****

实验报告

|  |  |
| --- | --- |
| 姓名： | 强珂阳 |
| 学号： | 57118106 |

东南大学网络空间安全学院

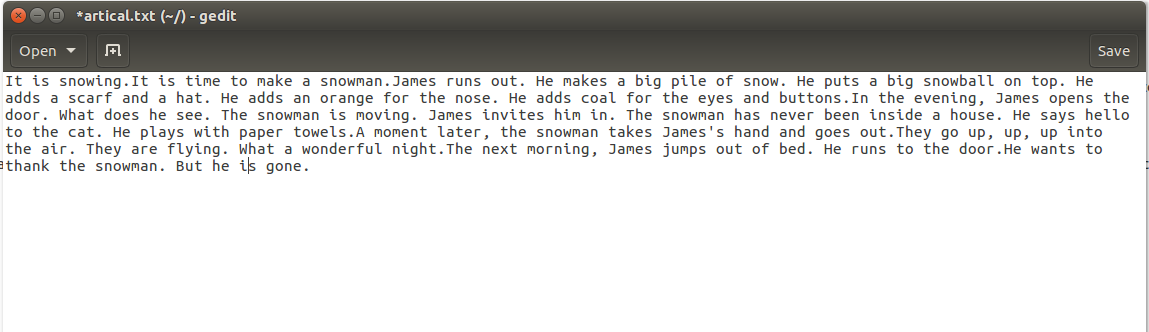
School of Cyber Science & Engineering

Southeast University

2020年9月

实验一

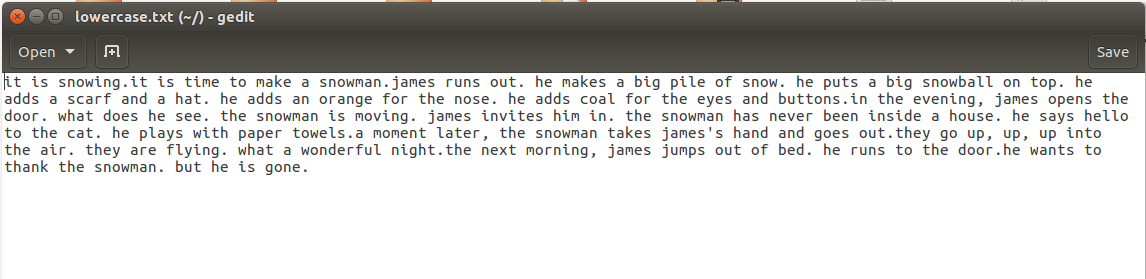
TASK1：Frequency Analysis Against Monoalphabetic Substitution Cipher

先复制一篇英文文章:

