《信息安全引论》第一次课程实验报告

- 姓名:
- 学号:
- 日期:

1. 实验环境：

- 在配套的在线平台进行实验操作。
- 由于在线实验平台安装的 python 编程语言版本是 2.7 版本，与现在大多设备上安装的 3.x 版本语法上略有不同，因此，为了避免修改代码或者配置环境的麻烦，建议大家在线上平台执行代码并查看结果。
- 有余力也可按照说明自行安装 WSL 或 VirtualBox+Ubuntu 配置实验环境。

2. 实验内容：

[1] 单向哈希函数与 MAC 实验：https://www.lanqiao.cn/courses/242

[2] 密钥加解密实验：https://www.lanqiao.cn/courses/241

请大家按照操作步骤对每一环节的中间结果进行截图，并回答每一节题目描述中提出的问题。

3. 实验完成情况：

Ubuntu 指令介绍:
vi 编辑界面保存文件：按 esc 键，再输入 :wq 保存退出
vi 不保存退出：按 esc 键，再输入 :q! 不保存退出

ls 列出当前目录文件（不包括隐含文件）
ls -a 列出当前目录文件（包括隐含文件）
ls -l 列出当前目录下文件的详细信息（包括文件大小）

cd .. 回当前目录的上一级目录
cd - 回上一次所在的目录
cd ~ 或 cd 回当前用户的宿主目录

遇到权限问题在指令前加 sudo

单向哈希函数与 MAC 实验：

1 实验一：略，截图

2 实验二：略，截图并回答左侧描述中的问题

3 实验三：请在平台上完成，截图并回答左侧描述中的问题

4　实验四：实验平台提供的程序有问题，请使用助教提供的 hash.py。

- 执行命令：python hash.py

（如果遇到：No such file or directory，请注意 hash.py 的路径）

- 需要的输入：一个任意的 sha1 结果，以及任意的数据

观察输出结果，尤其注意输出结果 hash 的前 5 个字符。填写实验平台左侧描述的问题，可多次实验寻找规律。

输出样例：

```
ming@DESKTOP-G2B2LO1:~/myPro/cpp/tmp$ python hash.py
请输入sha1的值，将根据前20位寻找原值
6E32D0943418C2C33385BC35A1470250DD8923A9

请输入任意数据，将根据前20位寻找碰撞
666
输入数据的HASH为：cd3f0c85b158c08a2b113464991810cf2cdfc387
type2.找到碰撞：960696。其HASH值为：cd3f03254846bcba12db603b8f48cf675b002b21
type1：找到原值：1620344。其HASH值为：6e32d87cda478c2df587be0ed3b20b0264c5767b
type1：找到原值：4244775。其HASH值为：6e32d5ad2927118d72dd95201153025fc1d05f14
type1：找到原值：4457100。其HASH值为：6e32d8fb68d7e310ab5f5fd4cf6f55d8387b50c7
type1：找到原值：4471516。其HASH值为：6e32d7ab218d5fbb43ad7a92110ff1f1558f90c6
type2.找到碰撞：4955692。其HASH值为：cd3f0a040d8e309e7d55d3c6b7fb485707cad143
type2.找到碰撞：5183730。其HASH值为：cd3f0d7b505cadc0ec6d7d6a1a169c539fbe78a4
type1：找到原值：5586718。其HASH值为：6e32d73480cc69c4f2ac12c70b1eabbe788fae2b
type2.找到碰撞：5815162。其HASH值为：cd3f09ab5f393cc247473ebdc11ff52c0088910d
type1：找到原值：6297783。其HASH值为：6e32d927ae3f4121c5b637eae17f9f6afcee44aa
type2.找到碰撞：6370988。其HASH值为：cd3f0a4658be2193c83ff826fe2c074768ac83ee
type2.找到碰撞：7004142。其HASH值为：cd3f0dcffa9660cc93673864269b885c2818b2c1
type2.找到碰撞：7400189。其HASH值为：cd3f0461de8d84621691410eb1c9e1a76c6bc9aa
type1：找到原值：8059094。其HASH值为：6e32dd2a53567f2e80a784b395c60867a60eda42
type2.找到碰撞：8841307。其HASH值为：cd3f09ccd641a854cd4f8b520b5ccd30c66e8aa4
type1：找到原值：9263138。其HASH值为：6e32d43b47cc391da1afc7c5e48f624f954bc610
type2.找到碰撞：9266476。其HASH值为：cd3f0b5153825fabf4cd395ecacd74eacfc2844b
type2.找到碰撞：9288047。其HASH值为：cd3f0da9788cb2c8b65d08d8e344679c0574c743
type2.找到碰撞：9932682。其HASH值为：cd3f010d02403c1934cebed6d2a988e920ddfd10
```

