实验一 古典密码算法及攻击方法

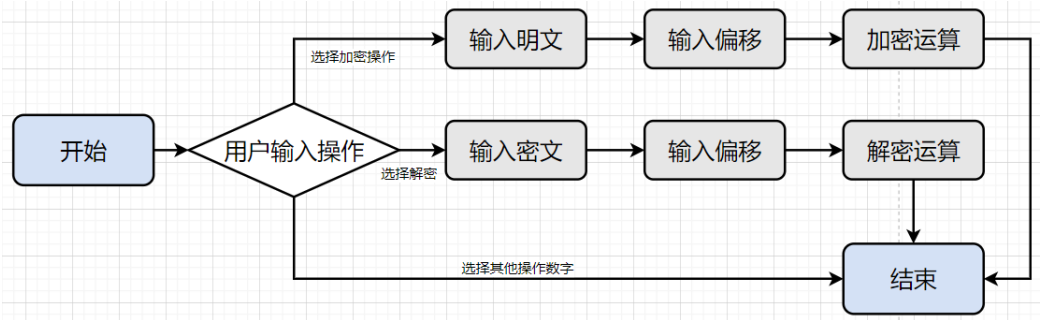
姓名：范毓哲　学号：1910378

一、 实验目的

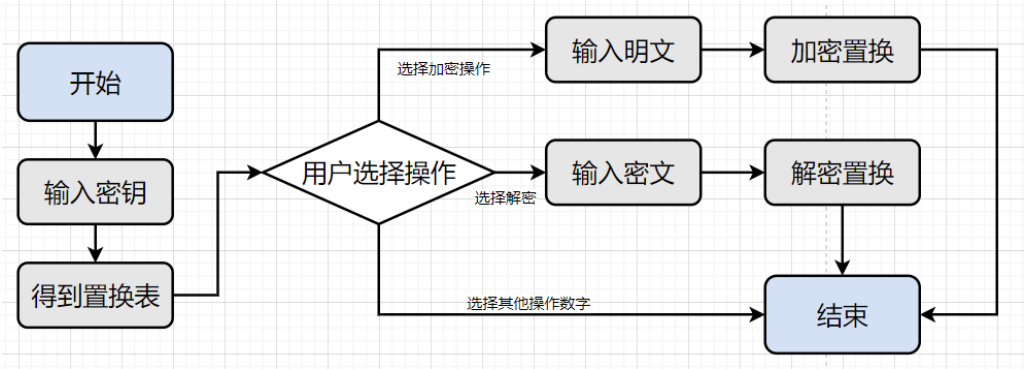
通过 C＋＋编程实现移位密码和单表置换密码算法，加深对经典密码体制的了解。并通过对这两种密码实施攻击，了解对古典密码体制的攻击方法。

二、 设计流程

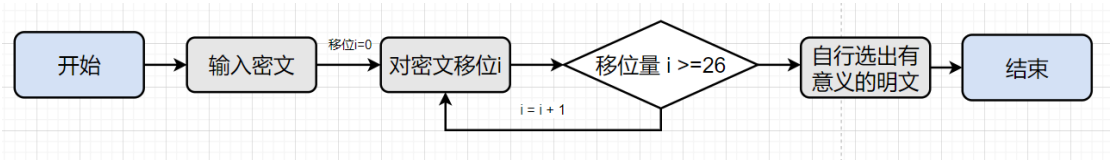
移位密码的加解密：



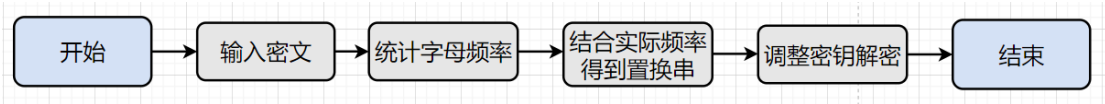
单表置换密码的加解密：



移位密码的攻击：



单表置换密码的攻击：



三、 实验环境

Windows10 操作系统+VS2019(VC17)。

同级目录下，Ccaesar.cpp 为移位密码的实现，Ctable.cpp 为单表置换密码，tableCrack.cpp 为单表置换密码的密钥破解，对应的 exe 分别为其可执行程序。

