**密码安全**

姓名：钱煜 学号：57118105

1. 实验目的

学习密钥加密的加密算法、加密工作机制、填充和初始向量、使用工具和程序对消息进行加密和解密。

二、实验内容

1.单字母替代密码的频率分析；

2.

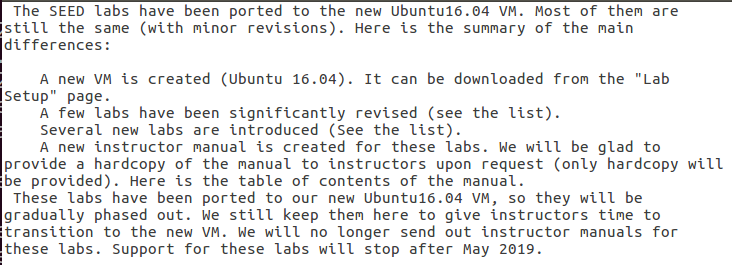
三、实验环境

Virtual Box，Seed Ubuntu 16.04。

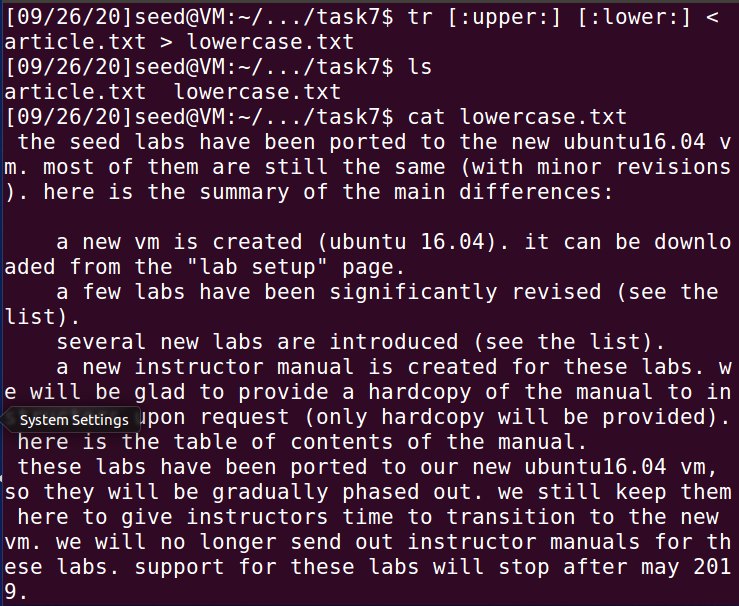
1. 实验

**Task 1.单字母替代密码的频率分析**

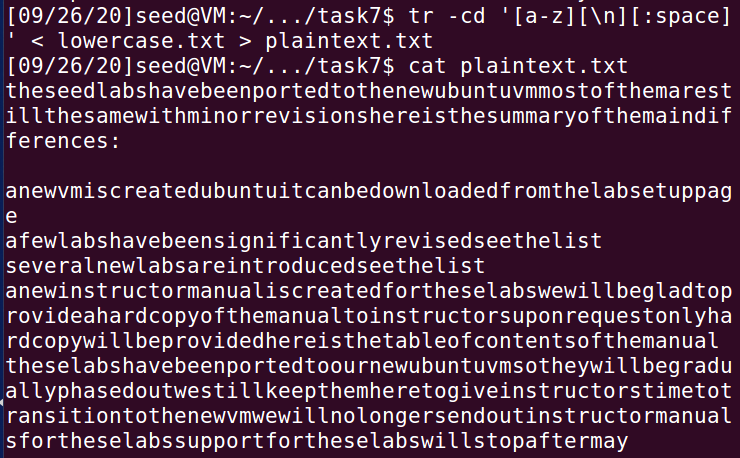
创建一个txt：



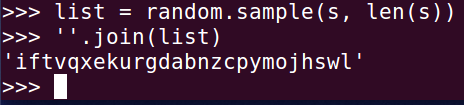
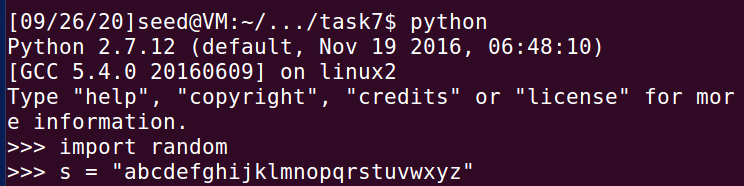
将所有的大写字母变为小写：



