实验一古典密码算法及攻击方法

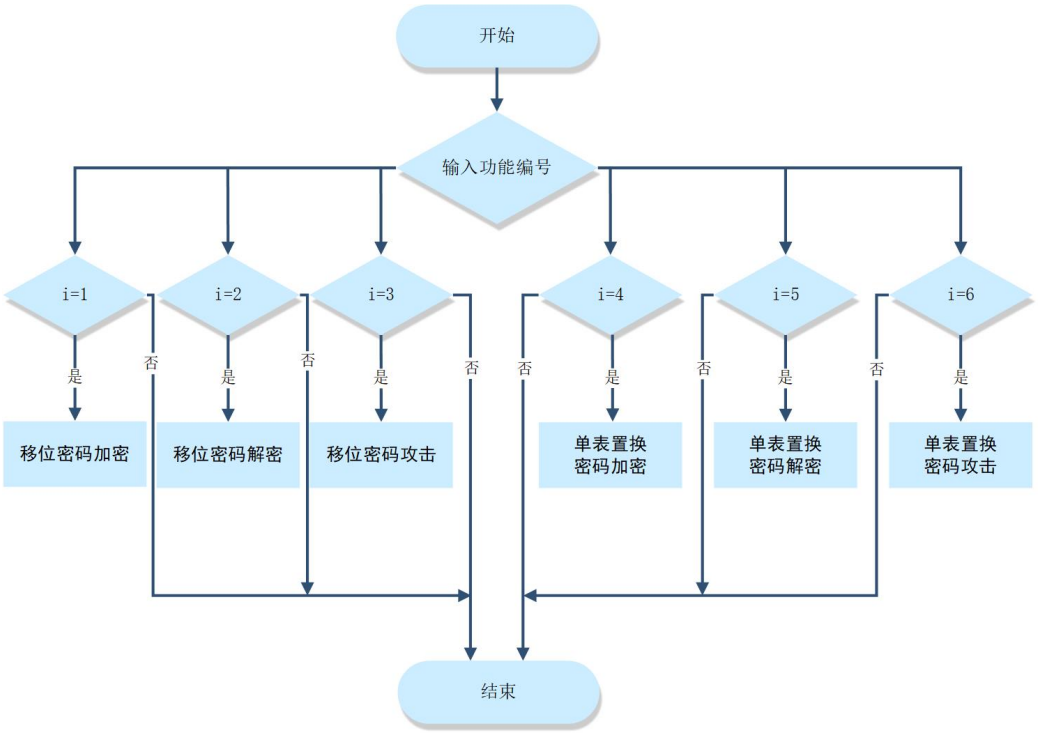
摘要

通过 C ++编程实现移位密码和单表置换密码算法，加深对经典密码体制的了解。并通过对这两种密码实施攻击，了解对古典密码体制的攻击方法。

目录

1 流程图

整体流程图如下：



2 移位密码

2.1 实验原理

移位密码：将英文字母向前或向后移动一个固定位置。例如向后移动 3 个位置，即对字母表作置换（不分大小写）。

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

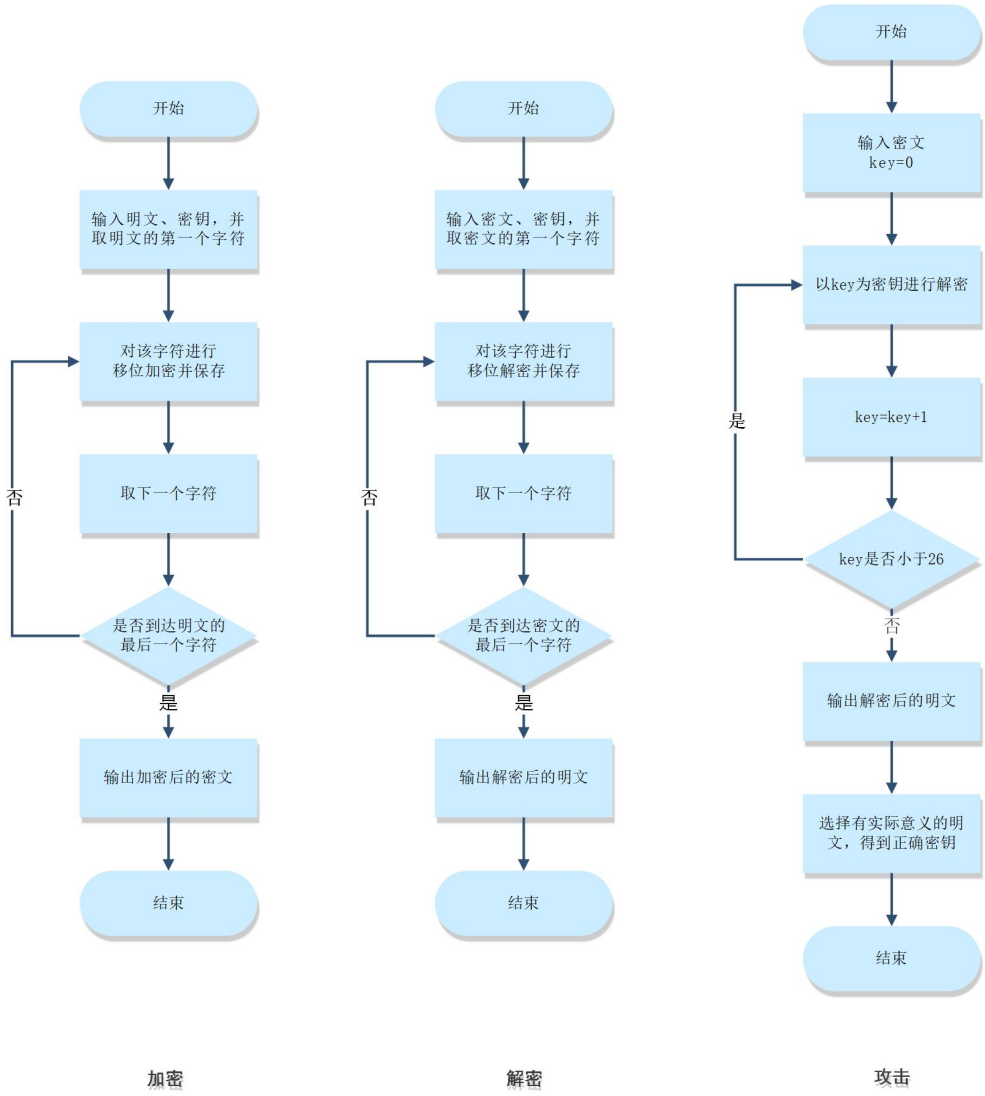
设明文为：public keys, 则经过以上置换就变成了：sxeolf nhbv。如果将 26 个英文字母进行编码：A→0，B→1，…，Z→25，则以上加密过程可简单地写成：

明文：m = $m_1 m_2 \cdots m_i \cdots$, 则有

密文：c=$c_1 c_2 \cdots c_i \cdots$, 其中 c_i=(m_i+key mod26)，i = 1，2，…。

2.2 算法流程图

移位密码流程图如下：



加密　　解密　　攻击

2.3　移位密码攻击

移位密码是一种最简单的密码，其有效密钥空间大小为 25。因此，很容易用穷举的方法攻破。穷举密钥攻击是指攻击者对可能的密钥的穷举，也就是用所有可能的密钥解密密文，直到得到有意义的明文，由此确定出正确的密钥和明文的攻击方法。对移位密码进行穷举密钥攻击，最多只要试译 25 次就可以得到正确的密钥和明文。

2.4　实验结果

(一) 移位密码加密：

```
----------------------移位密码加密----------------------

请输入要进行加密的明文（不分大小写）：
public KEys
明文为：
public keys
请输入密钥：
3
加密后的密文为
sxeolf nhbv
```

(二) 移位密码解密：

```
------------------------移位密码解密------------------------

请输入要进行解密的密文（不分大小写）：
sxeolf nhbv
要解密的密文为：
sxeolf nhbv
请输入密钥：
3
解密后的明文为
public keys
```

