古典密码算法及攻击方式

1611532 刘一静 信息安全

实验分为两部分：实现移位密码与单表置换密码的加密与攻击方法。

一、移位密码

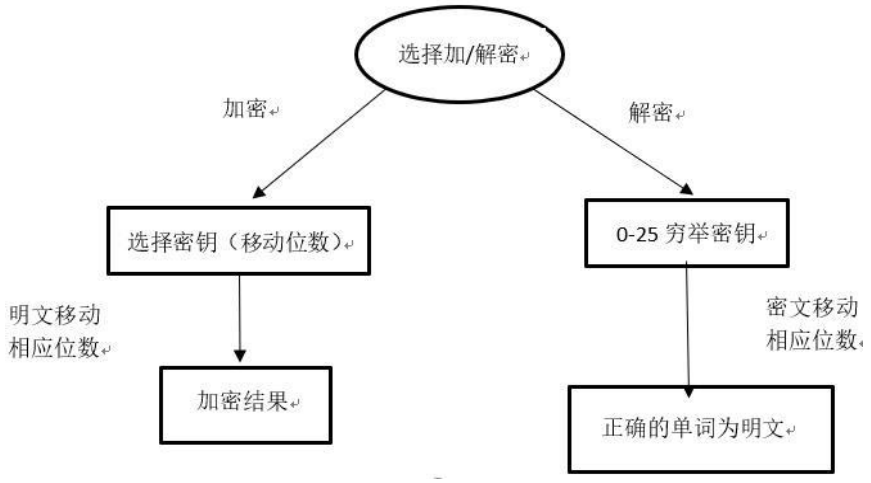
加密过程：

明文：m＝m1m2…mi…，则有

密文：c=c1c2…ci…，其中 ci=(mi+key mod26)，i＝1，2，…。

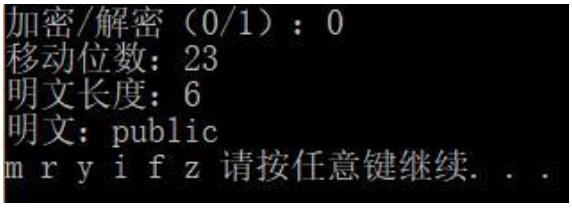
解密方法：穷举密钥攻击（用所有可能的密钥解密密文，直到得到有意义的明文）

流程图：



实现效果：

加密：



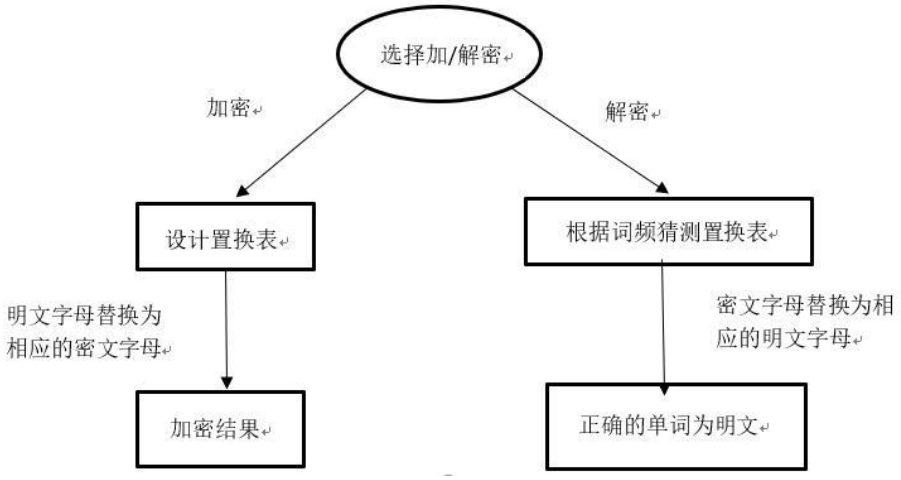
解密：

```
加密/解密（0/1）：1
密文长度：6
密文：m r y i f z
移动位数:0      m r y i f z
移动位数:1      n s z j g a
移动位数:2      o t a k h b
移动位数:3      p u b l i c
移动位数:4      q v c m j d
移动位数:5      r w d n k e
移动位数:6      s x e o l f
移动位数:7      t y f p m g
移动位数:8      u z g q n h
移动位数:9      v a h r o i
移动位数:10     w b i s p j
移动位数:11     x c j t q k
移动位数:12     y d k u r l
移动位数:13     z e l v s m
移动位数:14     a f m w t n
移动位数:15     b g n x u o
移动位数:16     c h o y v p
移动位数:17     d i p z w q
移动位数:18     e j q a x r
移动位数:19     f k r b y s
移动位数:20     g l s c z t
移动位数:21     h m t d a u
移动位数:22     i n u e b v
移动位数:23     j o v f c w
移动位数:24     k p w g d x
移动位数:25     l q x h e y
请按任意键继续. . .
```