四、 程序实现

1. 移位密码

移位密码的实现较为简单，其加密、解密和攻击破解的代码如下：

```
#include<string>
#include<iostream>
using namespace std;
char res[100];    //记录程序结果
void JieMi(char *txt, int offset, int tag)    //加解密函数，tag 为 1 时加密，-1 解密
{
    int real_offset = (offset % 26)*tag;      //计算实际偏移，范围 0-25，加密加，解密减
    int length = strlen(txt);
    for (int i = 0; i < length; i++)
    {
        if (txt[i] >= 65 && txt[i] <= 90)     //区分大写和小写的情况，只处理字母
        {
            int temp = txt[i] + real_offset;
            if (temp < 65) temp += 26;
            if (temp > 90) temp -= 26;
            res[i] = (char)temp; continue;
        }
        if (txt[i] >= 97 && txt[i] <= 122)
        {
            int temp = txt[i] + real_offset;
            if (temp < 97) temp += 26;
            if (temp > 122) temp -= 26;
            res[i] = (char)temp; continue;
        }
        res[i] = txt[i];
    }
    res[length] = '\0';     //结束字符
    cout << "结果为:  " << res<< endl;
}

int main()
{
    int flag, offset = 0;
    cout << "请输入一个数字，以选择您要进行的操作。" << endl;
    cout << "(操作提示：0 加密，1 解密，2 攻击，其余退出)" << endl;
    while (1)
```

```
    {
        char txt[100]; cout << "选择操作数： "; cin >> flag;
        switch (flag)
        {
            case 0: cout << "【加密】请输入明文和偏移量： ";
                    cin >> txt >> offset; JieMi(txt, offset, 1); break;
            case 1: cout << "【解密】请输入密文和偏移量： ";
                    cin >> txt >> offset; JieMi(txt, offset, -1); break;
            case 2: cout << "【攻击】请输入待破解的密文： ";
                 cin >> txt; cout << "可能的明文情况如下。" << endl;
                for (int i = 0; i < 26; i++)   //攻击时尝试 26 种可能即可
                {cout << "移位为  " << i << "  时的明文  "; JieMi(txt, i, -1);}break;
            default: return 0;
        }
    }
    return 0;
}
```

2. 单表置换密码

首先实现的是单表置换密码的加解密，程序实现如下：

```
#include<iostream>
#include<map>
#include<string>
#include<stdio.h>
using namespace std;
map<char, char> p2cList,c2pList;  //两个字典，分别用于加密和解密
bool isk[26];char res[1000];  //isk 用于在转化置换表时，标记密钥字母是否出现过
void getKey(char * CKey)  //得到导出表，CKey 为用户输入的密钥串
{
    int t = 0;
    for (int i = 0; i < strlen(CKey); i++)  //密钥串的部分，依次对应进表中
    {
        CKey[i] = tolower(CKey[i]);
        if (CKey[i] >= 97 && CKey[i] <= 122 && !isk[CKey[i] - 'a'])
        {
            isk[CKey[i] - 'a'] = 1;
            p2cList[(char)('a' + t)] = CKey[i];  //在两个 List 当中添加映射
            c2pList[CKey[i]] = (char)('a' + t); t++;
        }
    }
    for (int j = t; j < 26; j++)   //密钥串之外的部分，按顺序与剩下的字母对应
    {
        char temp = '\0';
        for (int k = 0; k < 26; k++)
```

```
        {  if (isk[k] == 0) { isk[k] = 1;temp = (char)('a' + k);break;} }
        p2cList[(char)('a' + j)] = temp;c2pList[temp] = (char)('a' + j);
    }
    cout << endl << "替换表为:   " << endl;
    for (int j = 0; j < 26; j++)  cout << (char)('a' + j) << " "; cout << endl;
    for (int j = 0; j < 26; j++)  cout <<p2cList[(char)('a'+j)]<<" "; cout << endl;

}
void getRes(char* inTxt, int tag)  //加解密操作，inTxt 为用户输入的明文或密文
{    //tag 代表着加密或解密的操作，为 0 加密，为 1 解密
    int len = strlen(inTxt);
    for (int j = 0; j < len; j++)
    {
        inTxt[j] = tolower(inTxt[j]);
        if (inTxt[j] < 97 || inTxt[j] > 122) res[j] = inTxt[j];
        else
        {  //需要操作的字符是字母，则在映射表中进行查找置换
            if (tag == 0) { res[j] = p2cList.at((char)(inTxt[j])); }
            else { res[j] = c2pList.at((char)(inTxt[j])); }
        }
    }  res[len] = '\0';cout << "结果:  " << res << endl<<endl;
}
int main()
{
    cout << "请输入一个数字，以选择您要进行的操作。" << endl;
    cout << "(操作提示：0 加密，1 解密，其余退出。两种操作均需先输入密钥)" << endl;
    while (1)
    {
        int flag = 0; cout << "选择操作数:  "; cin >> flag;
        if(flag>1) { cout << "【退出】程序结束。" << endl; return 0; }

        char CKey[100]; for (int i = 0; i < 26; i++) isk[i] = 0;
        //这里一开始用成 memset 了，导致程序只能正常运行一次，需要注意
        cout << "请输入您的密钥:  "; cin.ignore(); cin.getline(CKey, 100);
        if (strlen(CKey) > 26) CKey[26] = '\0';
        getKey(CKey);//将密钥转换为密钥表
        char plaintext[1000]; char ciphertext[1000];  //明密文
        if (flag == 0)
        {
            cout << "【加密】请输入需加密的明文:  ";
            cin.getline(plaintext, 1000);   getRes(plaintext, 0);
        }
        else if(flag == 1)
        {
```

```
            cout << "【解密】请输入需解密的密文： ";
            cin.getline(ciphertext, 1000);   getRes(ciphertext, 1);
        }
    }
    return 0;
}
```

