第二次作业答案

1、使用穷尽密钥搜索方法破译如下利用移位密码加密的密文

BEEAKFYDJXUQYHYJIQRYHTYJIQFBQDUYJIIKFUHCQD

* K=10，明文为：  
  Look up in the air, it’s a bird, it’s a plane, it’s superman.

2、（a）设下列的π是集合{1, 2, … , 8}上的置换：

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

求出逆置换π-1。

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

（b）解密下列使用置换密码加密的密文，密钥是（a）中的置换π。

TGEEMNELNNTDROEOAAHDOETCSHAEIRLM

按8个字母分组，TGEEMNEL NNTDROEO AAHDOETC SHAEIRLM

解密得：GENTLEME NDONOTRE ADEACHOT HERSMAIL

明文为： gentlemen do not read each others mail.

3、（a）代换密码

提示：F解密为w。

Step 1，字母频数统计：

A : 5 B : 0 C : 37 D : 8 E : 12 F : 9 G : 24

H : 5 I : 15 J : 7 K : 18 L : 7 M : 5 N : 13

O : 10 P : 6 Q : 1 R : 0 S : 20 T : 0 U : 14

V : 0 W : 5 X : 7 Y : 15 Z : 13

猜测 S ( e ) = C。

Step 2，考虑双字出现的频率，CG出现7次，猜测G为R,S,N,D,A中的一个，GC没有出现，所以G不是r。G出现24次（0.09），猜测S ( a ) = G。

S出现20次，SC出现较少，猜测S ( o ) = S。

ZC出现7次，Z的频率与h近似，猜测 S ( h ) = Z。

发现wheeN出现3次，猜测S ( l ) = N。

发现Uhe出现2次，猜测 S ( t ) =U。

根据DaYYow，猜测S ( r ) = Y, S (b ) = D。

根据Hlower，猜测S ( f ) = H。

根据Wrow，猜测S ( g ) = W。

根据leaAe，猜测S ( v ) = A。

…

得到明文I may not be able to grow flowers, but my garden produces just as many dead leaves, old overshoes pieces of rope and bushels of dead grass as anybody’s. And today I bought a wheelbarrow to help in clearing it up. I have always loved and respected the wheelbarrow. It is the one wheeled vehicle of which I am perfect master.

（b）维吉尼亚密码

指数重合法

m=1, Ic= 0.043718

m=2, Ic= 0.044151，0.052792

m=3, Ic=0.064296，0.056601，0.056760

m=4, Ic=0.048581，0.054138，0.049036，0.060374

m=5, Ic=0.056661，0.057093，0.047004，0.049677，0.057251

m=6, Ic=0.079101，0.100128，0.066327，0.081633，0.059949，0.089923

确定m=6.

密文分为6组，按每一组根据频率猜测密钥，可知密钥为：CRYPTO

明文为：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）仿射密码

仿射密码：密文=（k1 \*明文 + k2）mod 26

按字频分析，猜测S ( e ) = C，即k1 \*4 + k2 = 2。

由于K1和26互质，尝试与26互质的数，得到

密钥：密文=（明文\*19 + 4）mod 26。明文=（密文 - 4）\* 11 mod26

明文为：

Ô Canada!

Terre de nos aïeux,  
Ton front est ceint de fleurons glorieux!

Car ton bras sait porter l'épée,   
Il sait porter la croix!

Ton histoire est une épopée

Des plus brillants exploits.

Et ta valeur, de foi trempée,

Protégera nos foyers et nos droits.

(d)未知具体密码

Step 1， 计算各字母出现频率：

F:0.046 G:0.043 H:0.043 I:0.043 J:0.032 K:0.035 L:0.062 M:0.056 N:0.013

O:0.019 P:0.021 Q:0.016 R:0.040 S:0.062 T:0.032 U:0.032 V:0.056 W:0.029

X:0.024 Y:0.059 Z:0.019 发现相对于英文字母的频率更加平均，故首先尝试维吉尼亚密码。

Step 2，指数重合法，得到m=6;

将密文分为6组，按单表代换根据字母猜测密钥，得到 THEORY。

明文：

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 speak a whole sentence in company and was considered not too briaht. So I enrolled in a speech couqse taught by orville Sand, the founder of reflexive relaxology, a self hypnotic technique that enabled a person to speak up to three hundred words per minute.