二、单表置换密码

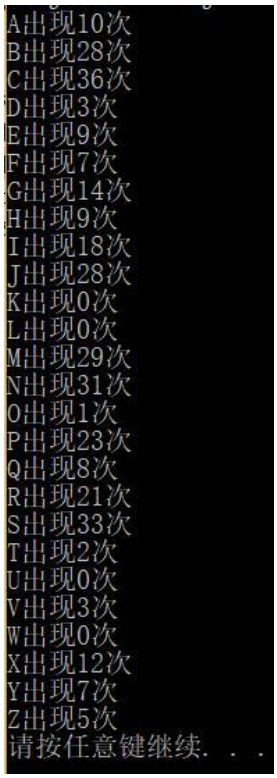
单表置换密码就是根据字母表的置换对明文进行变换的方法。 单表置换实现的一个关键问题是关于置换表的构造。置换表的构造可以有各种不同的途径，主要考虑的是记忆的方便。如使用一个短语或句子，删去其中的重复部分，作为置换表的前面的部分，然后把没有用到的字母按字母表的顺序依次放入置换表中。

流程图：



攻击的实现方式：

首先分析各字母出现次数



根据字母频率建立明文与密文单词的对应关系

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

初步得到的置换表为：

```
A对应明文U出现10次
B对应明文A出现28次
C对应明文E出现36次
D对应明文W出现3次
E对应明文C出现9次
F对应明文Y出现7次
G对应明文L出现14次
H对应明文M出现9次
I对应明文H出现18次
J对应明文N出现28次
K对应明文X出现0次
L对应明文J出现0次
M对应明文I出现29次
N对应明文O出现31次
O对应明文K出现1次
P对应明文S出现23次
Q对应明文P出现8次
R对应明文R出现21次
S对应明文T出现33次
T对应明文V出现2次
U对应明文Q出现0次
V对应明文B出现3次
W对应明文Z出现0次
X对应明文D出现12次
Y对应明文F出现7次
Z对应明文G出现5次
请按任意键继续. . .
```

将密文中的单词替换为通过置换表得到的明文单词，初步解密的结果如下：

```
THE LEATSOU DSIMUEP NA LSFDTICSODHF NR THOT IY TSOARPNTTNAC NAYISPOTNIA YSIP O DINAT O TI O DINAT M MF PEOAR IY O DIRRNM
UF NARELGSE LHOAAEU NA RGLH O BOF THOT THE ISNCNAOU PERROCE LOA IAUF ME SELIVESEW MF THE SNCHTYGU SELNDNEATR THE DOSTNLN
DOATR NA THE TSOAROLTNIA OSE OUNLE THE ISNCNAOTIS IY THE PERROCE MIM THE SELENVES OAW IRLOS O DIRRNMUE IDDIAEAT BHI BNRH
ER TI CONA GAOGTHISNKEW LIATSIU IY THE PERROCE请按任意键继续. . .
```

存在很多错误单词，需要根据语义手动更改置换表进行完善。

1、首先我发现了很多由一个字母 O 组成的单词，根据常用单字母单词，猜测 O 应该为 A，置换表中更改为 N->A。此时解密的结果为：

```
THE LEATSAU DSIMUEP NA LSFDTICSADHF NR THAT IY TSAARPNTTNAC NAYISPATNIA YSIP A DINAT A TI A DINAT
M MF PEAAR IY A DIRRNMUF NARELGSE LHAAAEU NA RGLH A BAF THAT THE ISNCNAAU PERRACE LAA IAUF ME
SELIVESEW MF THE SNCHTYGU SELNDNEATR THE DASTNLNDAATR NA THE TSAARALTNIA ASE AUNLE THE ISNCNAATIS
IY THE PERRACE MIM THE SELENVES AAW IRLAS A DIRRNMUE IDDIAEAT BHI BNRHER TI CANA GAAGTHISNKEW
LIATSIU IY THE PERRACE
```