实现单表置换的攻击破解。这里不能再使用穷举法，而需要利用字母频率和语言特性、结合一定的统计规律与猜测进行实现：

```
#include<iostream>
#include<string>
#include<algorithm>
using namespace std;
struct sig2freq{char sig='a'; int num=0;}txtList[26];   //结构体：字符-出现次数
bool cmp(sig2freq a, sig2freq b)
{  return a.num > b.num;  }  //结构体比较函数
int main()
{
    char re[27];  //用来存储密钥结果
    cout << "请输入待破译的密文串： " << endl;char text[1000];
    cin.getline(text, 1000);   int len = strlen(text);
    double num = 0;//所有字母出现的总次数
    for (int i = 0; i < len; i++)
    {  //统计用户输入的密文串当中各字母出现次数
        text[i] = tolower(text[i]);
        if (text[i] >= 97 && text[i] <= 122)
        {num++; txtList[text[i] - 'a'].num++;}
    }
    cout << "\n 这段文本的字符频率信息统计如下： " << endl;
    for (int i = 0; i < 26; i++)
    {
        txtList[i].sig='a' + i;
        cout << (char)('a' + i) << "   " << (double)(txtList[i].num/ num) << endl;
    }
    char freq[26] = { 'e','t','o','i','a','n','s','r','h','l','d','u','c','m','p','y','f','g','w','b','v','k','x','j','q','z' };  //实际的频率排序
    sort(txtList, txtList + 26,cmp);  //用户密文的频率排序
    for (int i = 0; i < 26; i++)
         re[freq[i] - 'a'] = txtList[i].sig;
    //将密文字母频率与实际字母频率相对应，作为置换密钥
    re[26] = '\0';cout << "\n 据此得到的密钥为： " << re << endl;
    return 0;
}
```

五、 实验结果

移位密码的加解密：

```
请输入一个数字，以选择您要进行的操作。
(操作提示：0加密，1解密，2攻击，其余退出)
选择操作数： 0
【加密】请输入明文和偏移量： hellomynku 102
结果为： fcjjmkwlis
选择操作数： 1
【解密】请输入密文和偏移量： fcjjmkwlis 102
结果为： hellomynku
```

