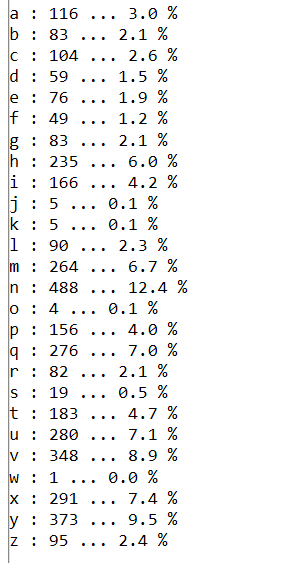
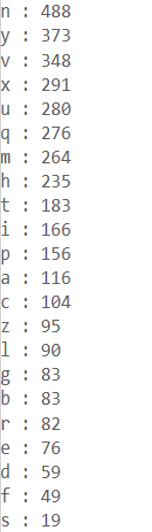
Lab1

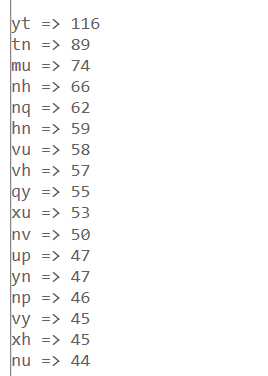
Task1：

在指南中的网站<http://www.richkni.co.uk/php/crypta/freq.php>上分析词频

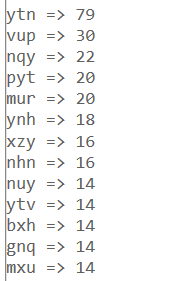
单字母词频如下

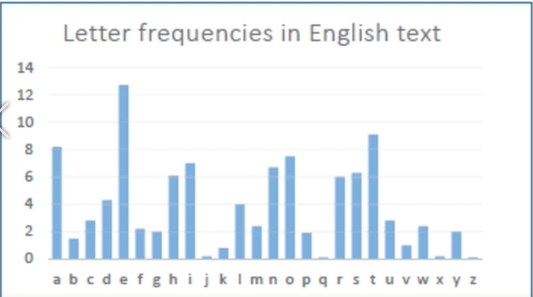
双字母词频如下

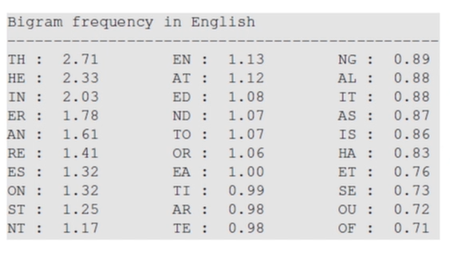