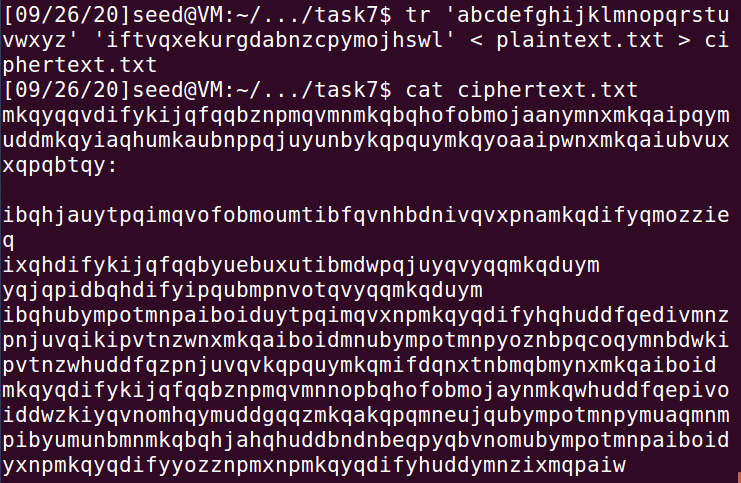
去掉所有标点符号和数字：



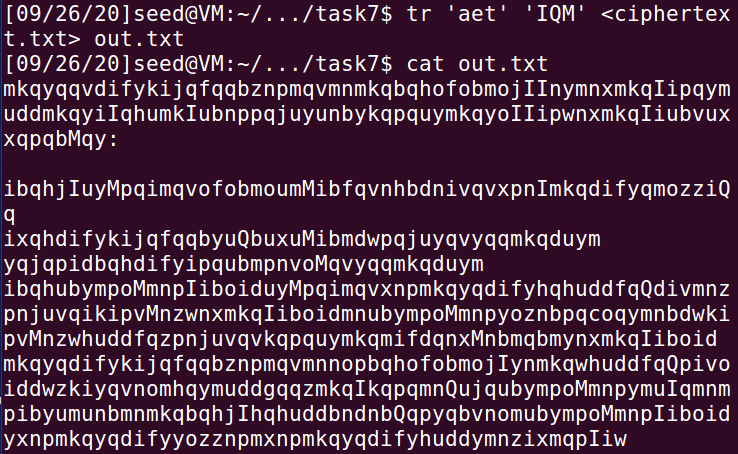
随机生成替换表：



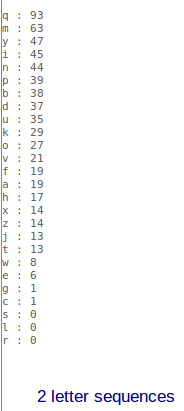
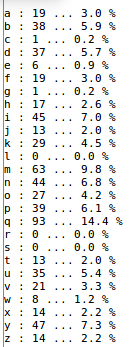
通过随机替换表进行加密：



