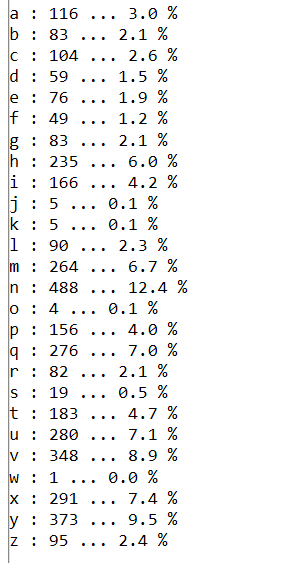
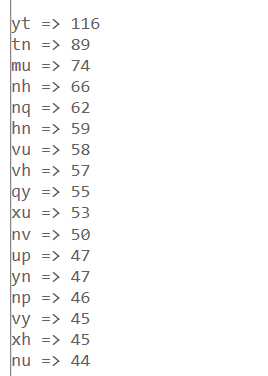
Task1：破解单表代换密码

先分析密文词频

单字母 双字母

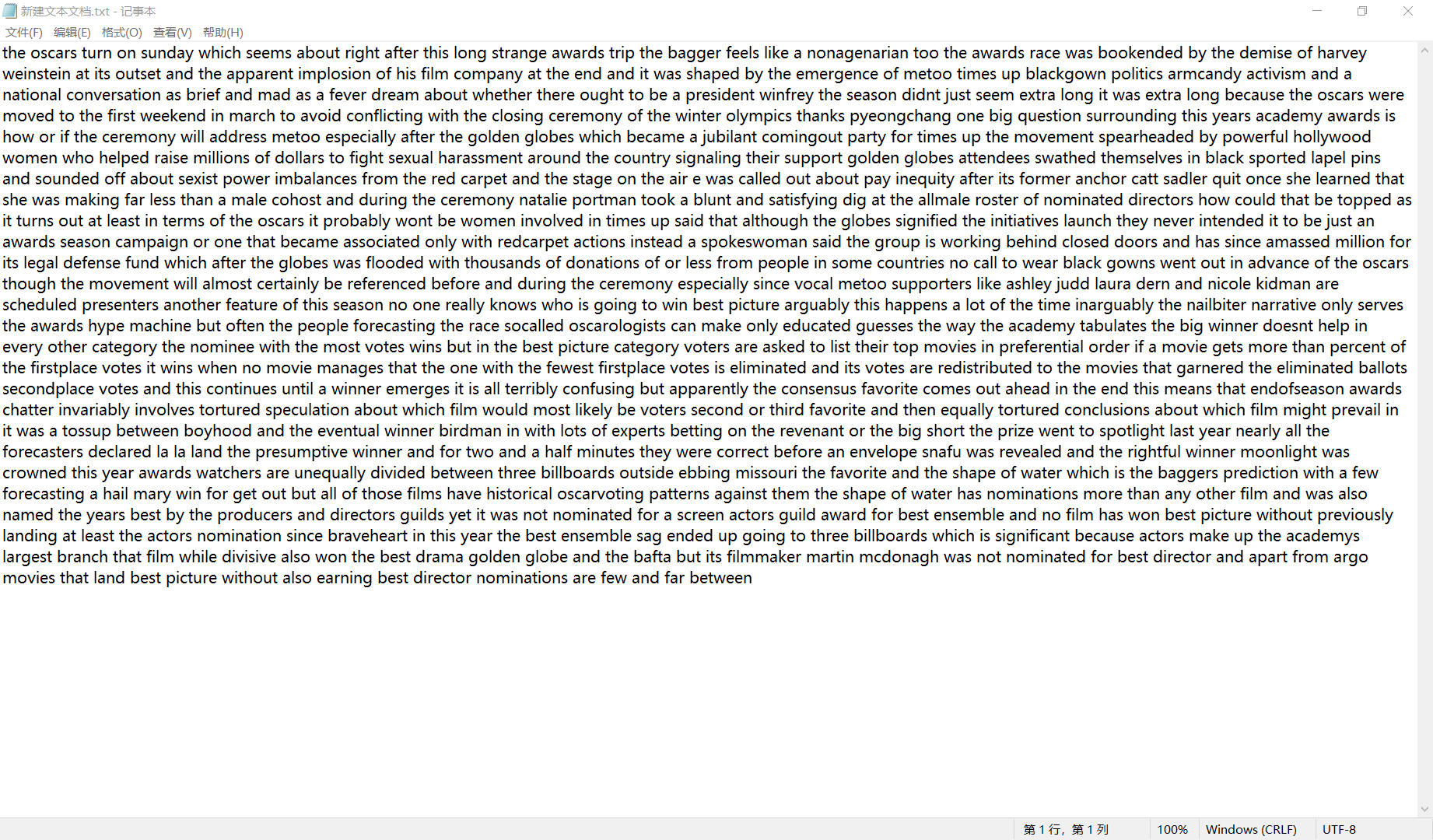
 

与标准词频比较，猜测yt可能为th，n可能为e