将其字母全部改为小写：



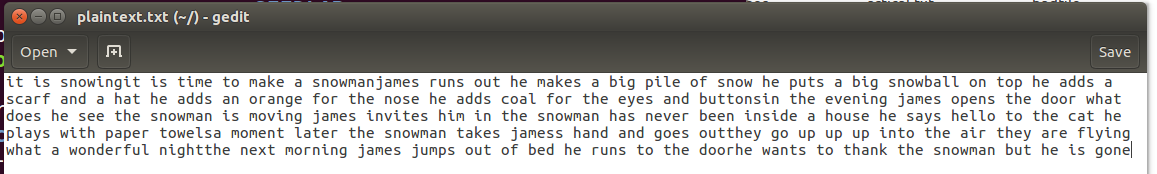
改过之后如图：



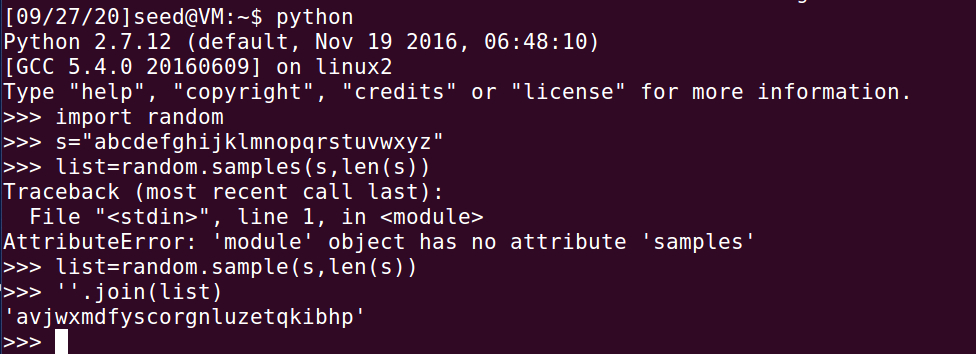
把标点、换行去除，保留空格：



明文如下：



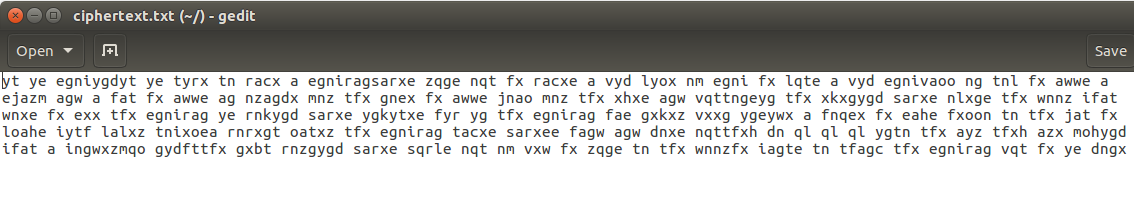
生成替换表：



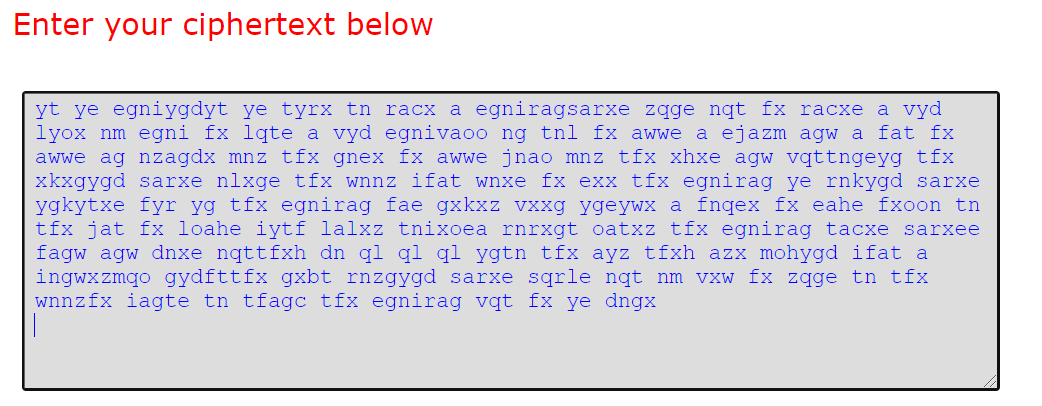
即abcdefghijklmnopqrstuvwxyz对应生成：avjwxmdfyscorgnluzetqkibhp

