第二次作业

计 21 2012011401 张梦豪

1. 解：look up in the air its a bird its a plane its superman

具体见程序 hw1.cpp。

2. 解：（a）

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

（b）

密文 TGEEMNEL NNTDROEO AAHDOETC SHAEIRLM

解密 gentlemen donot read each others mail

具体见程序 hw2.cpp。

3. （a）

解：统计词频表如下：

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

由词频信息，猜想 S(e)=C;

EMGLOSUDCGDNCUSWYSFHNSFCYKDPUMLWGYICOXYSIPJCKQPKUGKMGOLICGINCG ACKSNISACYKZSCKXECJCKSHYSXCGOIDPKZCNKSHICGIWYGKKGKGOLDSILKGOIUSIGLED SPWZUGFZCCNDGYYSFUSZCNXEOJNCGYEOWEUPXEZGACGNFGLKNSACIGOIYCKXCJUC IUZCFZCCNDGYYSFEUEKUZCSOCFZCCNCIACZEJNCSHFZEJZEGMXCYHCJUMGKUCY

统计 e 前和 e 后一个字母的信息，如下：

ebefore:

A:0 B:0 C:2 D:1 E:0 F:3 G:2 H:1 I:3 J:3 K:3 L:1 M:1 N:0 O:0 P:1 Q:0 R:0 S:6 T:0 U:3 V:0 W:0 X:1 Y:2 Z:4

eafter:

A:5 B:0 C:3 D:1 E:1 F:1 G:0 H:1 I:3 J:2 K:0 L:0 M:0 N:5 O:1 P:0 Q:0 R:0 S:1 T:0 U:2 V:0 W:0 X:3 Y:1 Z:7

由于 er 和 re 出现的频率都很高，故猜想 S(r)=Y。由于 the 在文章中一般频率较高，结合密文中 C 的前两个词，统计在信息如下：

UDC DNC SFC YIC PJC LIC INC GAC SAC ZSC XEC CJC SXC KZC HIC FZC ZCC SZC JNC GAC SAC IYC KXC JUC UZC FZC ZCC UZC SOC FZC ZCC CNC IAC JNC MXC YHC KUC

猜想 S(t)=U,S(h)=Z;

在结合词频信息进行大量猜想和尝试，试图不断修改密码表（类似模拟退火的思路），最后得到的密钥表如下：

int jiemi[26]={'v'-97,'x'-97,'e'-97,'b'-97,'i'-97,

'w'-97,'a'-97,'f'-97,'d'-97,'c'-97,
's'-97,'y'-97,'m'-97,'l'-97,'n'-97,
'u'-97,'j'-97,'k'-97,'o'-97,'z'-97,
't'-97,'q'-97,'g'-97,'p'-97,'r'-97,
'h'-97};

解密后的明文如下：

i may not be able to grow flowers but my garden produces just as many dead leaves old over shoes pieces of rope and bushels of dead grass as anybody s 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 wheeled vehicle of which i am perfect master

具体见程序 hw3a.cpp。

（b）

KCCPKBGUFDPHQTYAVINRRTMVGRKDNBVFDETDGILTXRGUDDKOTFMBPVGEGLTGCKQRACQCWDNAWCRXIZAKFTLEWRPTYCQKYVXCHKFTPONCQQRHJVAJUWETMCMSPKQDYHJVDAHCTRLSVSKCGCZQQDZXGSFRLSWCWSJTBHAFSIASPRJAHKJRJUMVGKMITZHFPDISPZLVLGWTFPLKKEBDPGCEBSHCTJRWXBAFSPEZQNRWXCVYCGAONWDDKACKAWBBIKFTIOVKCGGHJVLNHIFFSQESVYCLACNVRWBBIREPBBVFEXOSCDYGZWPFDTKFQIYCWHJVLNHIQIBTKHJVNPIST

- 密钥长度测算：设置不同的密钥长度（d），从 d=1：10，计算不同的 d 下的字母重合次数，确定 d 的具体数值，我在这里使用的方法并不严格，严格的话可以使用重合指数进行计算。
- 密钥中各字符之间的相对位移的确定。根据确定好了的密钥长度 d，分别计算各个字符不同相对位移下的重合指数，并将结果与 0.065 比较，从而确定各字符之间的相对位移。
- 解密。

解密后的明文如下：

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

具体见代码 hw3b.cpp，可以使用《重合指数计算.cpp》进行密钥长度的计算和验证。

（3）

KQEREJEBCPPCJCRKIEACUZBKRVPKRBCIBQCARBJCVFCUPKRIOFKPACUZQEPBKRXPEIIE

ABDKPBCPFCDCCAFIEABDKPBCPFEQPKAZBKRHAIBKAPCCIBURCCDKDCCJCIDFUIXPAFFERBICZDFKABICBBENEFCUPJCVKABPCYDCCDPKBCOCPERKIVKSCPICBRKIJPKABI

仿射密码的加密函数是$e(x) = ax + b \pmod m$，其中

- a和m互质。
- m是字母的数目。

解码函数是$d(x) = a^{-1}(x - b) \pmod m$，其中$a^{-1}$是$a$在$\mathbb{Z}_m$群的乘法逆元。

密钥空间 = (a 可以取的值)×(b 可以取的值)= 12 ×26 = 312，所以可以采取枚举密钥的思路一个个进行尝试，那么如何判断枚举的结果是否符合题意呢，由于是英语语言，我在这里采取重合指数法进行判断，将计算出的重合指数和 0.065 进行比较判断，从而解得相应的值。

解密后的明文如下：

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

网上查了一下，这个居然是加拿大国歌，坑死我了，很早就破解出来了，一直以为这个不是英语！

具体见 hw3c.cpp。

（4）

不妨用维吉尼亚密码尝试一下：

可以复用（2）中的程序，发现密钥长度为 6，再尝试求密钥，解密，成功！

解密后的明文如下：

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 orvilles and the founder of reflexive relaxology a self hypnotic technique that enabled a person to speak up to three hundred words per minute

具体见 hw3d.cpp，密钥长度可以使用《重合指数计算.cpp》进行计算和验证。