替换这些字母后继续比较、尝试

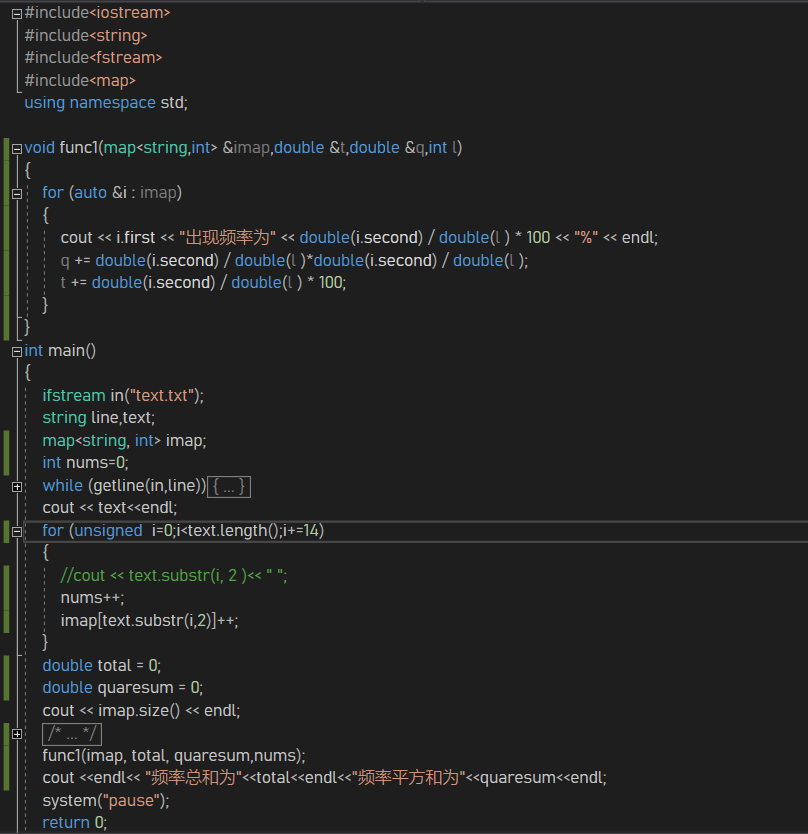
最后得出x为o、u为n等等

将全部字母替换后得出的明文如下



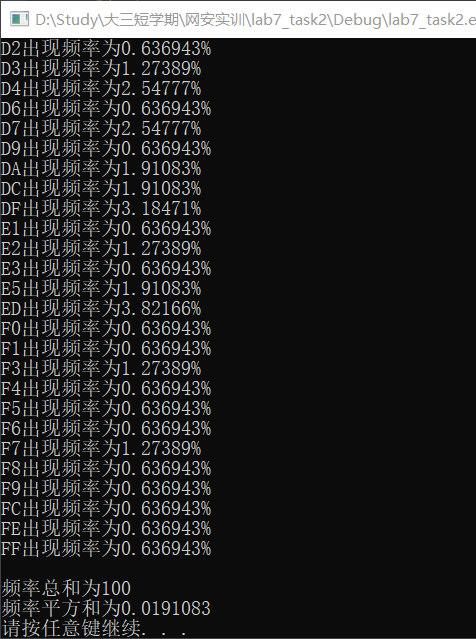
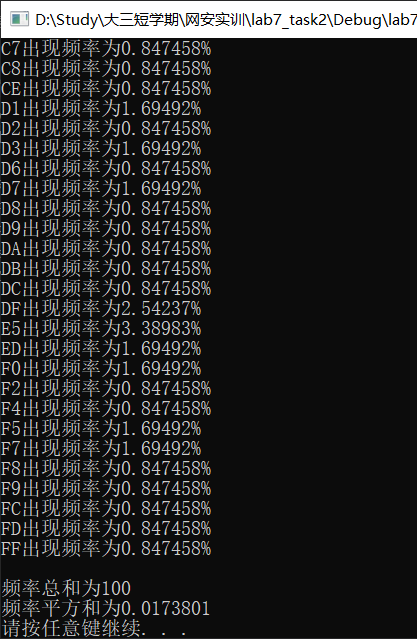
Task2:破解维吉尼亚密码