移位密码的攻击破解：

```
选择操作数： 2
【攻击】请输入待破解的密文： fcjjmkwlis
可能的明文情况如下。
移位为 0 时的明文结果为： fcjjmkwlis
移位为 1 时的明文结果为： ebiiljvkhr
移位为 2 时的明文结果为： dahhkiujgq
移位为 3 时的明文结果为： czggjhtifp
移位为 4 时的明文结果为： byffigsheo
移位为 5 时的明文结果为： axeehfrgdn
移位为 6 时的明文结果为： zwddgeqfcm
移位为 7 时的明文结果为： yvccfdpebl
移位为 8 时的明文结果为： xubbecodak
移位为 9 时的明文结果为： wtaadbnczj
移位为 10 时的明文结果为： vszzcambyi
移位为 11 时的明文结果为： uryybzlaxh
移位为 12 时的明文结果为： tqxxaykzwg
移位为 13 时的明文结果为： spwwzxjyvf
移位为 14 时的明文结果为： rovvywixue
移位为 15 时的明文结果为： qnuuxvhwtd
移位为 16 时的明文结果为： pmttwugvsc
移位为 17 时的明文结果为： olssvtfurb
移位为 18 时的明文结果为： nkrrusetqa
移位为 19 时的明文结果为： mjqqtrdspz
移位为 20 时的明文结果为： lippsqcroy
移位为 21 时的明文结果为： khoorpbqnx
移位为 22 时的明文结果为： jgnnqoapmw
移位为 23 时的明文结果为： ifmmpnzolv
移位为 24 时的明文结果为： hellomynku
移位为 25 时的明文结果为： gdkknlxmjt
```

验证攻击结果，可以看到，攻击是成功的：

```
选择操作数： 1
【解密】请输入密文和偏移量： fcjjmkwlis 24
结果为： hellomynku
选择操作数： 0
【加密】请输入明文和偏移量： hellomynku 24
结果为： fcjjmkwlis
```

单表置换密码的加解密：

```
选择操作数：  0
请输入您的密钥：  yi ge xin de key

替换表为：
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
y i g e x n d k a b c f h j l m o p q r s t u v w z
【加密】请输入需加密的明文：  hello,nankai!
结果：  kxffl,jyjcya!

选择操作数：  1
请输入您的密钥：  yi ge xin de key

替换表为：
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
y i g e x n d k a b c f h j l m o p q r s t u v w z
【解密】请输入需解密的密文：  kxffl,jyjcya!
结果：  hello,nankai!

选择操作数：  9
【退出】程序结束。
```

单表置换密码的攻击，输入实验提供的密文串作为样本：

```
Microsoft Visual Studio 调试控制台
请输入待破译的密文串：
SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFMPQNSJMB FPMQ N XMJBS N SM
H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SINS SIC MPJEJBNA QCRRNEC GNB MBAY
TCPCD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJXNBSR JB SIC SPNBRNGSJMB NPC NAJGC SIC MPJEJBN
IC QCRRNEC HMH SIC PCGCJTCP NBD MRGNP N XMRRJHAC MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOCD
MF SIC QCRRNEC

这段文本的字符频率信息统计如下：
a    0.0296736
b    0.0830861
c    0.106825
d    0.00890208
e    0.0267062
f    0.0207715
g    0.041543
h    0.0267062
i    0.0534125
j    0.0830861
k    0
l    0
m    0.0860534
n    0.0919881
o    0.00296736
p    0.0682493
q    0.0237389
r    0.0623145
s    0.0979228
t    0.00593472
u    0
v    0.00890208
w    0
x    0.0356083
y    0.0207715
z    0.0148368

据此得到的密钥为：  bvexcyzimloghjnqurpsatdkfw
```

最初得到的密钥为 bvexcyzimloghjnqurpsatdkfw，我们将它输入到之前完成的单表置换加解密程序进行解密：

```
请输入您的密钥：  bvexcyzimloghjnqurpsatdkfw

替换表为：
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
b v e x c y z i m l o g h j n q u r p s a t d k f w
【解密】请输入需解密的密文：  SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFM
PQNSJMB FPMQ N XMJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SIN
S SIC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPCD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJXNBSR JB S
IC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTCP NBD MRGNP N XMRRJHAC
MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOCD GMBSPMA MF SIC QCRRNEC
结果：  the leatsou dsimuep na lsfdticsodhf nr thot iy tsoarpnttnac nayispotnia ysip o dinat o
 ti o dinat m mf peoar iy o dirrnmuf narelgse lhoaaeu na rglh o bof thot the isncnaou perroce
 loa iauf me selivesew mf the snchtygu selndneatr the dostnlndoatr na the tsoaroltnia ose oun
le the isncnaotis iy the perroce mim the selenves oaw irlos o dirrnmue iddiaeat bhi bnrher ti
 cona gaogthisnkew liatsiu iy the perroce
```

