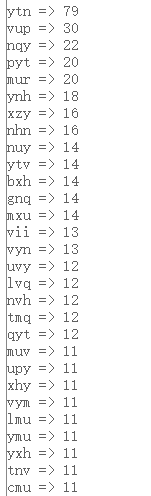
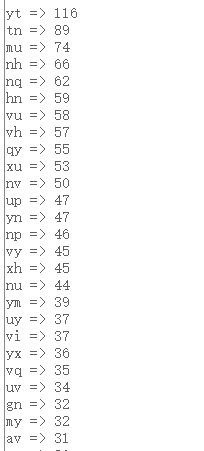
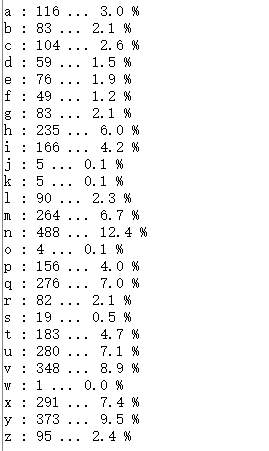
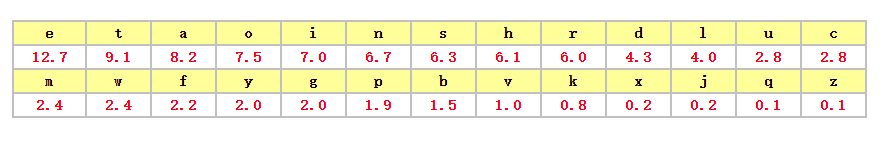
**Lab[7]-report**

57118123刘康辉

**Task 1**



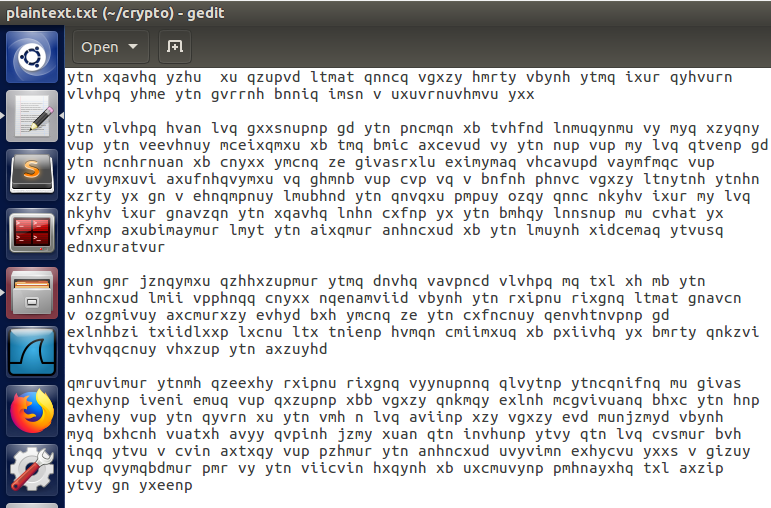
利用<http://www.richkni.co.uk/php/crypta/freq.php>网站对密文进行频率统计，如上图所示。



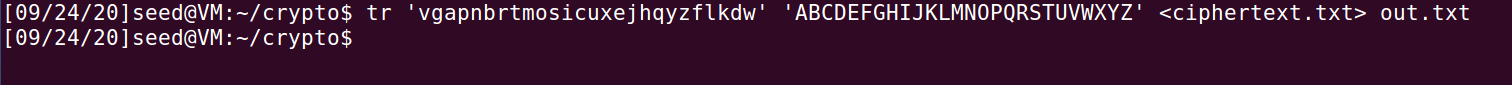
根据上图的字母频率表，推测部分明文中字母与密文中字母的对应关系，然后再根据单词组成和语义推测剩余字母的对应关系。



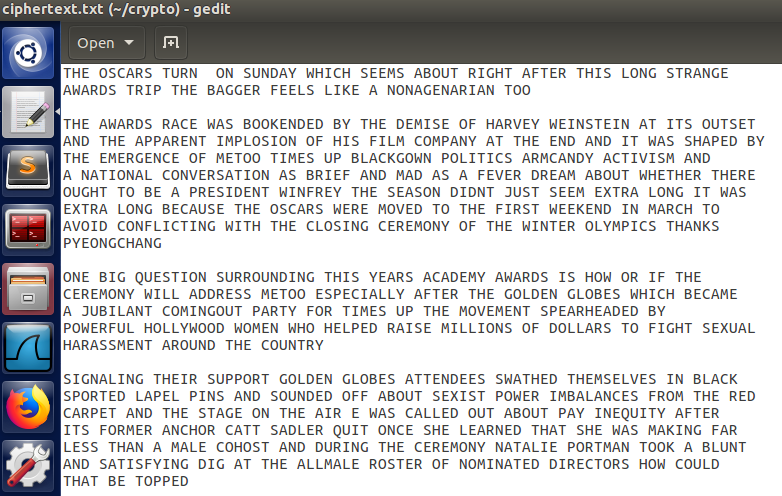
根据推测可得明文中字母与密文中字母的对应关系如上图所示，明文为大写，密文为小写，以便区分是否被解密。