明文大写：



使用网站分析频率：



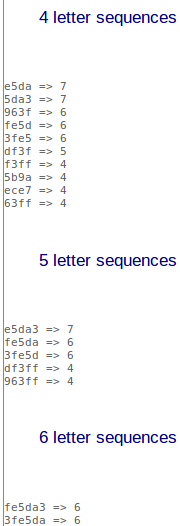
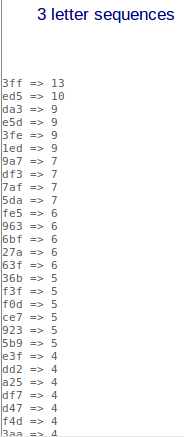
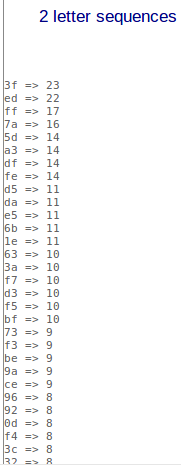
对比替换得到：

Qmyinpbdukovfahxzjtwegcslr

Abcdefghijklmnopqrstuvwxyz

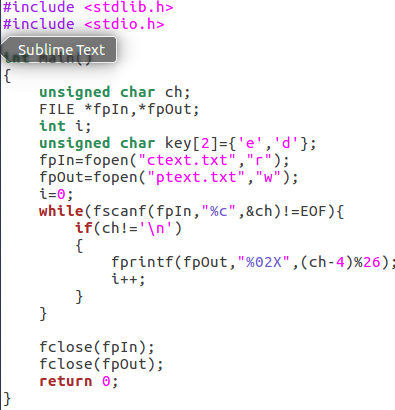
**TASK 2.破解维吉尼亚密码**

首先，通过网站分析维吉尼亚密码的秘钥：

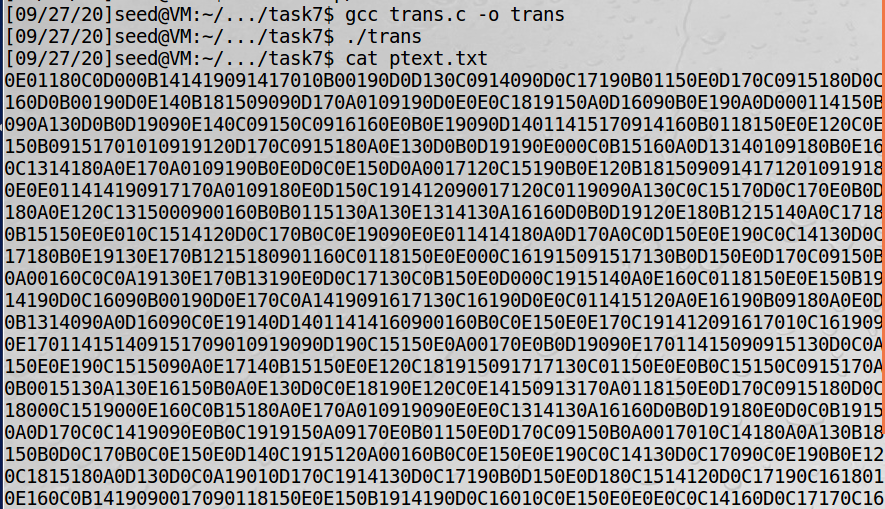


密钥全为字母：ed

编写破译程序：

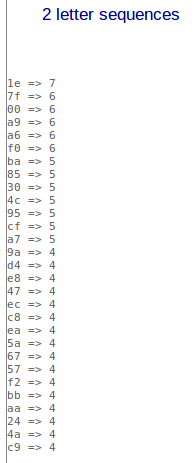


破译：



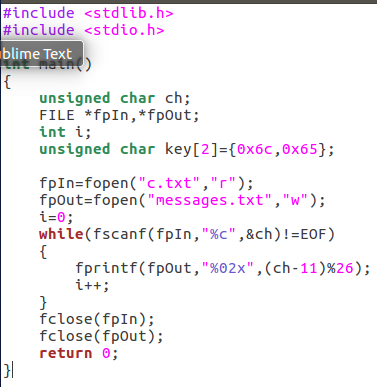
TASK 3.异或运算破解

分析重复率：



得到密钥为：le

编写程序：



得到结果：