2、解密出的假明文中双字母单词（括号内为出现次数）：

NA（3），NR（1），IY（4），TI（2），ME（1），MF（1）

根据常用双字母单词的出现频率及字母特征对置换表的对应关系进行修改

to	3.02	of	2.61
is	1.68	in	1.57

猜测 TI 是 TO,IY 是 OF，在置换表中更改 M->I 为 M->O，F->Y 为 F->F。

解密的结果为：

```
THE LEATSAU DSOMUEP NA LSFDTOCSADHF NR THAT OF TSAARPNTTNAC NAFOSPATNOA FSOP A DONAT A TO A DONAT
M MF PEAAR OF A DORRNMUF NARELGSE LHAAAEU NA RGLH A BAF THAT THE OSNCNAAU PERRACE LAA OAUF ME
SELOVESEW MF THE SNCHTFGU SELNDNEATR THE DASTNLNDAATR NA THE TSAARALTNOA ASE AUNLE THE OSNCNAATOS
OF THE PERRACE MOM THE SELENVES AAW ORLAS A DORRNMUE ODDOAEAT BHO BNRHER TO CANA GAAGTHOSNKEW
LOATSOU OF THE PERRACE
```

3、猜测为 is that of 结构，置换表中将 J->N 改为 J->I；R->R 改为 R->S。

解密的结果为：

```
THE LEATSAU DSOMUEP IA LSFDTOCSADHF IS THAT OF TSAASPITTIAC IAFOSPATIOA FSOP A DOIAT A TO A DOIAT
M MF PEAAS OF A DOSSIMUF IASELGSE LHAAAEU IA SGLH A BAF THAT THE OSICIAAU PESSACE LAA OAUF ME
SELOVESEW MF THE SICHTFGU SELIDIEATS THE DASTILIDAATS IA THE TSAASALTIOA ASE AUILE THE OSICIAATOS
OF THE PESSACE MOM THE SELEIVES AAW OSLAS A DOSSIMUE ODDOAEAT BHO BISHES TO CAIA GAAGTHOSIKEW
LOATSOU OF THE PESSACE
```

4、猜测为 from to 结构　置换表中将 P->S 改为 P->R,Q->P 改为 Q->M。

解密的结果为：

```
THE LEATRAU DROMUEM IA LRFDTOCRADHF IS THAT OF TRAASMITTIAC IAFORMATIOA FROM A DOIAT A TO A DOIAT
M MF MEAAS OF A DOSSIMUF IASELGRE LHAAAEU IA SGLH A BAF THAT THE ORICIAAU MESSACE LAA OAUF ME
RELOVEREW MF THE RICHTFGU RELIDIEATS THE DARTILIDAATS IA THE TRAASALTIOA ARE AUILE THE ORICIAATOR
OF THE MESSACE MOM THE RELEIVER AAW OSLAR A DOSSIMUE ODDOAEAT BHO BISHES TO CAIA GAAGTHORIKEW
LOATROU OF THE MESSACE
```

5、猜测 BHO 为 WHO，在置换表中将　V->B 改为 V->W。

解密的结果为：

```
THE LEATRAU DROMUEM IA LRFDTOCRADHF IS THAT OF TRAASMITTIAC IAFORMATIOA FROM A DOIAT A TO A DOIAT
M MF MEAAS OF A DOSSIMUF IASELGRE LHAAAEU IA SGLH A WAF THAT THE ORICIAAU MESSACE LAA OAUF ME
RELOVEREW MF THE RICHTFGU RELIDIEATS THE DARTILIDAATS IA THE TRAASALTIOA ARE AUILE THE ORICIAATOR
OF THE MESSACE MOM THE RELEIVER AAW OSLAR A DOSSIMUE ODDOAEAT WHO WISHES TO CAIA GAAGTHORIKEW
LOATROU OF THE MESSACE
```

