用csetuid重写0扇区

**hf mf csetuid -u 362EE20B**



##### 对门禁卡进行复制攻击

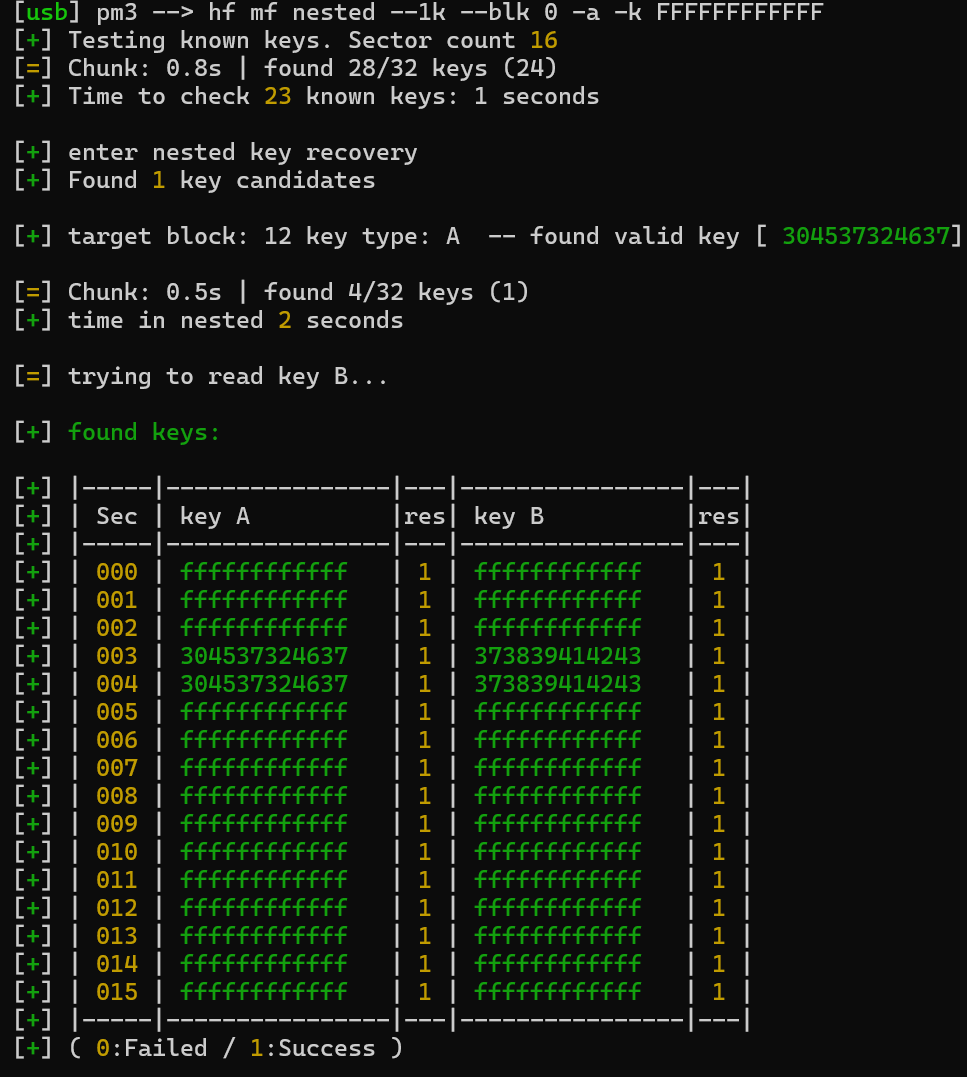
也是进行相同的操作读卡，知道UID为13BDD7E4