得到奇怪的明文串，显而易见，o 和 a 应该对换：

```
替换表为：
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
n v e x c y z i m l o g h j b q u r p s a t d k f w
【解密】请输入需解密的密文：  SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFM
PQNSJMB FPMQ N XMJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SIN
S SIC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPCD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJXNBSR JB S
IC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTCP NBD MRGNP N XMRRJHAC
MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOCD GMBSPMA MF SIC QCRRNEC
结果：  the leotsau dsimuep no lsfdticsadhf nr that iy tsaorpnttnoc noyispatnio ysip a dinot a
 ti a dinot m mf peaor iy a dirrnmuf norelgse lhaooeu no rglh a baf that the isncnoau perrace
 lao iouf me selivesew mf the snchtygu selndneotr the dastnlndaotr no the tsaoraltnio ase aun
le the isncnoatis iy the perrace mim the selenves aow irlas a dirrnmue iddioeot bhi bnrher ti
 cano goagthisnkew liotsiu iy the perrace
```

这当中，ase 明显不是一个正常的单词，ase 应该原本是 are，所以 s 和 r 应该对换，新的结果如下：

```
请输入您的密钥：  nvexcyzimloghjbquprsatdkfw

替换表为：
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
n v e x c y z i m l o g h j b q u p r s a t d k f w
【解密】请输入需解密的密文：  SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFM
PQNSJMB FPMQ N XMJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SIN
S SIC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPCD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJXNBSR JB S
IC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTCP NBD MRGNP N XMRRJHAC
MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOCD GMBSPMA MF SIC QCRRNEC
结果：  the leotrau drimuep no lrfdticradhf ns that iy traospnttnoc noyirpatnio yrip a dinot a
 ti a dinot m mf peaos iy a dissnmuf noselgre lhaooeu no sglh a baf that the irncnoau pessace
 lao iouf me reliverew mf the rnchtygu relndneots the dartnlndaots no the traosaltnio are aun
le the irncnoatir iy the pessace mim the relenver aow islar a dissnmue iddioeot bhi bnshes ti
 cano goagthirnkew liotriu iy the pessace
```

然后 nf 应该是单词 of，n 和 o 对换，密钥是 nvexcyzimlogqbjhuprsatdkfw：

```
替换表为：
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
n v e x c y z i m l o g h b j q u p r s a t d k f w
【解密】请输入需解密的密文：  SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFM
PQNSJMB FPMQ N XMJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SIN
S SIC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPCD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJXNBSR JB S
IC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTCP NBD MRGNP N XMRRJHAC
MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOCD GMBSPMA MF SIC QCRRNEC
结果：  the lentrau drimuep on lrfdticradhf os that iy transpottonc onyirpatoin yrip a diont a
 ti a diont m mf peans iy a dissomuf onselgre lhanneu on sglh a baf that the iroconau pessace
 lan inuf me reliverew mf the rochtygu relodoents the dartolodants on the transaltoin are auo
le the iroconatir iy the pessace mim the releover anw islar a dissomue iddinent bhi boshes ti
 caon gnagthirokew lintriu iy the pessace
```

可以发现，peans 应该是 means，所以 p 和 m 也对换。

```
替换表为：
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
n v e x c y z i m l o g q b j h u p r s a t d k f w
【解密】请输入需解密的密文： SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFM
PQNSJMB FPMQ N XMJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SIN
S SIC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPCD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJXNBSR JB S
IC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTCP NBD MRGNP N XMRRJHAC
MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOCD GMBSPMA MF SIC QCRRNEC
结果： the lentrau dripuem on lrfdticradhf os that iy transmottonc onyirmatoin yrim a diont a
 ti a diont p pf means iy a dissopuf onselgre lhanneu on sglh a baf that the iroconau messace
 lan inuf pe reliverew pf the rochtygu relodoents the dartolodants on the transaltoin are auo
le the iroconatir iy the messace pip the releover anw islar a dissopue iddinent bhi boshes ti
 caon gnagthirokew lintriu iy the messace
```