文件plaintext.txt中的密文如上图所示。

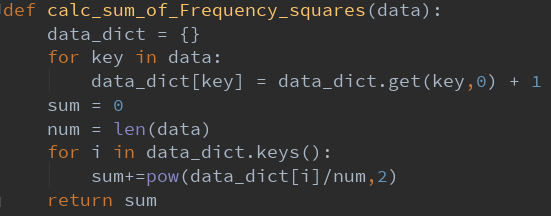


根据分析得到的对应关系，输入命令将plaintext.txt文件中的密文字母全部转换成明文字母，并将解密得到的明文写入ciphertext.txt文件。

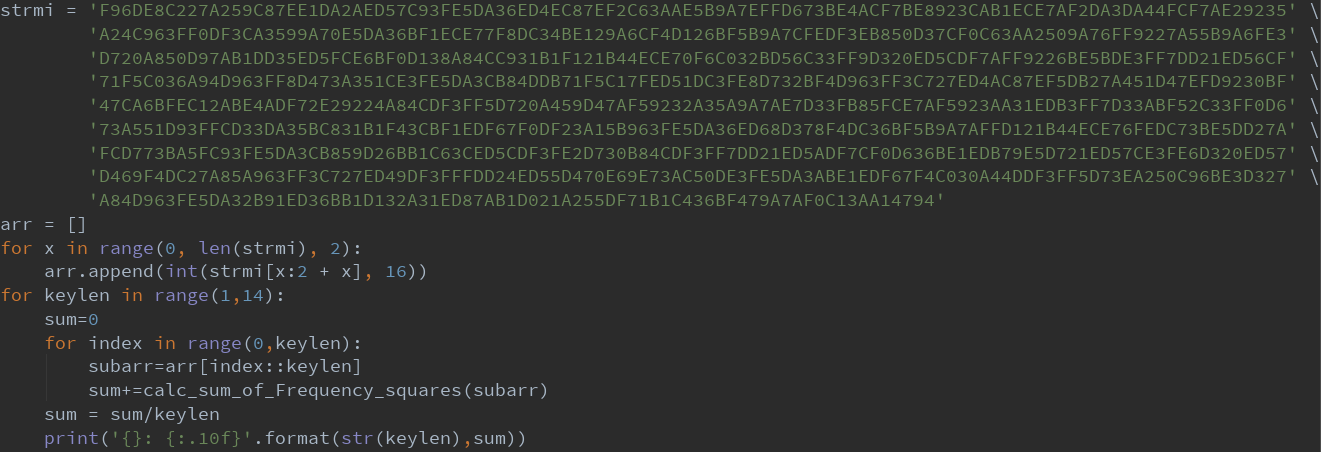


文件ciphertext.txt中的明文如上图所示。根据内容可知，字母均为大写并且单词组成和语义合理，因此解密成功。

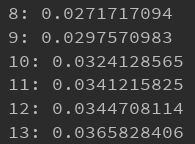
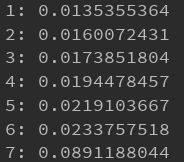
**Task 2**



创建函数统计密文中每个字符的频率及其平方和，记录每个字符的出现次数，再除以密文总长度得到频率，然后计算频率平方和。当频率平方和最大时，对应的密钥长度即为实际密钥长度。



将密文写入程序中并转换成ASCII码进行操作，依次测试1~14位的密钥长度，每隔密钥长度提取密文，由于这些密文字母对应同一位密钥，因此利用上述的函数寻找可能的密钥长度。