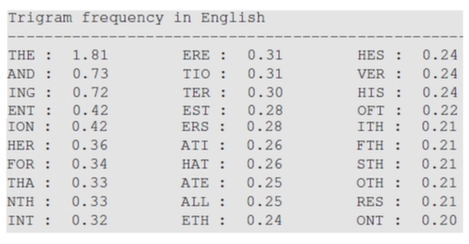
三字母词频如下



与正常情况下的单字母、双字母、三字母词频比较





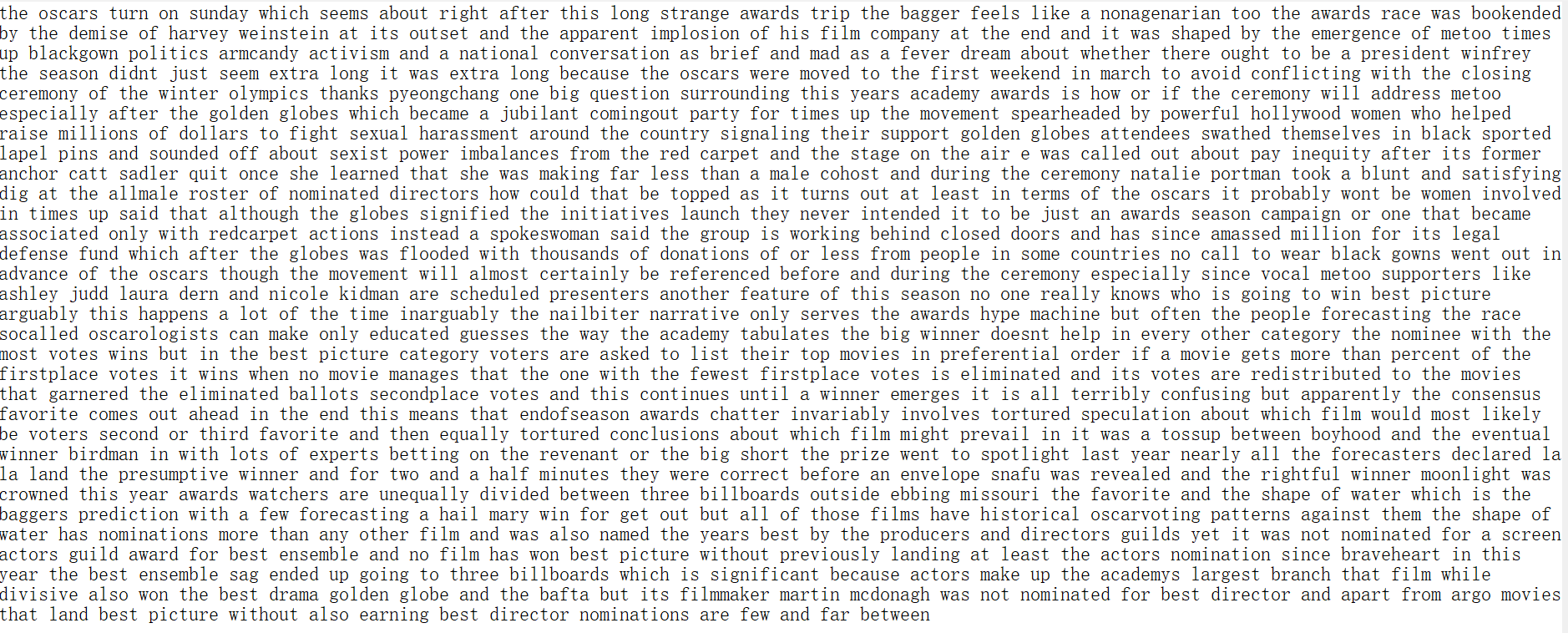


可知ytn很大可能为THE，用命令



用流将文件中的ytn变为THE。

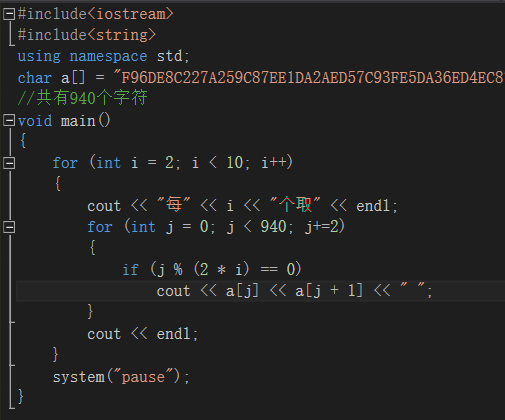
再根据单字单词v一定是A，双字词xu、mu、vu等双字幕单词可能为of、on、or、at等数量有限的单词，可大概判断x为O、u为N、g为B、y为D、b为F、m为I、h为R、q为S；将这些已经判断出的字母用之前的命令再次修改文件，通过以下单词的组合就可判断出全文如下