(三) 移位密码攻击：

```
------------------------移位密码攻击------------------------

请输入要进行攻击的密文（不分大小写）：
sxeolf NhbV
要进行攻击的密文为
sxeolf nhbv
当密钥为1时，解密出的明文为：rwdnke mgau
当密钥为2时，解密出的明文为：qvcmjd lfzt
当密钥为3时，解密出的明文为：public keys
当密钥为4时，解密出的明文为：otakhb jdxr
当密钥为5时，解密出的明文为：nszjga icwq
当密钥为6时，解密出的明文为：mryifz hbvp
当密钥为7时，解密出的明文为：lqxhey gauo
当密钥为8时，解密出的明文为：kpwgdx fztn
当密钥为9时，解密出的明文为：jovfcw eysm
当密钥为10时，解密出的明文为：inuebv dxrl
当密钥为11时，解密出的明文为：hmtdau cwqk
当密钥为12时，解密出的明文为：glsczt bvpj
当密钥为13时，解密出的明文为：fkrbys auoi
当密钥为14时，解密出的明文为：ejqaxr ztnh
当密钥为15时，解密出的明文为：dipzwq ysmg
当密钥为16时，解密出的明文为：choyvp xrlf
当密钥为17时，解密出的明文为：bgnxuo wqke
当密钥为18时，解密出的明文为：afmwtn vpjd
当密钥为19时，解密出的明文为：zelvsm uoic
当密钥为20时，解密出的明文为：ydkurl tnhb
当密钥为21时，解密出的明文为：xcjtqk smga
当密钥为22时，解密出的明文为：wbispj rlfz
当密钥为23时，解密出的明文为：vahroi qkey
当密钥为24时，解密出的明文为：uzgqnh pjdx
当密钥为25时，解密出的明文为：tyfpmg oicw
从中选择最合适的密钥：
3
您选择的结果为：public keys
```

3 单表置换密码

3.1 实验原理

单表置换密码就是根据字母表的置换对明文进行变换的方法，例如，给定置换:

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
H K W T X Y S G B P Q E J A Z M L N O F C I D V U R

明文：public keys, 则有密文：mckebw qxuo。

单表置换实现的一个关键问题是关于置换表的构造。置换表的构造可以有各种不同的途径，主要考虑的是记忆的方便。如使用一个短语或句子，删去其中的重复部分，作为置换表的前面的部分，然后把没有用到的字母按字母表的顺序依次放入置换表中。

