信息安全引论 第一次实验

实验环境

学生自备计算机进行实验操作
具体实验环境如下：
Python 3.8
安装 PyCryptodome 库：`pip install pycryptodome`
有余力同学可以按照说明自行安装 WSL 或 VirtualBox+Ubuntu 配置实验环境

实验内容

1.密钥加解密实验

1.1 使用不同加密算法进行加密

使用 **Python** 调用附件中的 `Encrypt.py`，对不同加解密算法进行体验。

1.2 学习 ECB 与 CBC 的区别

使用 **Python** 调用附件中的 `EncryptPic.py`，使用不同方式对附件中的 **`pic_original.bmp`** 进行加密，并观察 ECB 加密的结果与 CBC 加密的结果的区别，说明原因。

1.3 损坏的密文

分别使用 ECB 模式和 CBC 模式对 `sample.txt` 进行加密，随后修改其密文的第 30 个字节的内容。请对修改后的密文进行解密，观察解密结果并给出相应的分析。

1.4 密文的填充

分别使用 ECB 模式和 CBC 模式对 16 个字节内的不同文本加密，观察密文的长度，分析加密方法是否使用了填充。

2.单向哈希函数与 MAC 实验

2.1 生成消息摘要和 MAC

使用 **Python** 调用附件中的 `Hash.py`，使用三种不同的哈希函数将 `hello.txt` 中的文本转化为固定长度的哈希值

2.2 Keyed Hash 和 HMAC

使用 **Python** 调用附件中的 `HMAC.py`，使用三种不同的 HMAC 完成对 `hello.txt` 的签名

2.3 单向哈希函数的随机性

使用 **Python** 调用附件中的 `Random.py`，输入种子，观察随机数低 3 位的概率分布

2.4 单向特性

使用 **Python** 调用附件中的 `Collision.py`，对哈希函数输出的前导零数量进行碰撞，观察输出结果

提交要求

信息安全引论》第一次课程实验报告

- 姓名:
- 学号:
- 日期:
- 实验内容：截图并回答实验内容中描述的问题
- **提交作业的文件名采用“学号+姓名+第几次实验作业”**