Github（或者 Coding）账号：https://github.com/eric-huyl

个人博客关于密码学实验的链接：**crypto repo 的 GitHub pages，待建**

实验题目（中文）：密码学实验一

实验摘要（中文）：

关于密码学实验的说明

1. 密码学实验将进行四次，每次实验，需按要求上传提交代码截图、相关结果等。
2. 请建立自己的技术博客或者其它记录载体，简单记录每次实验内容，所遇到的问题以及心得（建议）。
3. 因学校要求提交实验报告以给出成绩，我们只交一次纸质版实验报告，内容 4 次实验任选。
4. 最终提交时间 11 月 30 日晚 23:00 前。
5. 请建立自己的代码托管账号，Github 或 Coding 或其他托管平台均可，建立合理的文件目录托管代码，请清晰命名，给出必要注释；
6. 电子版提交学在西电，提交 pdf 版附件命名“姓名_学号_密码学实验”。

实现流密码相关的设计实现与破解，主要集中在单字节异或或者多字节循环（KEY）的异或。

题目描述（清楚描述题目中文，写出自己的理解，请勿复制原题目）

1. Many Time Pad

给出了十条使用同一个密钥加密不同文本的密文，要求找出密钥。

2. PA1 Option

设计程序暴力破解类维吉尼亚密码，其中按字节的异或代替了加摸 26。就是说维吉尼亚密码中的那个密码表要修改一下，用异或重新计算。

3. Cryptopals Set 1

1) 将十六进制编码的字符串转为 base64 编码
2) 将等长的字符串异或
3) 暴力破解单字节异或加密后的字符串‘
4) 找出（检测）一个经过单字节异或加密后的字符串
5) 实现一个循环密钥异或加密
6) 暴力破解一段循环密钥加密后的字符串
7) 使用 ECB 模式的 AES-128 解密一段字符串
8) 找出（检测）一个 ECB 模式加密后的字符串

过程（包括背景，原理：必要的公式，图表；步骤，如有必要画出流程图，给出主要实现步骤代码）

1. Many Time Pad

首先考虑两条思路：**ascii** 编码的冗余性和英文词频。这里使用前一条思路。关键点在于发现大写字母和空格异或之后成了小写字母，小写字母和空格异或之后变成大写字母，两字母异或之后不是字母。于是将密文两两异或，对于同一个密文的同一个位置，如果出现足够次数的字母，那就可以认为明文是空格，于是推出这个位置的密钥。以此类推。

2. PA1 Option

维吉尼亚密码其实也是一种重复密钥密码，每个 **KEY SIZE** 的明文都使用同一个密钥也就是 **key** 加密，这里就是按字节异或，原来的密码是加。首先猜测密钥长度，然后按照密钥长度切分密文，就可以爆破密码了。

3. Cryptopals Set 1

1) 这没啥好说的，看代码就行了
2) 这也没啥好说的
3) 可以暴力破解，也可以用词频来猜测明文 **e** 对应的密文
4) 用上一题的函数来进行词频分析，找到最像的
5) 纯代码，没啥好说的
6) 首先用题目给出的汉明距离的方法猜测长度，得到长度是 **4**，然后对于所有块的同一位置，相当于是一个单字节异或，解法同上
7) 调个库函数，没啥好说的
8) 寻找相同的十六字节串就行了

总结（完成心得与其它，主要自己碰到的问题和解决问题的方法）

真的很难啊。首先是英文的题目总是有点歧义，需要自己尝试多个思路，才能明确做法。其次是对于 **python** 需要有比较熟练的掌握，不然写起来磕磕巴巴的。好在现在有 **gpt** 可以实现一些指定的功能，比如切分字符串，格式转换，不用挨个查阅，方便了很多。对于理论掌握之后，实现的部分还是相对简单的。

参考文献（包括参考的书籍，论文，URL 等，很重要）

https://blank-vax.github.io/

https://chatgpt.com/?model=auto