3.2 算法流程图

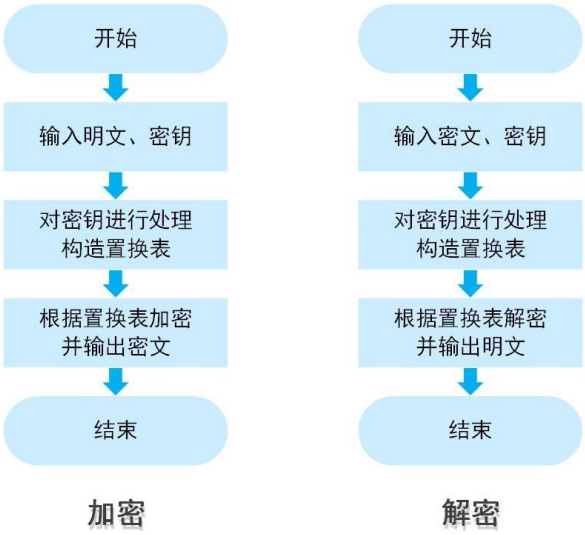


图 1: 单表置换密码流程图

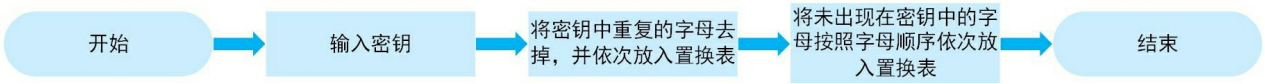


图 2: 置换表构造

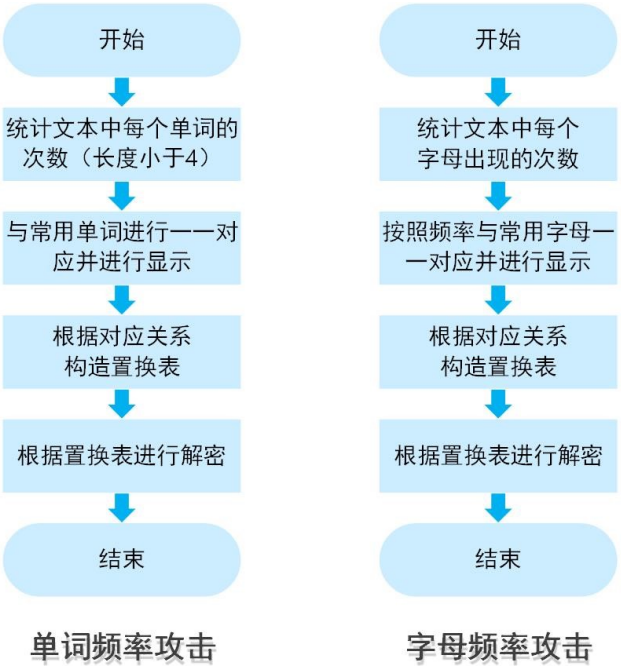


图 3: 单表置换密码攻击流程图

3.3 单表置换密码攻击

在单表置换密码中，由于置换表字母组合方式有 26！种，约为 4.03×10^{26}。

所以采用穷举密钥的方法不是一种最有效的方法。对单表置换密码最有效的攻击方法是利用自然语言的使用频率：单字母、双字母组/三字母组、短语、词头/词尾等，这里仅考虑英文的情况。英文的一些显著特征如下:

短单词 (small words)：在英文中只有很少几个非常短的单词。因此，如果在一个加密的文本中可以确定单词的范围，那么就能得出明显的结果。一个字母的单词只有 a 和 I。如果不计单词的缩写，在从电子邮件中选取 500k 字节的样本中，只有两个字母的单词仅出现 35 次，而两个字母的所有组合为 $26\times26 = 676$ 种。而且，还是在那个样本中，只有三个字母的单词出现 196 次，而三个字母的所有组合为 $26\times26\times26 = 17576$ 种。

常用单词 (common words): 再次分析 500k 字节的样本，总共有 5000 多个不同的单词出现。在这里，9 个最常用的单词出现的总次数占总单词数的 21%，20 个最常用的单词出现的总次数占总单词数的 30%，104 个最常用的单词占 50%，247 个最常用的单词占 60%。样本中最常用的 9 个单词占总词数的百分比为：

the-4.65 to-3.02 of-2.61 I-2.2 a-1.95
and-1.82 is-1.68 that-1.62 in-1.57

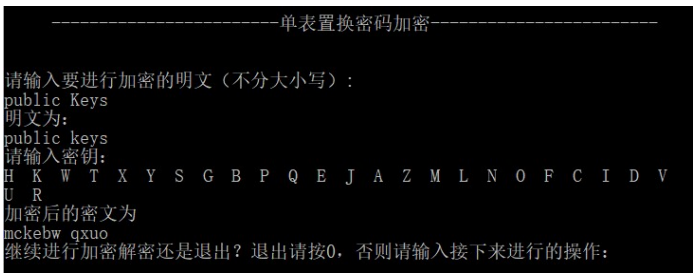
字母频率 (character frequency): 在 1M 字节旧的电子文本中，对字母”A”到“Z”（忽略大小写）分别进行统计。发现近似频率（以百分比表示）：

e-11.67 t-9.53 o-8.22 i-7.81 a-7.73 n-6.71 s-6.55 r-5.97 h-4.52
l-4.3 d-3.24 u-3.21 c-3.06 m-2.8 p-2.34 y-2.22 f-2.14 g-2.00
w-1.69 b-1.58 v-1.03 k-0.79 x-0.30 j-0.23 q-0.12 z-0.09