然后初始密码尝试，发现3、4扇区密码不是FFFFFFFFFFFF



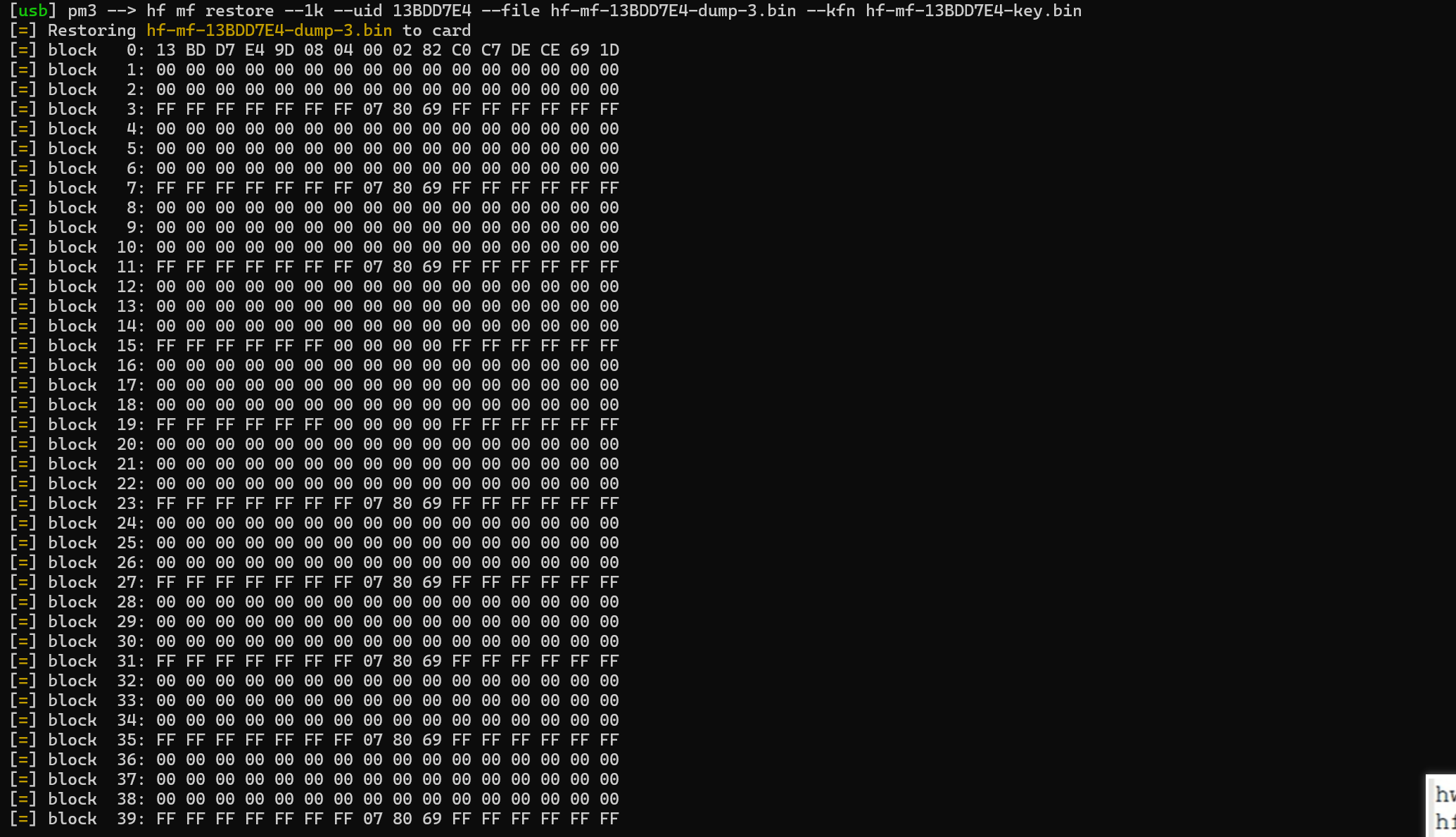
通过嵌套读取，根据扇区0的内容破解3、4扇区密码

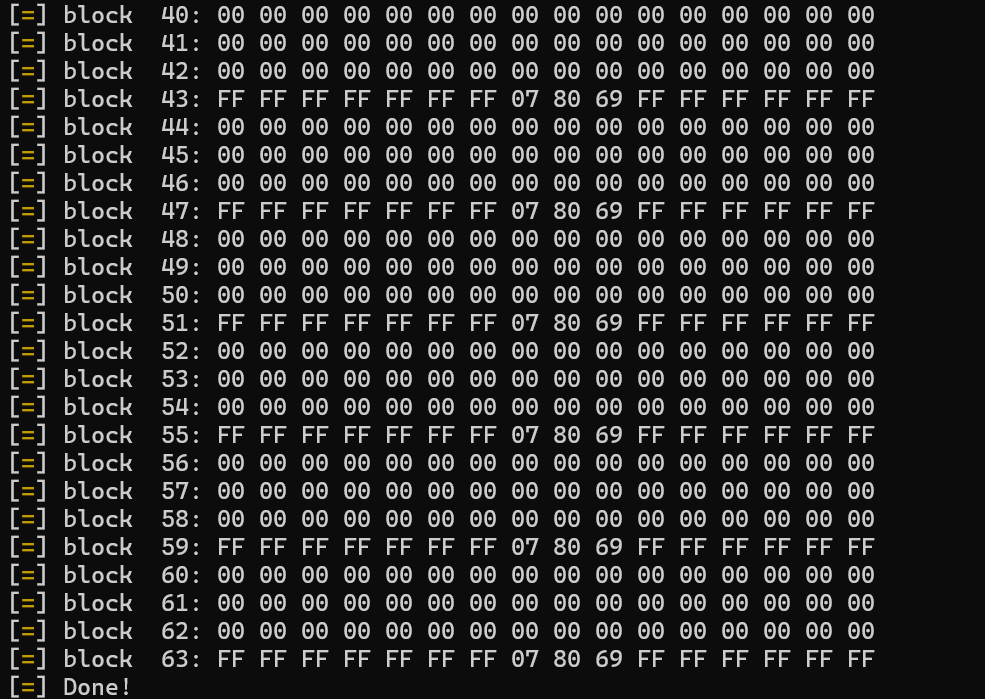


然后将数据保存起来