6、猜测 MESSACE 为 MESSAGE　，在置换表中将 E->C 改为 E->G。

解密的结果为：

```
THE LEATRAU DROMUEM IA LRFDTOGRADHF IS THAT OF TRAASMITTIAG IAFORMATIOA FROM A DOIAT A TO A DOIAT
M MF MEAAS OF A DOSSIMUF IASELGRE LHAAAEU IA SGLH A WAF THAT THE ORIGIAAU MESSAGE LAA OAUF ME
RELOVEREW MF THE RIGHTFGU RELIDIEATS THE DARTILIDAATS IA THE TRAASALTIOA ARE AUILE THE ORIGIAATOR
OF THE MESSAGE MOM THE RELEIVER AAW OSLAR A DOSSIMUE ODDOAEAT WHO WISHES TO GAIA GAAGTHORIKEW
LOATROU OF THE MESSAGE
```

7、猜测 MEAAS 为 MEANS，在置换表中将 B->A 改为 B->N

解密的结果为：

```
THE LENTRAU DROMUEM IN LRFDTOGRADHF IS THAT OF TRANSMITTING INFORMATION FROM A DOINT A TO A DOINT
M MF MEANS OF A DOSSIMUF INSELGRE LHANNEU IN SGLH A WAF THAT THE ORIGINAU MESSAGE LAN ONUF ME
RELOVEREW MF THE RIGHTFGU RELIDIENTS THE DARTILIDANTS IN THE TRANSALTION ARE AUILE THE ORIGINATOR
OF THE MESSAGE MOM THE RELEIVER ANW OSLAR A DOSSIMUE ODDONENT WHO WISHES TO GAIN GNAGTHORIKEW
LONTROU OF THE MESSAGE
```

8、猜测 DOINT 为 POINT，在置换表中将 X->D 改为 X->P。

解密的结果为：

```
THE LENTRAU PROMUEM IN LRFPTOGRAPHF IS THAT OF TRANSMITTING INFORMATION FROM A POINT A TO A POINT
M MF MEANS OF A POSSIMUF INSELGRE LHANNEU IN SGLH A WAF THAT THE ORIGINAU MESSAGE LAN ONUF ME
RELOVEREW MF THE RIGHTFGU RELIPIENTS THE PARTILIPANTS IN THE TRANSALTION ARE AUILE THE ORIGINATOR
OF THE MESSAGE MOM THE RELEIVER ANW OSLAR A POSSIMUE OPPONENT WHO WISHES TO GAIN GNAGTHORIKEW
LONTROU OF THE MESSAGE
```

9、猜测 LONTROU 为 CONTROL，　在置换表中将 G->L 改为 G->C　A->U 改为 A->L。

解密的结果为：

```
THE CENTRAL PROMLEM IN CRFPTOGRAPHF IS THAT OF TRANSMITTING INFORMATION FROM A POINT A TO A POINT
M MF MEANS OF A POSSIMLF INSECGRE CHANNEL IN SGCH A WAF THAT THE ORIGINAL MESSAGE CAN ONLF ME
RECOVEREW MF THE RIGHTFGL RECIPIENTS THE PARTICIPANTS IN THE TRANSACTION ARE ALICE THE ORIGINATOR
OF THE MESSAGE MOM THE RECEIVER ANW OSCAR A POSSIMLE OPPONENT WHO WISHES TO GAIN GNAGTHORIKEW
CONTROL OF THE MESSAGE
```

10、猜测 PROMLEM 为 PROBLEM，在置换表中将 H->M 改为 H->B。

解密的结果为：

THE CENTRAL PROBLEM IN CRFPTOGRAPHF IS THAT OF TRANSMITTING INFORMATION FROM A POINT A TO A POINT B BF MEANS OF A POSSIBLF INSECGRE CHANNEL IN SGCH A WAF THAT THE ORIGINAL MESSAGE CAN ONLF BE RECOVEREW BF THE RIGHTFGL RECIPIENTS THE PARTICIPANTS IN THE TRANSACTION ARE ALICE THE ORIGINATOR OF THE MESSAGE BOB THE RECEIVER ANW OSCAR A POSSIBLE OPPONENT WHO WISHES TO GAIN GNAGTHORIKEW CONTROL OF THE MESSAGE