编写c++程序，功能是统计密文中不同ASCII码出现的频率并计算平方和，代码如下

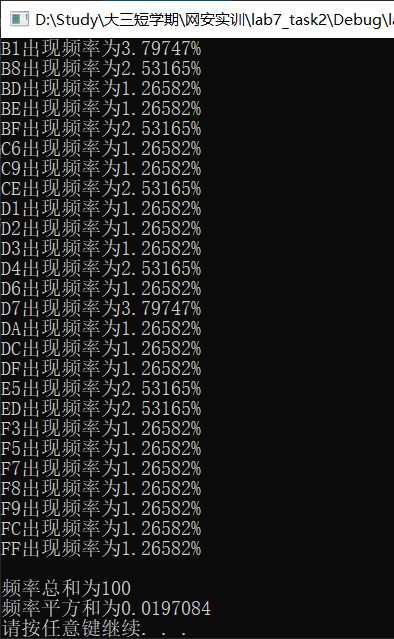
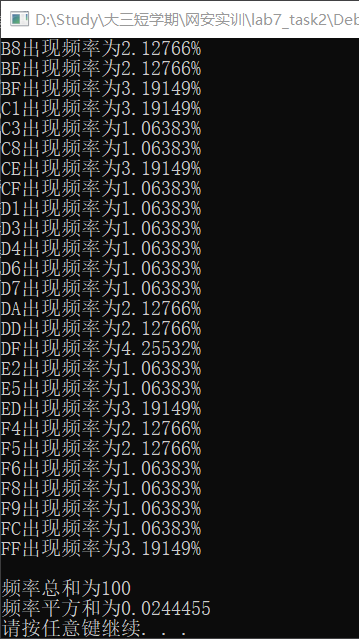


