

## 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

```
ZpHtX5RQ0MLP8hK4H2VDVQDGRBKHU5LJZKRKDGKqB8H0LMOHSLJVQDQqBqHQR3C1KRGARH7HGMqKHPVR2H2KqKH82H10HQRHQR3JKVqHVMqKHPR0LQRMKH2ZUUGRqH9B8WkHULR1KqXqVWkH1LUV0LMOHSLJZDVYHUBDQCBKHLGQMZQD
WLR2ZRUHMD00QDQDQqH1EXKWLKVRKHqR9LVMJWZKHqH7RQ0GLMOHSLJZRUH0DLM0HLEKLMQDQqH2KMH2ZVVRP2H0QDCEBMR8QDQqH1EXKWLKVRKHV9W1LFLVW0HqKHQV8VDQDQDQDGH0QDQSB0H8R7HAKH3KqH9V1H7VQDGH0BKH
KILUG0LMOHSLJZRUH0KqH2QDQDQqH0GDLKEXKWLKVRKH2W0LMD0FLNVLZVD0W0XKRGH9V7RPS0AH0L1QHL1UHQSO0DQGLP1KBLWRR0R9H0L1KHLR0XG1LZK0H0Q0H0V4HJ0R1ZK0D1Q0VqH0KH0H0DZ0R1K0D5SHG9H8R0V0D0V0BKH
QDQGH0KqH0H0H0H0LMOHSLJZV0LVDQDGH0V0Z0HqHJW0ZKRXV0H0GqH9V7H00H0KHL5L1QV1GHKqH0K0R0K0M0H5L1ZRX0QD0H0D1J0K0B1LQHP0DQDQGLP1KVR0KqH2DQWRZ0H
Dec: Shift: 3
Decrypted Text:
0K1CEP0AT1HE THE REBMSAN0MD0P0T0G0H04H0D1E1LTP1E5GAND0T0ENQ0H00F00T0E0P0S0M0H0E0X0R0E0LD00H0G0H5E0S0T0P0UT0INT0H0W0R0D0SE0K0ET0R0F0UR0T0E0S0T0F0R0ST1LTP1EPTG0M0K0R1AY0H0D0E0
T0N0K0AT1L0ND0B0E1TH1SH0U0S00T0D0STR0ATHE0S0C0ND1LTP1E7B0RKE0R0D1LTP1E7B0RDE0B0E0W0S0M0E0H0A1LX0T0D0N0D0H0E1TH1SH0U0S0E0T0ST0CKT0S0H0E0X0S0AND0C0ND0P0A0X0D0ET0H0R0S0E0T0F0D0E0T0H0D0E
T0H0R0D1LTP1E7B0RKE0R0D0L0X0D00ND0B1TH1SH0U0S0T1H0R0CK0S1T0S0M0S0T0UR0D0H0C0M0P0L0E1T0H0T0F0R0E0P0L0C0D0H0I0N0E0K1L00K0E1L0C0UL0D1T0S0T0D0E0T0R0G0S0T0ND0S0H0E0N0D0X0W0L0F0H0P0P0E0T0O0P00S0X0T0E
L0ND0H0E0R0E0T0R0E1LTP1E5G0LVD0N0S0S0H0E0T0R00H00E0D0E0S0M0E0L0LTP1E0G1N0D0E0T0H0U0T0H0E0P0G1N0D0M0K0E0A0N0T0H0E0A0N0D0S0H0E0T0B0E0A0N0T0E0
```

## Q2: break\_vigenere\_question

实验内容:

首先确认密钥长度，假设我们使用维吉尼亚密码加密的密文串为  $y=y_1y_2\cdots y_n$ 。将串  $y$  分割为  $m$  个长度相等的子串  $y_1y_2\cdots y_m$ ，这样可以以列的形式写出密文，组成一个  $m \times (n/m)$  矩阵。矩阵的每一行对应于子串  $y_i$ 。

如果  $y_1y_2\cdots y_m$  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  $y_i$  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  $y_1y_2\cdots y_m$ , 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”

5  
 ['J', 'A', 'N', 'E', 'T']  
 ONCEUPONATIMETHEREWASANOLDMOTHERIGHOHADTHREELITTLEPISANDNOTENOUGHFOODTOFEEDTHEMSOMWHENTHEYWEROLDENOUGHSHESENTTHEMOUTINTOWHERLORDSTOSEEKTHEIRFORTUNESTHEFIRSTLITTLEPISGASVERYLAZYHEDIDNTWANTTOPURSUATLAUNCHBUTTHISHOUSEOUTSTRAHESSECONDLITTLEPISGORKEDALITTLEBITTHARDBUTTHEWASSOMETHALAZYTOANDHEBUILTTHISHOUSEOUTOFSTICKSTHENTHEYANGANDONCEADANPLAYEDTOGETHERTHERESTOFTHEDAYTHETHIRDLITTLEPISGORKEDHARDALLDAYANDBUILTTHISHOUSEWITHBRICKSITWASASTURDYHOUSECOMPLETETHATINFEETREPLACEANDCHIMNEYITLOOKEDLIKEITCOULDN'TSTANDTHATSTANDSTRONGESTINDSTHEXTDAYAWOLFAPPEAREDTOPASSBYTHELANEWHEREHETHREELITTLEPISLIVEDANDSANTHESTRAMHOUSEANDHESMELLEDTHEPISINDEHETHOUGHTTHEPISGULDMAKEANIGHTYINEMEALANDHISMOUTHBEGANTOGATE

### 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"

```
[ 'KHOORZRUG', 'JGHNQYQTNF', 'TFMPXPSPME', 'HELLOWORLD', 'GOKKNVQKC', 'FCJHUMPJB', 'EBIILTLOIA', 'DAHHSKSHZ', 'CZGGJRJMGY', 'BYFFIQLFX', 'AXEEHPHKEW', 'ZWDDGOGJDV', 'YVCCFNFCU', 'XUBBEMEBHT', 'WTAADLDGAS', 'VSZCKCFZR', 'URYBYBEOY', 'TQXXAIXDP', 'SPWZHXCWO', 'ROVYGYBVN', 'QNUUXFXAUM', 'PMTWETWZL', 'OLSSVDVYSK', 'NKRRCUXR', 'MJQOTBTWQI', 'LIPPSASVPH' ]
```

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”

```
Original text: helloworld
Encrypted text: KHOORZRUOG
Decrypted text: 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
```