按替换表进行替换生成密文：

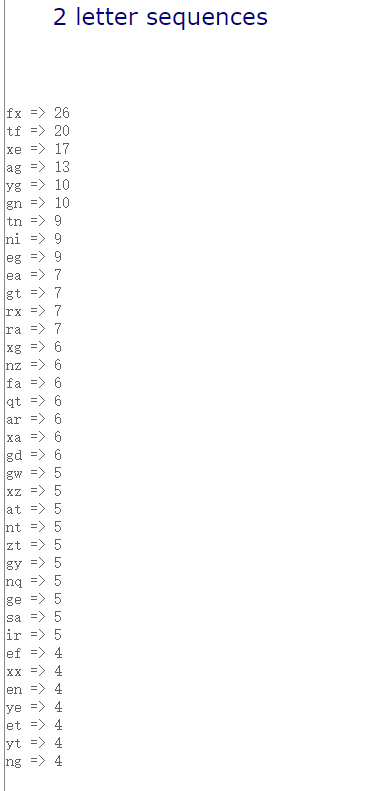
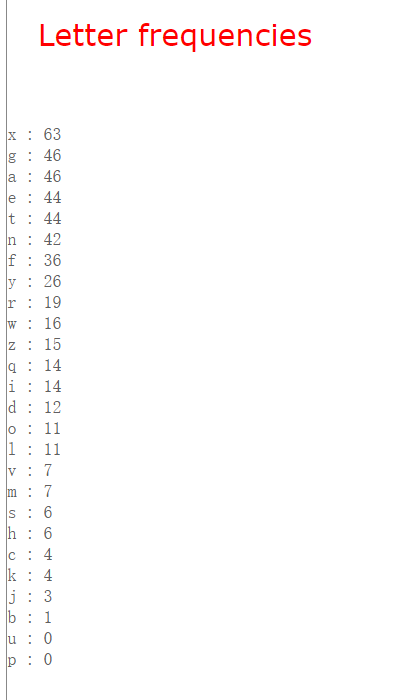
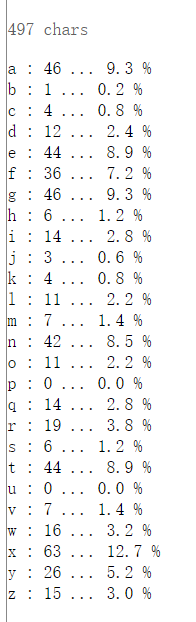