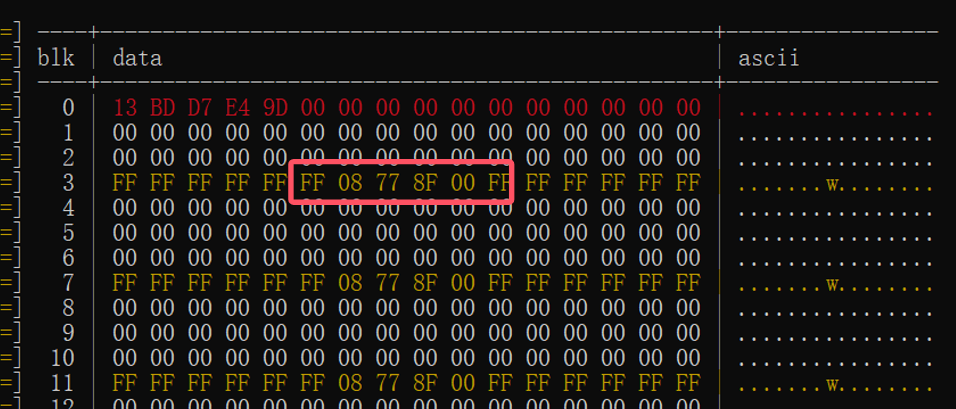
利用dump指令同门锁

然后写入数据





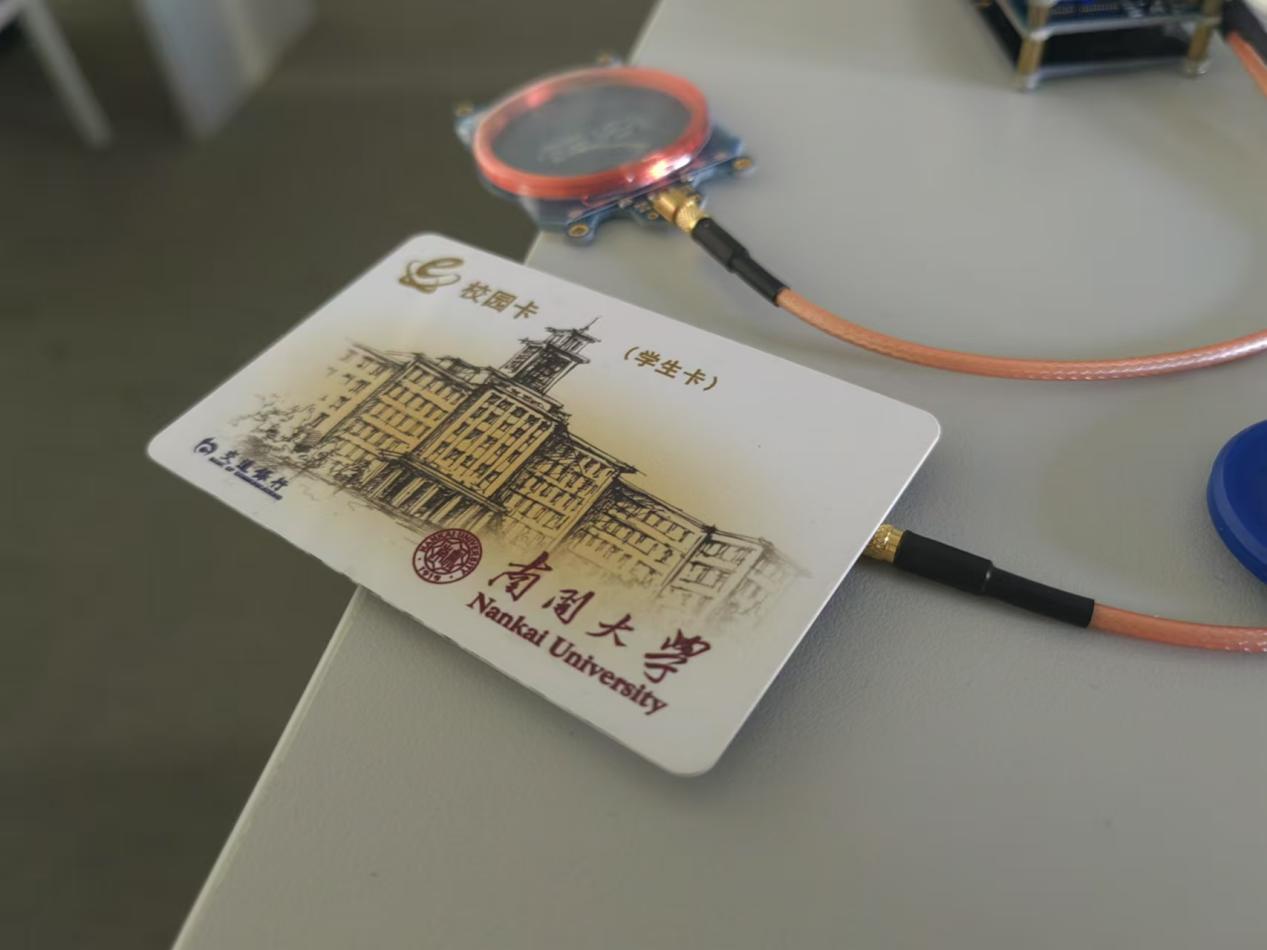
**猜测原理：**

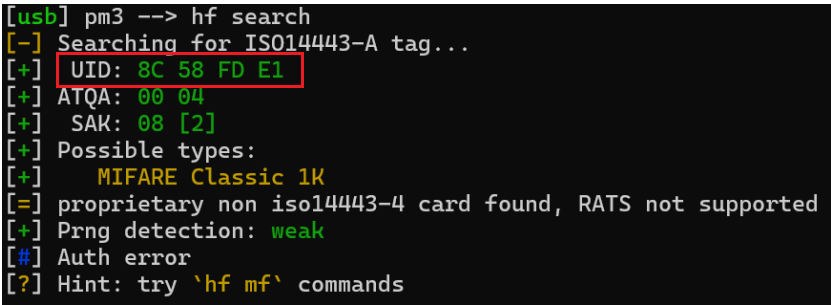


可能是每个门卫都有一个对应的号码，前面红色的是UID，可能要先对门号（楼号）进行检验，然后再检验UID。如果门禁系统仅使用 UID 验证（低安全性），可以通过修改 Magic卡的 UID 来伪造其他楼栋的门禁卡。如果门禁系统依赖卡片内部的数据，需要通过修改特定扇区的数据伪造其他楼栋的卡片。

