# 古典密码算法及攻击方式

学号：2013018　　姓名：许健　　专业：信息安全

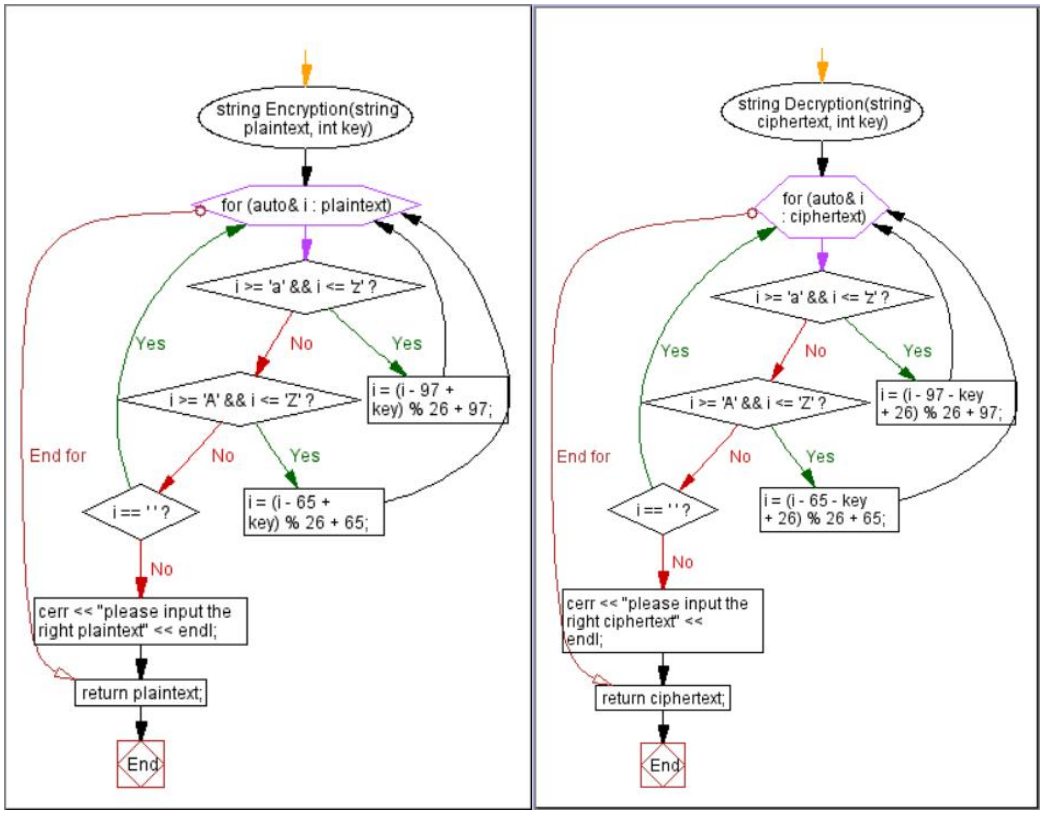
## 一、 实验目的

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。

## 二、 实验内容

**（一） 根据实验原理部分对移位密码算法的介绍，自己创建明文信息，并选择一个密钥，编写移位密码算法实现程序，实现加密和解密操作。**

**1. 算法流程图（加密和解密）**




**2. 程序演示**

明文 hello my name is jan

密钥 5

加密后的密文 mjqqt rd sfrj nx ofs

解密得到明文 hello my name is jan

**解密之后的内容与明文一致，说明解密过程是正确的**

```
欢迎使用移位密码系统，功能如下：
        1：加密解密
        2：攻击密文
        3：退出
请输入要进行的操作:1
请输入要加密的字符串:hello my name is jan
请输入要使用的密钥:5
明文:hello my name is jan
加密后:mjqqt rd sfrj nx ofs
解密后:hello my name is jan
欢迎使用移位密码系统，功能如下：
        1：加密解密
        2：攻击密文
        3：退出
请输入要进行的操作:
```