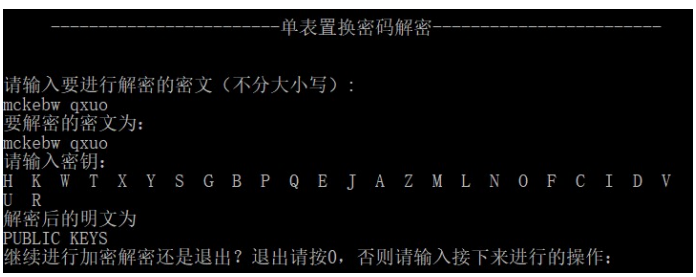
从该表中可以看出，最常用的单字母英文是 e 和 t，其他字母使用频率相对来说就小得多。这样，攻击一个单表置换密码，首先统计密文中最常出现的字母，并据此猜出两个最常用的字母，并根据英文统计的其他特征（如字母组合等）进行试译。

3.4 实验结果

(一) 移位密码加密：

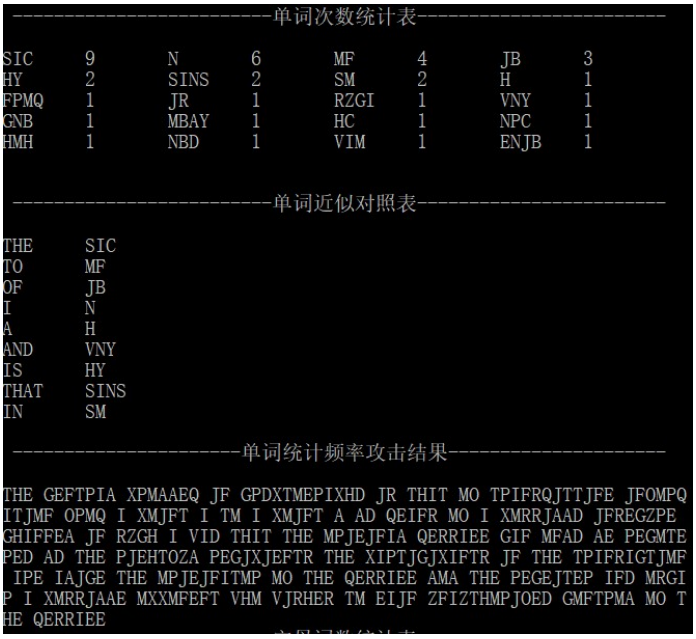


(二) 移位密码解密：

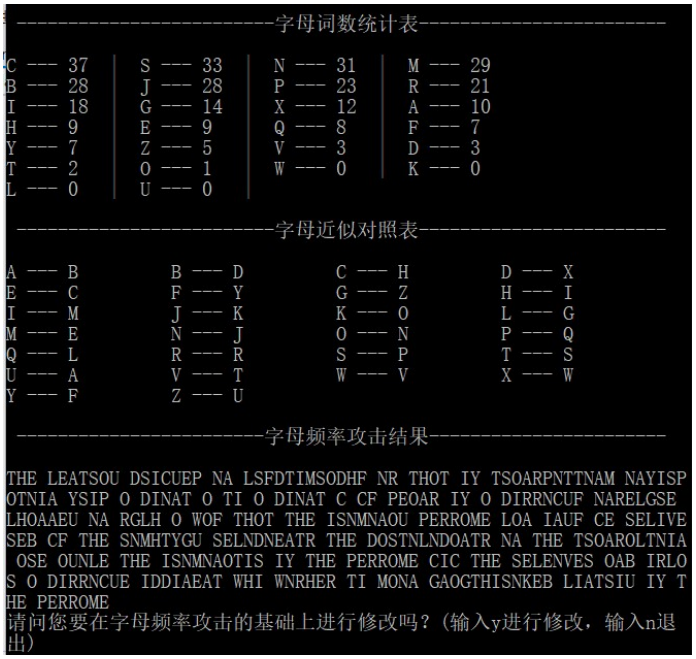


(三) 移位密码攻击：

1. 单词频率攻击：



2. 字母频率攻击：



3. 在字母频率攻击的基础上继续攻击：

(1) 观察到明文中的第一行出现了 thot 一词，依据常用单词，将其修改为 that。

```
请输入要修改的置换表中对应关系的个数
1
o a

 ----------------------------置换表----------------------------

A --- N     |    B --- D     |    C --- H     |    D --- X
E --- C     |    F --- Y     |    G --- Z     |    H --- I
I --- M     |    J --- K     |    K --- O     |    L --- G
M --- E     |    N --- J     |    O --- B     |    P --- Q
Q --- L     |    R --- R     |    S --- P     |    T --- S
U --- A     |    V --- T     |    W --- V     |    X --- W
Y --- F     |    Z --- U
THE LEOTSAU DSICUEP NO LSFDTIMSADHF NR THAT IY TSAORPNTTNOM NOYISP
ATNIO YSIP A DINOT A TI A DINOT C CF PEAOR IY A DIRRNCUF NORELGSE
LHAOOEU NO RGLH A WAF THAT THE ISNMNOAU PERRAME LAO IOUF CE SELIVE
SEB CF THE SNMHTYGU SELNDNEOTR THE DASTNLNDAOTR NO THE TSAORALTNIO