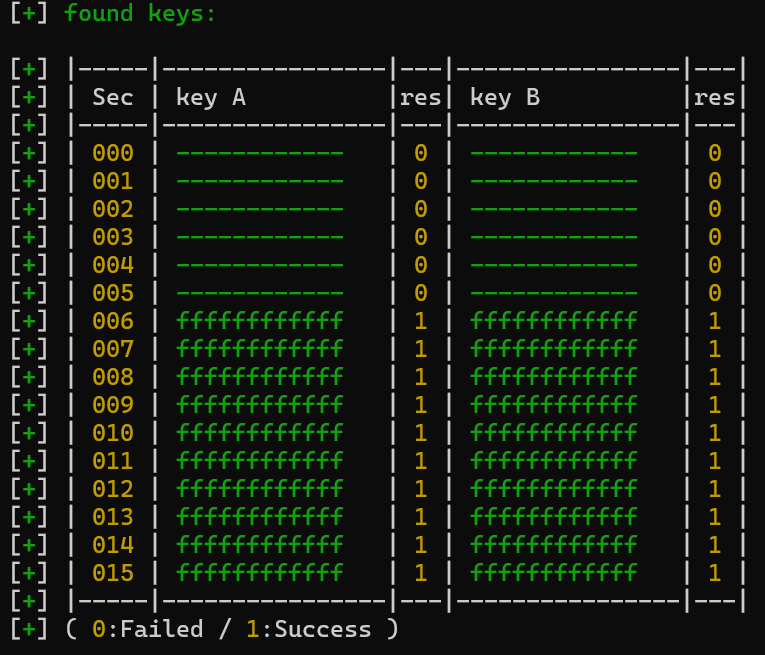
##### 4、对校园卡进行分析

先通过hf search了解其大概内容

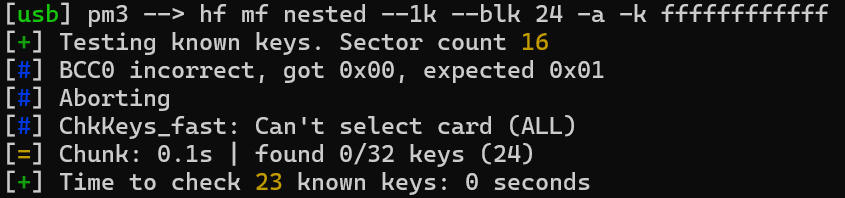




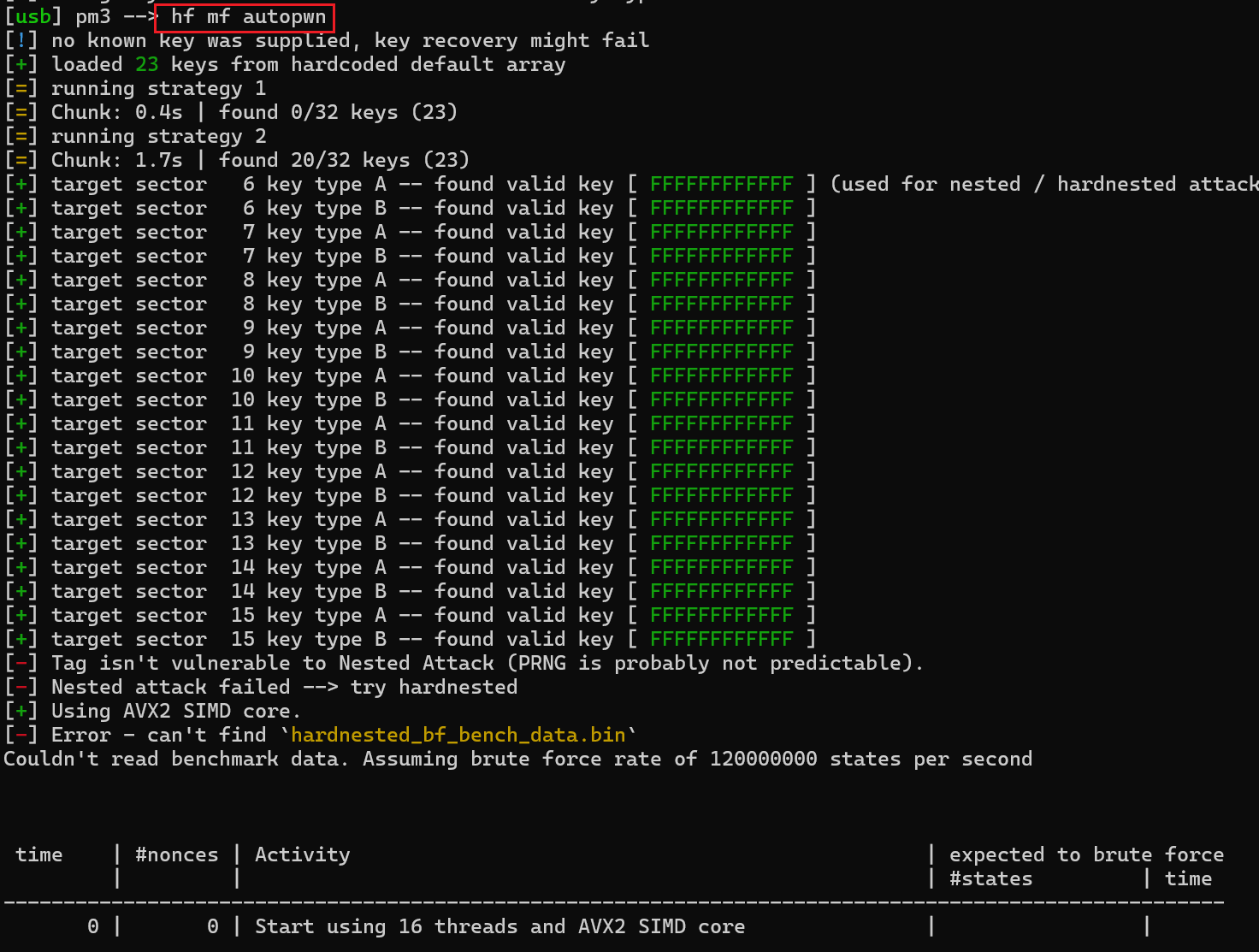
用hf mf chk --1k初始密码尝试，只有部分扇区被破解，显然数据在0~5扇区



尝试嵌套循环破解失败



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。