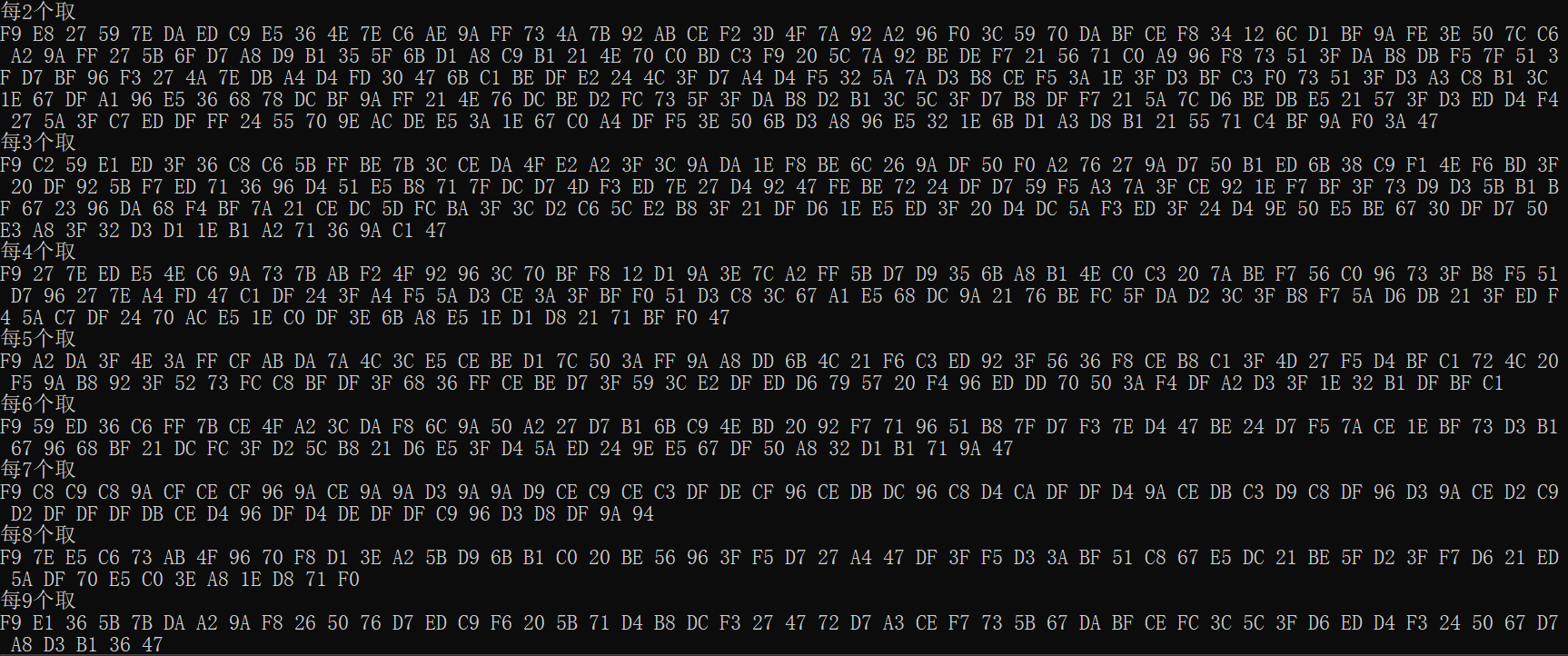


Lab2

维吉尼亚密码

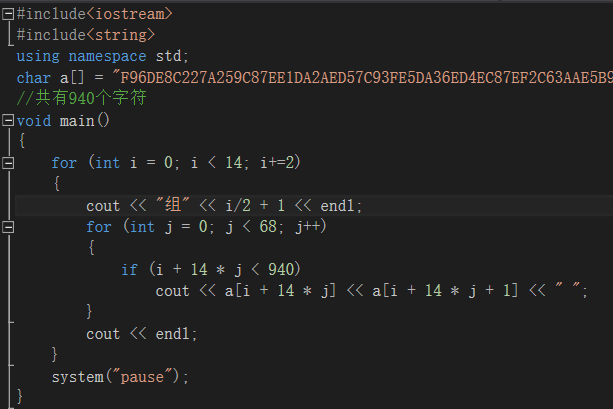
先找出密钥的长度，分别隔2~9取一对密文，代码及输出结果如下

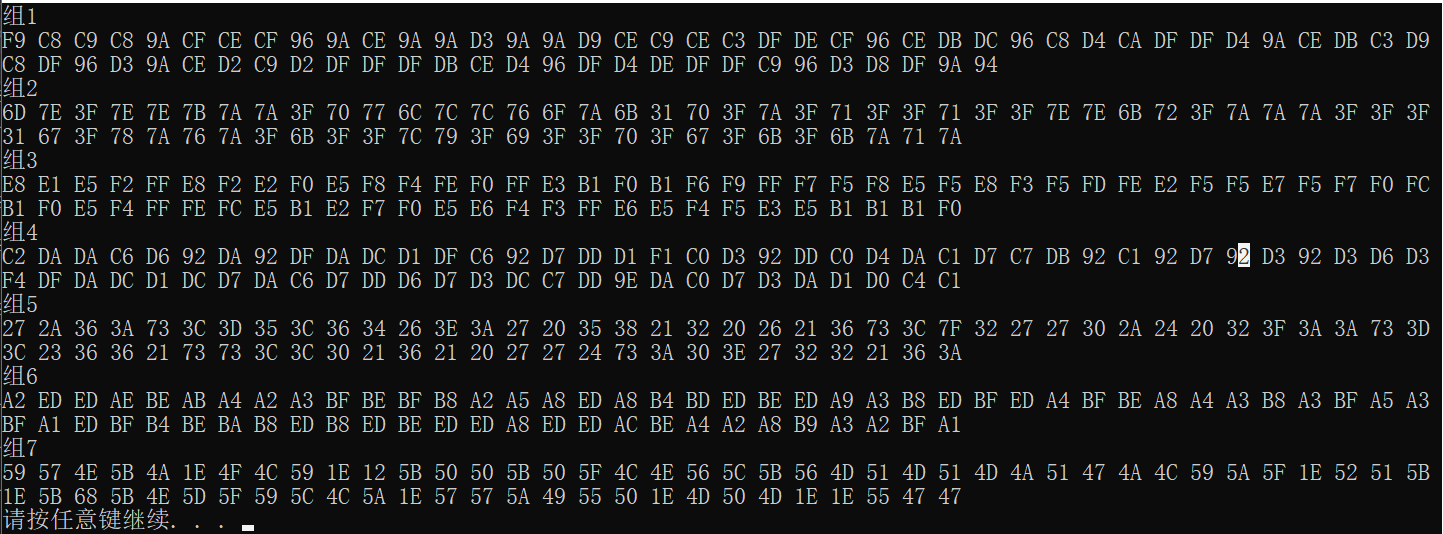




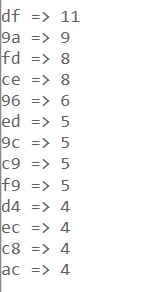
分别对每组做词频分析，计算可知每7组取时频率方差远大于其他几组，故密钥长度为7。

将密文分成7组代码及运行结果如下





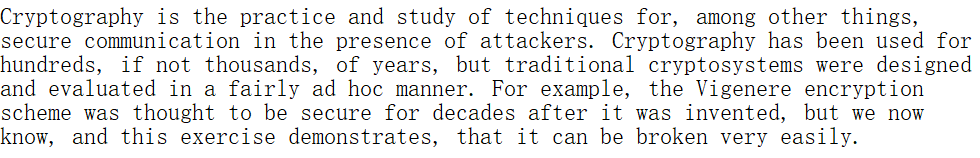
第一组词频分析如下



由于e的单字频率最高，当0xDF为e的密文时，将0xDF与e的十六进制ASCII码0x65按位异或，得可能得密钥0xBA，再将0xBA与其他密文异或，结果均在可见范围内。如果不在

可见范围内则依次尝试或尝试空格与逗号字符。

用同样的方式计算出7个密钥分别为0xBA、0x1F、0x91、0xB2、0x53、0xCD、0x3E，进而破解出得明文为



一次一密：

*BB3A65F6F0034FA957F6A767699CE7FABA855AFB4F2B520AEAD612944A801E*

*BA7F24F2A35357A05CB8A16762C5A6AAAC924AE6447F0608A3D11388569A1E*

*A67261BBB30651BA5CF6BA297ED0E7B4E9894AA95E300247F0C0028F409A1E*

*A57261F5F0004BA74CF4AA2979D9A6B7AC854DA95E305203EC8515954C9D0F*

*BB3A70F3B91D48E84DF0AB702ECFEEB5BC8C5DA94C301E0BECD241954C831E*

*A6726DE8F01A50E849EDBC6C7C9CF2B2A88E19FD423E0647ECCB04DD4C9D1E*

*BC7570BBBF1D46E85AF9AA6C7A9CEFA9E9825CFD5E3A0047F7CD009305A71E*

先观察找到某两奇数位按位与可以出现01形式，即为空格位置，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，那么一方面，可以通过明文异或和密文异或结果相同和空格ASCII码为0x20得出7F明文ASCII值为0x65，即为e，第三、四、六句中72为h；另一方面由于每条密文的密钥均相同，那么每条密文中的同位置的3A均为空格，故第五句第二个字符也为空格。

第一句中F与第二句中A异或前两位为01，假设F0代表空格则A3存在可见结果为s……

用这种方法和一些单词和固定搭配可逐渐测试出每一句话的内容。

解得明文如下：

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.