 ASE AUNLE THE ISNMNOATIS IY THE PERRAME CIC THE SELENVES AOB IRLA
S A DIRRNCUE IDDIOEOT WHI WNRHER TI MANO GOAGTHISNKEB LIOTSIU IY T
HE PERRAME

是否继续进行更改？（输入y继续，输入n退出）
```

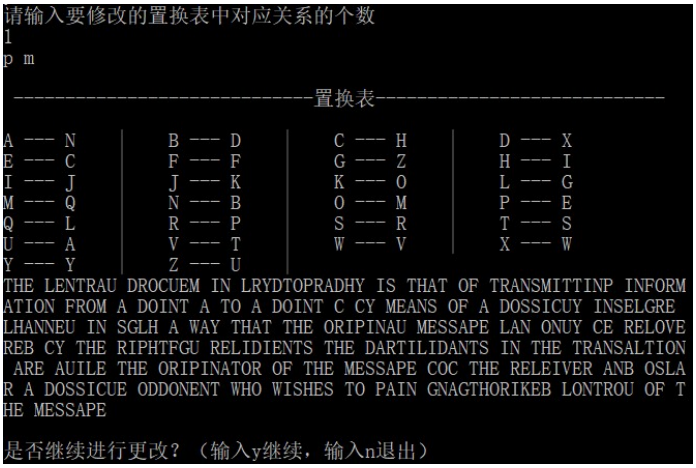
(2) 观察到明文中的第一行出现了 iy 一词，依据常用单词，将其修改为 of。

```
请输入要修改的置换表中对应关系的个数
2
i o y f

 ----------------------------置换表----------------------------

A --- N     |    B --- D     |    C --- H     |    D --- X
E --- C     |    F --- F     |    G --- Z     |    H --- I
I --- B     |    J --- K     |    K --- O     |    L --- G
M --- E     |    N --- J     |    O --- M     |    P --- Q
Q --- L     |    R --- R     |    S --- P     |    T --- S
U --- A     |    V --- T     |    W --- V     |    X --- W
Y --- Y     |    Z --- U
THE LEITSAU DSOCUEP NI LSYDTOMSADHY NR THAT OF TSAIRPNTTNIM NIFOSP
ATNOI FSOP A DONIT A TO A DONIT C CY PEAIR OF A DORRNCUY NIRELGSE
LHAIIEU NI RGLH A WAY THAT THE OSNMNIAU PERRAME LAI OIUY CE SELOVE
SEB CY THE SNMHTFGU SELNDNEITR THE DASTNLNDAITR NI THE TSAIRALTNOI
 ASE AUNLE THE OSNMNIATOS OF THE PERRAME COC THE SELENVES AIB ORLA
S A DORRNCUE ODDOIEIT WHO WNRHER TO MANI GIAGTHOSNKEB LOITSOU OF T
HE PERRAME

是否继续进行更改？（输入y继续，输入n退出）
```