**（二） 两个同学为一组，互相攻击对方用移位密码加密获得的密文，恢复出其明文和密钥。**

**1. 使用计算机编程辅助分析**

输入一段密文：Frpsxwhuv duh pdjlfdo

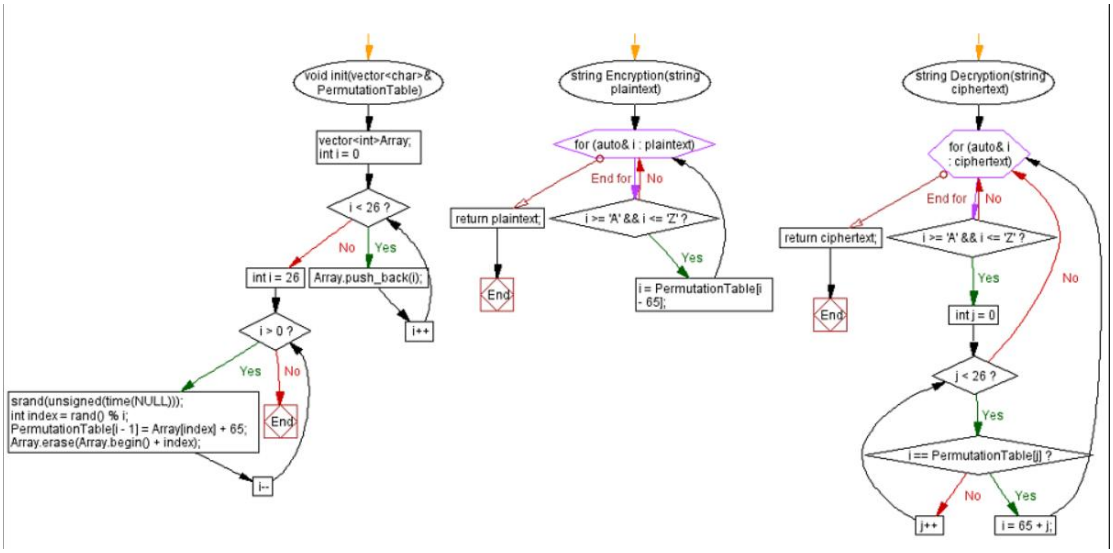
选择程序功能 2 攻击密文

在列出的解密结果中，寻找有意义的字符串。发现 Key = 3 时，得到 Computers are magical 我们认为它是明文串，密钥为 3

```
欢迎使用移位密码系统，功能如下：
        1：加密解密
        2：攻击密文
        3：退出
请输入要进行的操作:2
请输入要攻击的密文:Frpsxwhuv duh pdjlfdo
Key = 1解密后Eqorwvgtu ctg ocikecn
Key = 2解密后Dpnqvufst bsf nbhjdbm
Key = 3解密后Computers are magical
Key = 4解密后Bnlotsdqr zqd lzfhbzk
Key = 5解密后Amknsrcpq ypc kyegayj
Key = 6解密后Zljmrqbop xob jxdfzxi
Key = 7解密后Ykilqpano wna iwceywh
Key = 8解密后Xjhkpozmn vmz hvbdxvg
Key = 9解密后Wigjonylm uly guacwuf
Key = 10解密后Vhfinmxkl tkx ftzbvte
Key = 11解密后Ugehmlwjk sjw esyausd
Key = 12解密后Tfdglkvij riv drxztrc
Key = 13解密后Secfkjuhi qhu cqwysqb
Key = 14解密后Rdbejitgh pgt bpvxrpa
Key = 15解密后Qcadihsfg ofs aouwqoz
Key = 16解密后Pbzchgref ner zntvpny
Key = 17解密后Oaybgfqde mdq ymsuomx
Key = 18解密后Nzxafepcd lcp xlrtnlw
Key = 19解密后Mywzedobc kbo wkqsmkv
Key = 20解密后Lxvydcnab jan vjprlju
Key = 21解密后Kwuxcbmza izm uioqkit
Key = 22解密后Jvtwbalyz hyl thnpjhs
Key = 23解密后Iusvazkxy gxk sgmoigr
Key = 24解密后Htruzyjwx fwj rflnhfq
Key = 25解密后Gsqtyxivw evi qekmgep
```

**（三） 自己创建明文信息，并选择一个密钥，构建置换表。编写置换密码的加解密实现程序，实现加密和解密操作。**

**1. 算法流程图（置换表初始化、加密、解密）**




**简单起见，本次实验我们仅使用了大写字母**

**2. 程序演示**

启动程序会随机初始化置换表，也可以手动设置密钥

输入明文字符串 MY NAME IS JAN

加密后的密文 JY BIJU NG MIB

解密得到明文 MY NAME IS JAN

**上述的加密就是使用置换表进行字母代换，比如 M->J、N->B**

**解密之后的内容与明文一致，说明解密过程是正确的**

```
初始置换表
A:I     B:P     C:A     D:X     E:U     F:S     G:C     H:Z     I:N     J:M     K:V     L:K     M:J
N:B     O:H     P:L     Q:O     R:F     S:G     T:E     U:R     V:W     W:T     X:Q     Y:Y     Z:D
欢迎使用置换密码系统，功能如下：
        1：加密解密
        2：攻击密文
        3：重置置换表
        4：退出
请输入要进行的操作:1
请输入要加密的字符串:MY NAME IS JAN
明文:MY NAME IS JAN
加密后:JY BIJU NG MIB
解密后:MY NAME IS JAN
```

**（四） 用频率统计方法，试译下面用单表置换加密的一段密文。写出获得的明文消息和置换表**

**1. 编写频率统计函数辅助分析**

`void CharFrequency(string Unknown)`

统计单字符出现频率并按照频率信息解密密文

```
单字母频率
C: 10.68  S: 9.79  N: 9.20  M: 8.61  B: 8.31  J: 8.31  P: 6.82  R: 6.23  I: 5.34  G: 4.15  X: 3.56  A: 2.97  E: 2.67
H: 2.67  Q: 2.37  F: 2.08  Y: 2.08  Z: 1.48  D: 0.89  V: 0.89  T: 0.59  O: 0.30  K: 0.00  L: 0.00  U: 0.00  W: 0.00
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
```

```
void WordFrequency(string Unknown)
```

