现代密码学第一次大作业

计62 李源隆

1.5

使用程序对秘钥进行26次穷举的结果：



肉眼观察得出合理的明文为：

LOOKUPINTHEAIRITSABIRDITSAPLANEITSSUPERMAN

人工可断句为：

Look up in the air. It’s a bird. It’s a plane. It’s superman.

1.16

(a)

逆置换为：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| x | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| π-1(x) | 2 | 4 | 6 | 1 | 8 | 3 | 5 | 7 |

(b)

明文：

ETEGENLMDNTNEOORDAHATECOESAHLRMI

分为8个字母一组：

ETEGENLM | DNTNEOOR | DAHATECO | ESAHLRMI

使用逆置换进行替换：



结果为：

GENTLEME | NDONOTRE | ADEACHOT | HERSMAIL

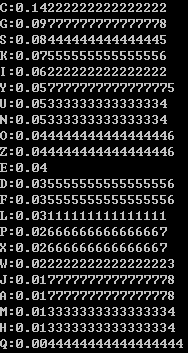
人工断句为：

Gentlemen don’t read each other’s mail.

1.21

(a)

对密文进行字符频率统计后得到结果：



可猜测C对应的字母是e

又由F对应的字母是w

且文中大量出现单词FZCCN，可猜测其为wheel，并得出对应(Z,h),(N,l)

又三元组UZC在密文中多次出现，可猜测对应(U,T)

根据如此多次猜测后可得出明文：

I may not be able to grow flowers, but my garden produces just as many dead leaves, old over shoes, peices of rope and bushels of dead grass as anybody and today I bought a wheel barrow to help in clearing it up. I have always loved and respected the wheel barrow. It is the one-wheel vehicle of which I am perfect master.

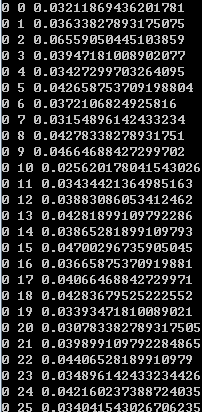
(b)

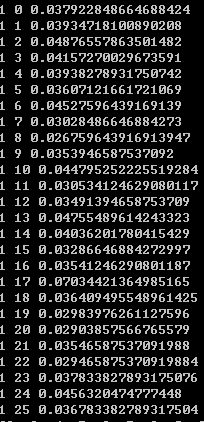
对维吉尼亚密码使用Kasiski测试法。

枚举发现子串HJV出现了五次，每次之间的字母间隔为18,156,210,222，它们的最大公因子为6。

可猜测密钥长度为6（如果长度是6的因子，可认为密钥是具有循环节的字符串）

枚举i从0到5，求使得Mg最接近0.65的g。（下图给了i=0和1的情况）





可猜测密钥为（2,17,24,15,19,14）

使用其对密文解密得到明文：

I learned how to calculate the amount of paper needed for a room when I was at school. You multiply the square footage of the walls by the cubic contents of the floor and ceiling combined and double it. You then allow half the total for openings such as windows and doors then you allow the other half for matching the pattern. Then you double the whole thing again to give a margin of error and then you order the paper.

(c)

使用英文词频统计可以猜测密文c对应的是明文e

由仿射密码的对应法则是ax+b(mod 26)且需保证a与26互质，故可枚举与26互质的a，并根据上述猜测解方程4a+b=2(mod 26)以得出b，并用(a,b)来进行解密。

当a=19,b=4时，可看出明文有意义：

O Canada terre de nos aieux ton front est ceint defleurons glorieux car ton bras sait porter lepee il sait porter la croix ton histoire est une epopee des plus brillants exploits et ta valeur de foi trempee protegera nos foyers et nos droits

(d)

分别用代换密码和维吉尼亚密码进行尝试，发现维吉尼亚可用

做法与(b)相同，通过发现密钥长度为6，可得到明文为：

I grew up among slow talkers men in particular who dropped words a few at a time like beans in a hill and when I got to Minneapolis where people took a lake wobegon comma to mean the end of a story I couldn’t speack a whole sentence in company and was considered not too briaht so I enrolled in a speech souqse taught by orvilles and the founder of reflexive relaxology a self hypnotic technique that enabled a person to speak up to three hundred wourd per minute.

1.26

(a)

已知m和n时，可直接将密文写成一个n\*m的矩阵，依次取矩阵各列构成明文

(b)

密文总长度为42，求其因子可知(m,n)可能为(2,21), (3,14), (6,7), (7,6), (14,3), (21,2)

可解密得多种明文：