当中的 os 应该是 is，iy 应该是 if，所以 o 和 i 对换，y 和 f 对换。

```
替换表为：
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
n v e x c f z i j l o g q b m h u p r s a t d k y w
【解密】请输入需解密的密文： SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFM
PQNSJMB FPMQ N XMJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SIN
S SIC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPCD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJXNBSR JB S
IC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTCP NBD MRGNP N XMRRJHAC
MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOCD GMBSPMA MF SIC QCRRNEC
结果： the lentrau dropuem in lrydtocradhy is that of transmittinc information from a doint a
 to a doint p py means of a dossipuy inselgre lhanneu in sglh a bay that the oricinau messace
 lan onuy pe reloverew py the richtfgu relidients the dartilidants in the transaltion are aui
le the oricinator of the messace pop the releiver anw oslar a dossipue oddonent bho bishes to
 cain gnagthorikew lontrou of the messace
```

这段明文中的 messace 应该是 message，c 和 g 对换：

```
替换表为：
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
n v z x c f e i j l o g q b m h u p r s a t d k y w
【解密】请输入需解密的密文： SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBF
PQNSJMB FPMQ N XMJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SI
S SIC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPCD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJXNBSR JB
IC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTCP NBD MRGNP N XMRRJHAC
MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOCD GMBSPMA MF SIC QCRRNEC
结果： the lentrau dropuem in lrydtogradhy is that of transmitting information from a doint
 to a doint p py means of a dossipuy inselcre lhanneu in sclh a bay that the originau messag
 lan onuy pe reloverew py the rightfcu relidients the dartilidants in the transaltion are au
le the originator of the message pop the releiver anw oslar a dossipue oddonent bho bishes t
 gain cnacthorikew lontrou of the message
```

dropuem 大概是 problem，所以 p 和 b 对换，u 和 l 对换：

```
替换表为：
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
n h z x c f e i j l o a q b m v u p r s g t d k y w
【解密】请输入需解密的密文： SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFM
PQNSJMB FPMQ N XMJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SIN
S SIC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPCD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJXNBSR JB S
IC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTCP NBD MRGNP N XMRRJHAC
MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOCD GMBSPMA MF SIC QCRRNEC
结果： the uentral droblem in urydtogradhy is that of transmitting information from a doint a
 to a doint b by means of a dossibly inseucre uhannel in scuh a pay that the original message
 uan only be reuoverew by the rightfcl reuidients the dartiuidants in the transaution are ali
ue the originator of the message bob the reueiver anw osuar a dossible oddonent pho pishes to
 gain cnacthorikew uontrol of the message
```

uontrol 应该是 control，pishes 应该是 wishes，所以 u 和 c 对换，p 和 w 对换：

```
替换表为:
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
n h g x c f e i j l o a q b m d u p r s z t v k y w
【解密】请输入需解密的密文:  SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFM
PQNSJMB FPMQ N XMJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SIN
S SIC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPCD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJXNBSR JB S
IC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTCP NBD MRGNP N XMRRJHAC
MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOCD GMBSPMA MF SIC QCRRNEC
结果:  the central droblem in crydtogradhy is that of transmitting information from a doint a
 to a doint b by means of a dossibly insecure channel in such a way that the original message
 can only be recoverep by the rightful recidients the darticidants in the transaction are ali
ce the originator of the message bob the receiver anp oscar a dossible oddonent who wishes to
 gain unauthorikep control of the message
```

之前换好的表又被打乱了一部分，调整之（p 和 d 对换），同时，unauthoriked 应该是 unauthorized，所以最终的密钥是 nhgdcfeijlwaqbmxuprsztvkyo：

```
选择操作数:  1
请输入您的密钥:  nhgdcfeijlwaqbmxuprsztvkyo

替换表为:
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
n h g d c f e i j l w a q b m x u p r s z t v k y o
【解密】请输入需解密的密文:  SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFM
PQNSJMB FPMQ N XMJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SIN
S SIC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPCD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJXNBSR JB S
IC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTCP NBD MRGNP N XMRRJHAC
MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOCD GMBSPMA MF SIC QCRRNEC
结果:  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 ali
ce the originator of the message bob the receiver and oscar a possible opponent who wishes to
 gain unauthorized control of the message
```

于是，实际得到的明文为：

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 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