调整密钥长度，发现密钥长度较小时频率平方和在0.02上下波动，如图

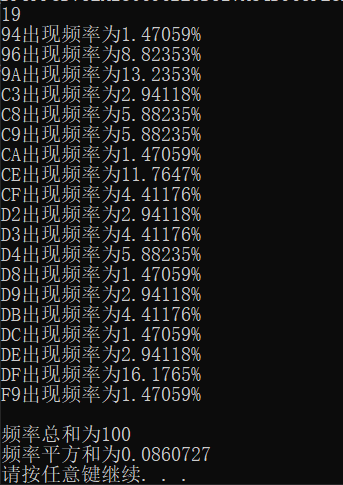
密钥长度为3： 密钥长度为4：



密钥长度为5： 密钥长度为6：



但当密钥长度为7时，不同ASCII的数量大幅减少，频率平方和剧增，如图



密钥长度继续增长时，频率平方和在从7到8时急剧跌落到0.25左右，然后缓慢增长，原因应该是密文长度不够长导致密钥变长后取得的样本少，因而熵增大。

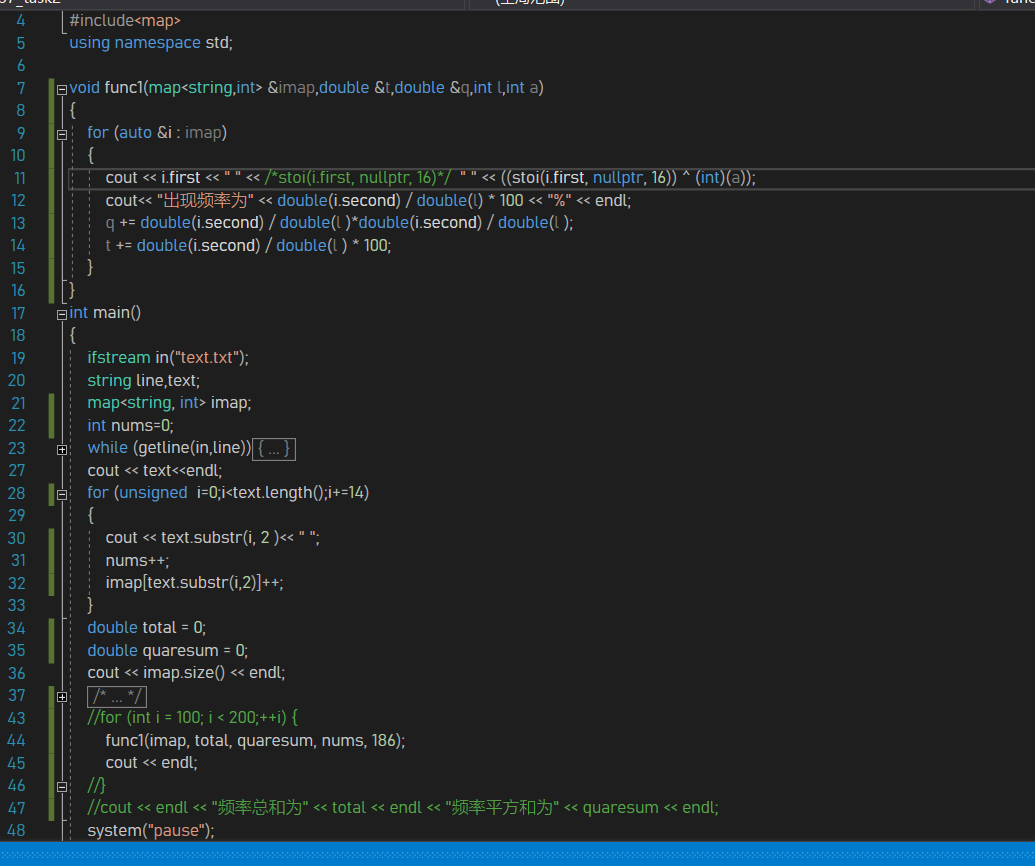
以上测试的是每一组密文（密钥长度的密文为一组）的第一个，在测试第二个、第三个时发现结果相同，都是密钥长度为7时剧增

根据以上测试结果，可以判断密钥长度就是7。

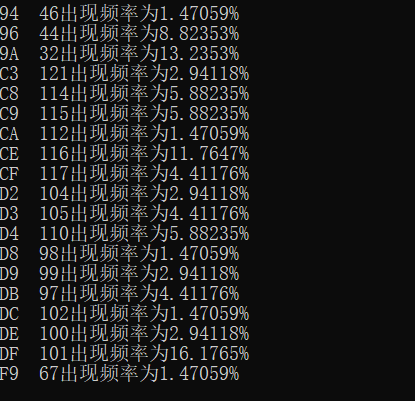
接下来便是将各组用相同密钥加密的密文进行单表代换的破解了。

对之前的程序稍作修改使其输出密文经过假设的密钥解密后的明文的ASCII码，若都在可见字符范围内（32-126）则该密钥可能为真密钥。

修改后程序如下



输出格式如下，第二列数字即为用尝试密钥解密的明文ASCII码



循环代码（上面截图中已注释）寻找可能的密钥，大约有十来组，一一尝试

最后得到密钥：

186, 31, 145, 178, 83, 205, 62，转换为16进制为BA,1F,91,B2,53,CD,3E

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.

Task3:破解一次一密密码

密文为：

BB3A65F6F0034FA957F6A767699CE7FABA855AFB4F2B520AEAD612944A801E

BA7F24F2A35357A05CB8A16762C5A6AAAC924AE6447F0608A3D11388569A1E

A67261BBB30651BA5CF6BA297ED0E7B4E9894AA95E300247F0C0028F409A1E

A57261F5F0004BA74CF4AA2979D9A6B7AC854DA95E305203EC8515954C9D0F

BB3A70F3B91D48E84DF0AB702ECFEEB5BC8C5DA94C301E0BECD241954C831E

A6726DE8F01A50E849EDBC6C7C9CF2B2A88E19FD423E0647ECCB04DD4C9D1E

BC7570BBBF1D46E85AF9AA6C7A9CEFA9E9825CFD5E3A0047F7CD009305A71E

由于相同密钥加密的密文异或后的结果与明文异或结果相同，而两字母异或后的二进制表达中前两位为00，其中有一个空格则为01，可以借此找到空格。

先找到密文中两奇数位异或结果为01的，第一句中3与第二句中7异或前两位为01，故其中一个可能为空格，假设3A代表空格的密文，那么可以知道7F明文ASCII值为0x65，即为e，第三、四、六句中72为h。还可以知道第五句第二个字符也为空格。

以此方法试出所有空格的位置并能同时得到部分字母，再进行补全，最后得到明文如下：

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.