统计单词出现频率

```
单词频率
单词出现总次数 : 23.00
ENJB : 4.35      FPMQ : 4.35      GCBSPNA : 4.35  GINBBCA : 4.35  GMBSPMA : 4.35  GNB : 4.35
GPYXSMEPNXIY : 4.35      H : 4.35        HC : 4.35       HMH : 4.35      HY : 8.70
JB : 13.04       JBFMPQNSJMB : 4.35      JBRCGZPC : 4.35 JR : 4.35       MBAY : 4.35
MF : 17.39       MPJEJBNA : 4.35 MPJEJBNSMP : 4.35       MRGNP : 4.35    MXXMBCBS : 4.35
N : 26.09        NAJGC : 4.35    NBD : 4.35      NPC : 4.35      PCGCJTCP : 4.35
PCGJXJCBSR : 4.35        PCGMTCPCD : 4.35        PJEISFZA : 4.35 QCNBR : 4.35    QCRRNEC : 8.70
RZGI : 4.35      SIC : 39.13     SINS : 8.70     SM : 8.70       SPNBRNGSJMB : 4.35
SPNBRQJSSJBE : 4.35      VIM : 4.35      VJRICR : 4.35   VNY : 4.35      XMJBS : 8.70
XMRRJHAC : 4.35 XMRRJHAY : 4.35 XNPSJGJXNBSR : 4.35     XPMHACQ : 4.35  ZBNZSIMPJOCD : 4.35
```

置换密码的明文越长被破解的可能性就越大，由于样本字符串太短导致频率信息不明显，只能与近似频率简单比对，无法得到太多信息。

将字符按照频率对应关系替换，我们得到一串包含了许多错误的单词字符，说明当前的置换关系是不正确的，但是也有一些正确的单词被置换出来，比如 **SIC->the**，因此我们得到置换表中三个字符的对应关系。还有一些较为明显的对应关系，比如：thot->that、ti->to，我们也可以确定这些字符的对应关系。

接下来的工作则是依据单词的语义信息以及频率对应信息进行挨个字符替换，随着我们确定的字符越来越多，剩下的工作也变得简单了起来。

### 2. 推导过程

```
the cent?al p?o?le? ?n c?ypto??aphy ?? that of t?an???tt?n? ?nfo??at?on f?o? a po?nt a to a po?nt ? ?y ?ean? of a po????
ly ?n?ec??e channel ?n ??ch a way that the o????nal ?e??a?e can only ?e ?ecove?ed ?y the ???htf?l ?ec?p?ent? the pa?t?c?
pant? ?n the t?an?act?on a?e al?ce the o????nato? of the ?e??a?e ?o? the ?ece?ve? and o?ca? a po????le opponent who w??h
e? to ?a?n ?na?tho???ed cont?ol of the ?e??a?e
```

发现一些可能的对应关系：cent?al->central、?ean?->means、po?nt->point

```
the central pro?lem in crypto?raphy is that of transmittin? information from a point a to a point ? ?y means of a possi?
ly insec?re channel in s?ch a way that the ori?inal messa?e can only ?e recovered ?y the ri?htf?l recipients the partici
pants in the transaction are alice the ori?inator of the messa?e ?o? the receiver and oscar a possi?le opponent who wish
es to ?ain ?na?thori?ed control of the messa?e
```

发现一些可能的对应关系：pro?lem->problem、crypto?raphy->cryptography、transmittin?->transmitting、possi?ly->possibly、insec?re->insecure、s?ch->such、ori?inal->oridinal、messa?e->message、ori?inator-> originator

```
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 unauthori?ed control of the message
```

发现一些可能的对应关系：Unauthori?ed ->unauthorized

至此我们已经得到所有出现字符的置换关系，得到最终的明文

### 3. 解密得到的明文以及置换表

**明文**

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 unauthorized control of the message

（密码学的核心问题是如何通过一种可能不安全的通道将信息从 a 点传送到 b 点，这种方式使得原始消息只能由合法的接收者恢复——交易的参与者是消息的发起者 Alice 和希望获得消息未经授权控制的可能的对手 Oscar）

```
请输入要进行的操作:2
SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFMPQNSJMB FPMQ N XMJBS N SM N XMJBS H HY QCNBR MF N XMRRJH
AY JBRCGZPC GINBBCA JB RZGI N VNY SINS SIC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPCD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJ
XNBSR JB SIC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTCP NBD MRGNP N XMRRJHAC MXXMBCBS VIM VJRI
CR SM ENJB ZBNZSIMPJOCD GMBSPMA MF SIC QCRRNEC
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 unauthorized control of the message
```

**置换表（K、L、U、W 未出现，无法确定置换关系）**

| A | B | C | D | E | F | G | H | I | J | K | L | M |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| l | n | e | d | g | f | c | b | h | i | ? | ? | o |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| a | z | r | m | s | t | v | ? | w | ? | p | y | u |