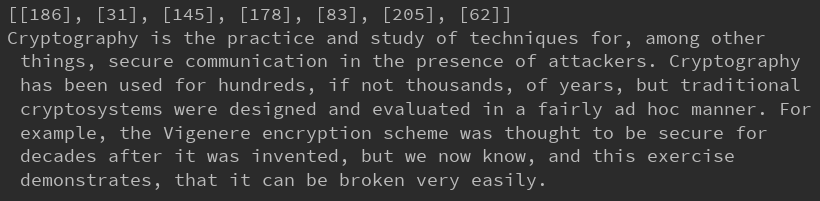


执行上述的程序，发现当密钥长度为7位时得到的频率平方和最大，结果如上图所示。因此可知，密钥的长度为7位。



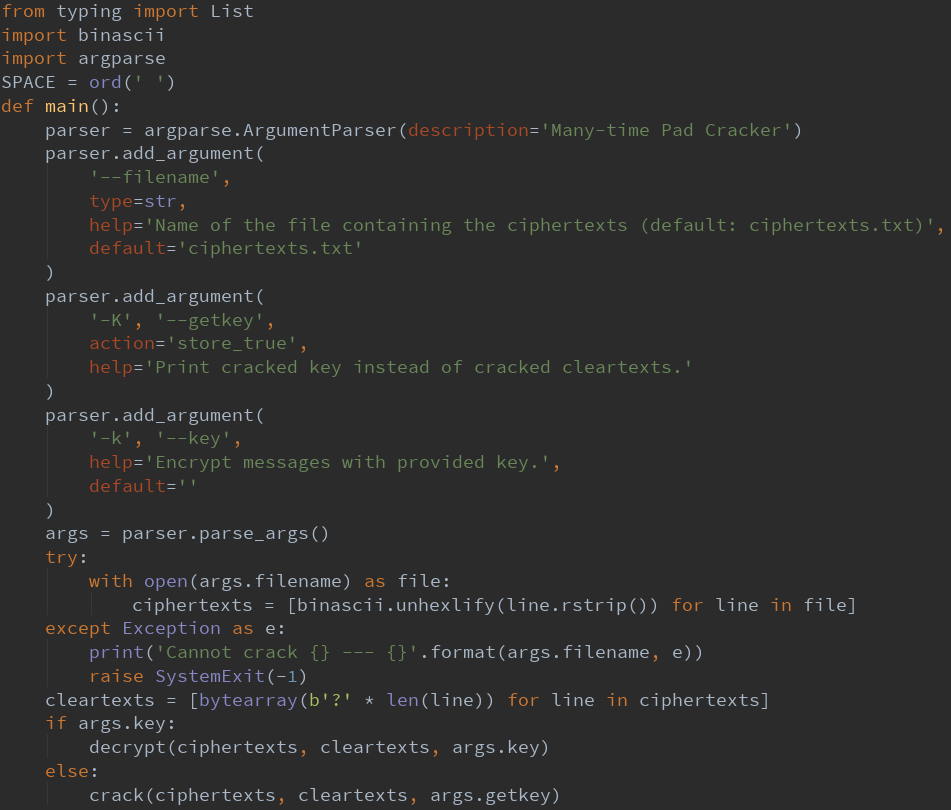


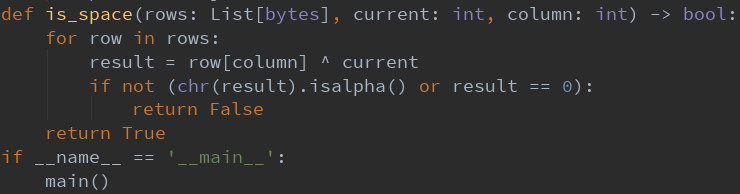
已知密钥长度为7位，创建函数寻找具体的密钥，0x00~0xFF中的每一个数与密文中每一个值进行异或操作。如果得到的结果不是英文、数字、逗号、句号、空格，就去除此数。此外，利用找到的密钥对密文进行解密，判断得到的明文是否正确合理。



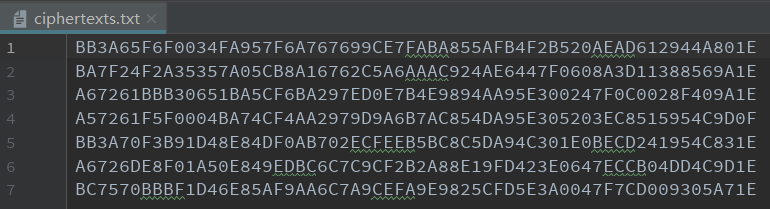
执行上述的程序，发现得到的结果是唯一的，密钥为**186 31 145 178 83 205 62**，即**0xBA 1F 91 B2 53 CD 3E**，解密得到的明文为**Cryptography is the practice and study of techniques for, among other things, secure communication in the presence of attackers. Cryptography has been used for hundreds, if not thousands, of years, but traditional 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.**，结果如上图所示。

**Task 3**

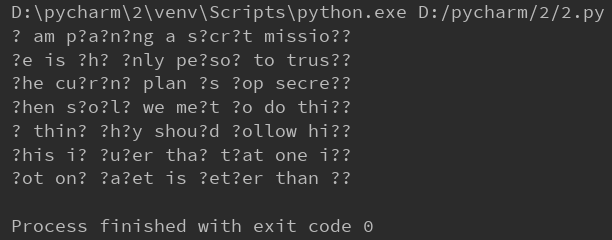




由于密文异或与明文异或的结果相同，而空格和字母异或与字母和字母异或的结果不同。创建程序破解一次一密，判断密文字符是否对应空格，再寻找具体的密钥并对密文进行解密。



将密文写入ciphertext.txt文件中。



执行上述程序，发现得到的结果如上图所示，再进行分析可得明文如下所示。

**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.**