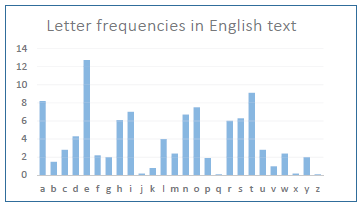


登录<http://richkni.co.uk/php/crypta/freq.php>并输入密文：

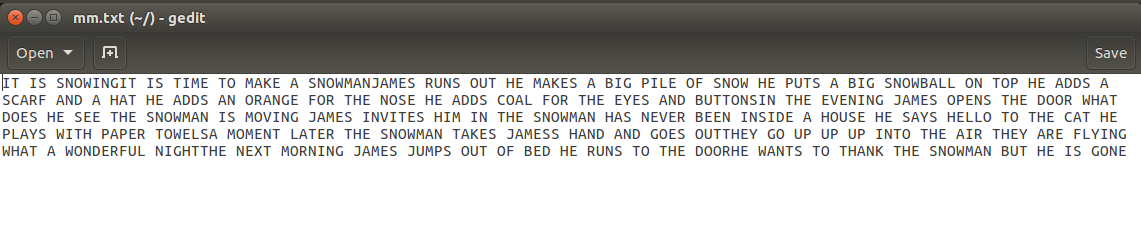


统计密文字母出现频率：





通过对比频率表猜测部分密文，并将已解密的单词换成大写字母逐步尝试，最终可以解得明文为：

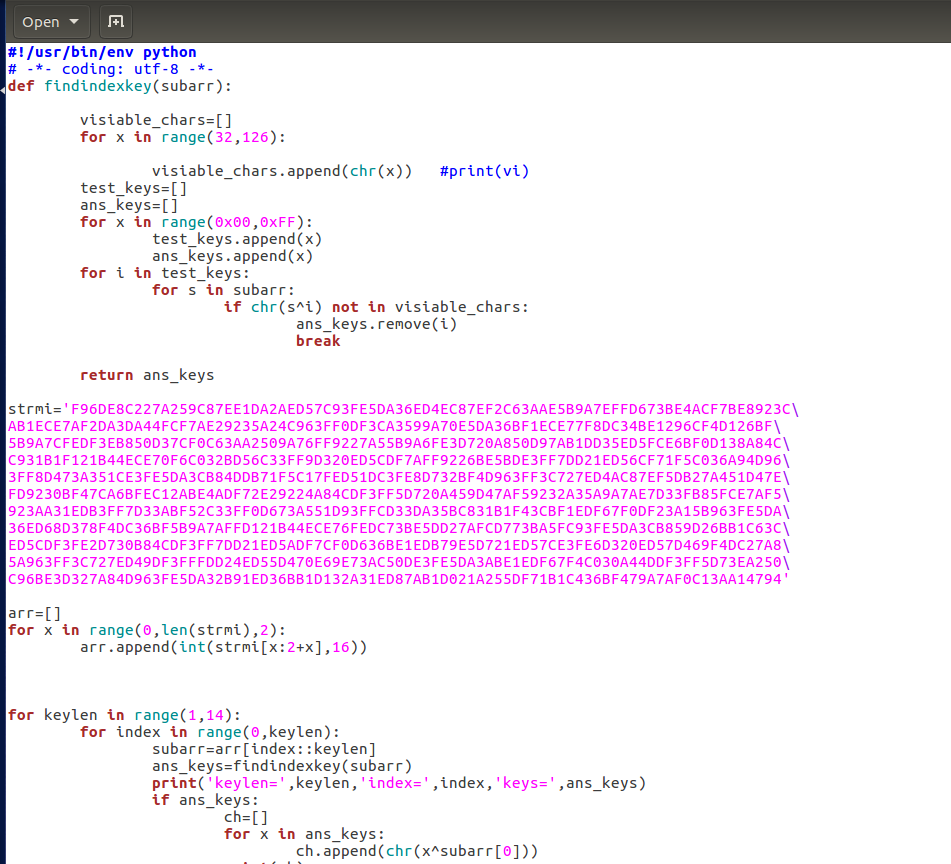


对照最初的明文可以发现，解密成功。

实验二

1.破解维吉尼亚密码

解密代码如下：



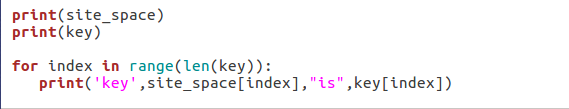


得到密文为：Cryptography is the practice and study of techniques for, among other things, secure communication in the presence of attackers. Cryptography has been used for hundreds, if not thousands, of years, but traditional cryptosystems were designed and evaluated in a fairly ad hoc manner. For example, the Vigenere encryption scheme was thought to be secure for decades after it was invented, but we now know, and this exercise demonstrates, that it can be broken very easily.

2.一次一密

解密代码如下：





密文1-7分别与除自身以外的密文进行异或，确定密钥：密钥 2 为 1a,密钥 3 为 4, 密钥 4 为 9b,密钥 5为 d0 , 密钥 6 为 73 , 密钥 8 为 c8, 密钥 10 为 98, 密钥 12 为 9, 密钥 14 为 bc, 密钥 15 为 86, 密钥 16 为 da, 密钥 17 为 c9, 密钥 19 为 39, 密钥 20 为 89 ,密钥 22 为 5f, 密钥 23 为 72, 密钥 24 为 67,密钥 25 为 83 ,密钥 26 为 a5 ,密钥 27 为 61 ,密钥 28 为 fd ,密钥 29 为 25。(均为十六进制)，用已知密钥求解各部分字段，再推测其余密钥，最终得到：I am planning a secret mission. He is the only person to trust. The current plan is top secret. When should we meet to do this?I think they should follow him. This is purer than that one is. Not one cadet is better than I.

**总结：**

实验一可以看出，在文章很短的情况下，字母出现频率与统计得到的频率并不完全一致，在猜测时只能参考，但是由于每个字母加密成的密文都一样，所以破译一个字母之后可以代入并猜测同单词的其他字母，破译难度并不高。

实验二的代码是参考的同学的代码，只是进行了代码的理解以及运行，对于维吉尼亚密码的破解有了具体过程的了解，比在讲义上平面理解更加具象了。