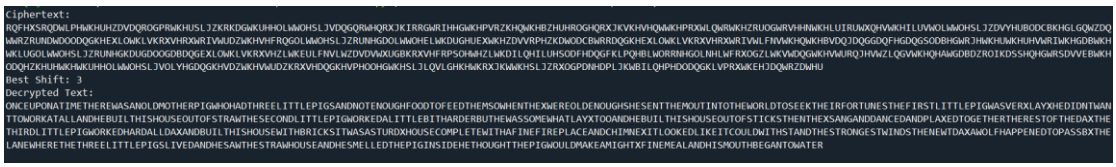
Q1: break_by_frequecy_question

实验内容：

关键思路在于英文的每个字母在文章中的频率分布是不均匀的，因此可以看密文中哪个字母的出现频率最高，与平常英文中频率最高的字母进行比对，然后确定移位的数值。比较的具体方法在于计算两个向量的余弦值，值越大，两个向量的相似度越大，越有可能找到移位的数值。

结果：移位数值为 3



Q2: break_vigenere_question

实验内容：

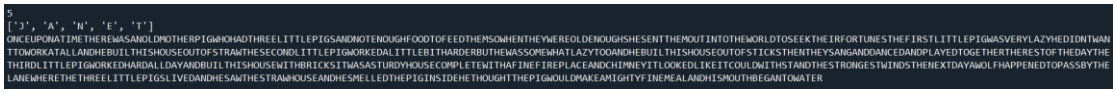
首先确认密匙长度，假设我们使用维吉尼亚密码加密的密文串为 y=y1y2…yn。将串 y 分割为 m 个长度相等的子串 y1y2…ym，这样可以以列的形式写出密文，组成一个 m x (n/m) 矩阵。矩阵的每一行对应于子串 yi。

如果 y1y2…ym 按上述方法构造，且 m 是实际上的密钥长度，那么每一个子串的重合指数都大约是 0.065. 如果 m 不是实际的密钥字长度，那么子串 yi 看起来就更为随机，因为它们是通过不同密钥以移位加密方式获得的。对一个完全随机的串，其重合指数为：0.038。

确定完密钥长度 m 后，我们就可以把密文分为 m 个子串 y1y2…ym ，现在每个子串就相当于一个移位密码的密文，通过使用移位密码的密文分析方法，逐个确定密钥。

结果：

维吉尼亚密码长度为 5，为“JANET”

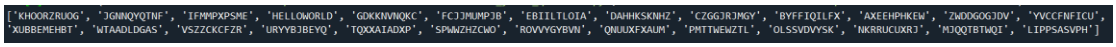


Q3: brute_force_question

实验内容：

纯暴力破解，分别将移位数值为 0 到 25 的结果进行输出

结果：移位数值为 3，明文为”HELLOWORLD”

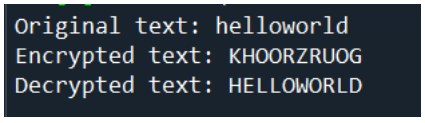


Q4: caesar_question

实验内容：

已知凯撒密码的移位数值为 3，则将大写后的密文的数值移动三位即可

结果：“HELLOWORLD”



Q5: vigenere_question

实验内容：

已知维吉尼亚密码的密钥为“KEY”，故将密文每三个分为一行，由于”K”、”E”、”Y”和”A”的 ACSII 码值分别相差 11，5，25，故每列分别移位 11，5，25 位即可

结果：“HELLOWORLD”

```
Plaintext: HELLOWORLD
Encrypted: EVWIFHLIWA
Decrypted: HELLOWORLD
```