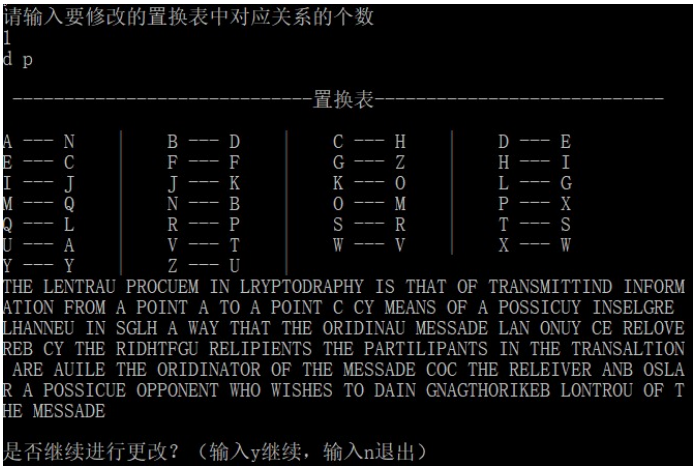
(3) 此时明文中多次出现以 n 开头的双字幕段单词，推测其为 is，所以将 nr 改为 is。

```
请输入要修改的置换表中对应关系的个数
2
n i r s

 ----------------------------置换表----------------------------

A --- N     |    B --- D     |    C --- H     |    D --- X
E --- C     |    F --- F     |    G --- Z     |    H --- I
I --- J     |    J --- K     |    K --- O     |    L --- G
M --- E     |    N --- B     |    O --- M     |    P --- Q
Q --- L     |    R --- P     |    S --- R     |    T --- S
U --- A     |    V --- T     |    W --- V     |    X --- W
Y --- Y     |    Z --- U
THE LENTRAU DROCUEP IN LRYDTOMRADHY IS THAT OF TRANSPITTINM INFORP
ATION FROP A DOINT A TO A DOINT C CY PEANS OF A DOSSICUY INSELGRE
LHANNEU IN SGLH A WAY THAT THE ORIMINAU PESSAME LAN ONUY CE RELOVE
REB CY THE RIMHTFGU RELIDIENTS THE DARTILIDANTS IN THE TRANSALTION
 ARE AUILE THE ORIMINATOR OF THE PESSAME COC THE RELEIVER ANB OSLA
R A DOSSICUE ODDONENT WHO WISHES TO MAIN GNAGTHORIKEB LONTROU OF T
HE PESSAME

是否继续进行更改？（输入y继续，输入n退出）
```

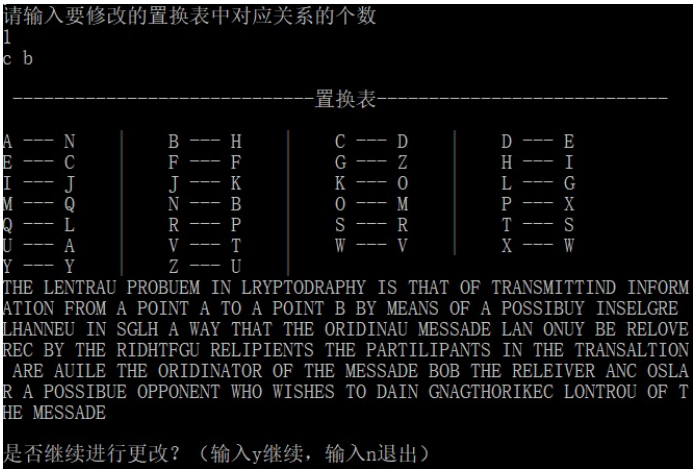
(4) 发现现在的明文中有 frop，推测其为 from，因此，将 p 换为 m。



(5) 发现 doint 一词，根据常用单词将其修改为 point。



(6) 根据“from a point a to a point c”和 cy，推测应该将 c 换成 b。



(7) 存在单词 probuem，推测其为 problem，所以将 u 换成 l。

(8) 存在单词 uentral，推测其为 central，所以将 u 换成 c。

(9) 存在单词 cryptodraphy，推测其为 crytography，所以将 d 换成 g。

(10) 存在单词 insecdre，推测其为 insecure，所以将 d 换成 u。

(11) 存在单词 unauthoriked，推测其为 unauthorized，所以将 k 换成 z。

(12) 最后结果如下：