源程序：

```python
import hashlib
print("请输入 sha1 的值，将根据前 20 位寻找原值")
x = input().lower()
print("\n 请输入任意数据，将根据前 20 位寻找碰撞")
y = input()
sha = hashlib.sha1()
sha.update(y.encode('utf-8'))
sha_y = sha.hexdigest()
print("输入数据的 HASH 为：" + sha_y)

for i in range(0,10000000):
    tmp = str(i)
    sha.update(tmp.encode('utf-8'))
    sha_tmp = sha.hexdigest()
    if sha_tmp[0:5] == x[0:5]:
```

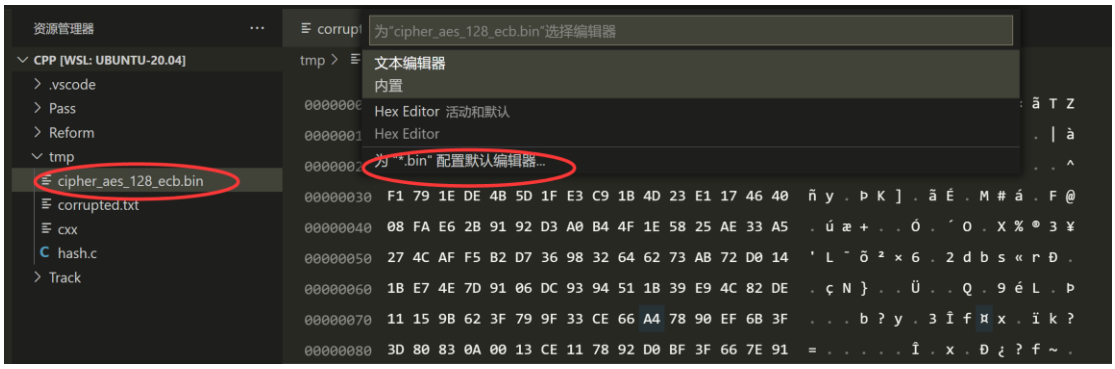
```
        print("type1：找到原值：" + str(i) + "。其 HASH 值为：" + sha_tmp)

    if sha_tmp[0:5] == sha_y[0:5] and i != y :
        print("type2.找到碰撞：" + str(i) + "。其 HASH 值为：" + sha_tmp)
```

密钥加解密实验（上）：

1 实验一：略

2 实验二：截图并回答左侧描述中的问题

- 可以在在线实验平台操作。
- 如果自己安装配置环境，由于涉及到二进制文件的修改，大家需要在 VScode 或者 VScodeInsider 中安装 hex editor 插件。



右键点击 cipher_aes_128_ecb.bin，点击“打开方式”，在中间弹出的框中选择“为*.bin 配置默认编辑器”，选择“Hex Editor”。

下面是一些需要注意的地方：

- 如果是在线平台操作，右键图片未看到 bless 打开选项，可能需要点击“使用其他应用程序打开”，选择“bless hex editor”打开。
- 注意复制替换的数据个数，54 组不能多也不能少
- 如果不能直接保存文件，可以点击左上角的“file”→“另存为”，选择桌

面等比较容易找到的地方，保存时注意一定要带上.bmp 后缀

3 实验三：略，截图并回答左侧描述中的问题

4 实验四：略，截图并回答左侧描述中的问题

密钥加解密实验（下）：

1 实验一：略

2 实验二：略

注：

- 请大家在实验过程中结合教学网的课件和参考资料对课程内容进行回顾，并尽量回答对题目描述中的问题的理解。