11、猜测 POSSIBLF 为 POSSIBLY，在置换表中将 Y->F 改为 Y->Y。

解密的结果为：

THE CENTRAL PROBLEM IN CRYPTOGRAPHY IS THAT OF TRANSMITTING INFORMATION FROM A POINT A TO A POINT B BY MEANS OF A POSSIBLY INSECGRE CHANNEL IN SGCH A WAY THAT THE ORIGINAL MESSAGE CAN ONLY BE RECOVEREW BY THE RIGHTFGL RECIPIENTS THE PARTICIPANTS IN THE TRANSACTION ARE ALICE THE ORIGINATOR OF THE MESSAGE BOB THE RECEIVER ANW OSCAR A POSSIBLE OPPONENT WHO WISHES TO GAIN GNAGTHORIKEW CONTROL OF THE MESSAGE

12、猜测 INSECGRE 为 INSECURE，在置换表中将 Z->G 改为 Z->U。

解密的结果为：

THE CENTRAL PROBLEM IN CRYPTOGRAPHY IS THAT OF TRANSMITTING INFORMATION FROM A POINT A TO A POINT B BY MEANS OF A POSSIBLY INSECURE CHANNEL IN SUCH A WAY THAT THE ORIGINAL MESSAGE CAN ONLY BE RECOVEREW BY THE RIGHTFUL RECIPIENTS THE PARTICIPANTS IN THE TRANSACTION ARE ALICE THE ORIGINATOR OF THE MESSAGE BOB THE RECEIVER ANW OSCAR A POSSIBLE OPPONENT WHO WISHES TO GAIN UNAUTHORIKEW CONTROL OF THE MESSAGE

13、猜测 ANW 为 AND，在置换表中将 D->W 改为 D->D。

得到最终解密结果为：

```
THE CENTRAL PROBLEM IN CRYPTOGRAPHY IS THAT OF TRANSMITTING INFORMATION FROM A POINT A TO A POINT B BY MEANS OF A POSSIB
LY INSECURE CHANNEL IN SUCH A WAY THAT THE ORIGINAL MESSAGE CAN ONLY BE RECOVERED BY THE RIGHTFUL RECIPIENTS THE PARTICI
PANTS IN THE TRANSACTION ARE ALICE THE ORIGINATOR OF THE MESSAGE BOB THE RECEIVER AND OSCAR A POSSIBLE OPPONENT WHO WISH
ES TO GAIN UNAUTHORIKED CONTROL OF THE MESSAGE请按任意键继续. . .
```

THE CENTRAL PROBLEM IN CRYPTOGRAPHY IS THAT OF TRANSMITTING INFORMATION FROM A POINT A TO A POINT B BY MEANS OF A POSSIBLY INSECURE CHANNEL IN SUCH A WAY THAT THE ORIGINAL MESSAGE CAN ONLY BE RECOVERED BY THE RIGHTFUL RECIPIENTS THE PARTICIPANTS IN THE TRANSACTION ARE ALICE THE ORIGINATOR OF THE MESSAGE BOB THE RECEIVER AND OSCAR A POSSIBLE OPPONENT WHO WISHES TO GAIN UNAUTHORIKED CONTROL OF THE MESSAGE

修改之后最终正确的移位表为：（左侧为密文 右侧为明文）

```
A对应明文L出现10次
B对应明文N出现28次
C对应明文E出现36次
D对应明文D出现3次
E对应明文G出现9次
F对应明文F出现7次
G对应明文C出现14次
H对应明文B出现9次
I对应明文H出现18次
J对应明文I出现28次
K对应明文X出现0次
L对应明文J出现0次
M对应明文O出现29次
N对应明文A出现31次
O对应明文K出现1次
P对应明文R出现23次
Q对应明文M出现8次
R对应明文S出现21次
S对应明文T出现33次
T对应明文V出现2次
U对应明文Q出现0次
V对应明文W出现3次
W对应明文Z出现0次
X对应明文P出现12次
Y对应明文Y出现7次
Z对应明文U出现5次
```

（报告中出现的白色背景截图为将解密结果复制到 txt 中，方便对特定单词进行标注）