南开大学

网络空间安全学院

密码学实验报告

古典密码算法及攻击方法

李佩诺

年级：2020 级

专业：信息安全

指导教师：古力

2022 年 11 月 15 日

目录

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

1. 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。
2. 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。
3. 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。
4. 用频率统计方法，试译下面用单表置换加密的一段密文：SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFMPQNSJMB FPMQ N XMJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SINS SIC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPCD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJXNBSR JB SIC 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 写出获得的明文消息和置换表。

三、 实验过程

(一) 移位密码

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 ＝ m1m2···mi···, 则有密文：c=c1c2···ci···, 其中 ci=(mi+key mod26)，i ＝ 1，2，···。

2. 算法流程图

加密

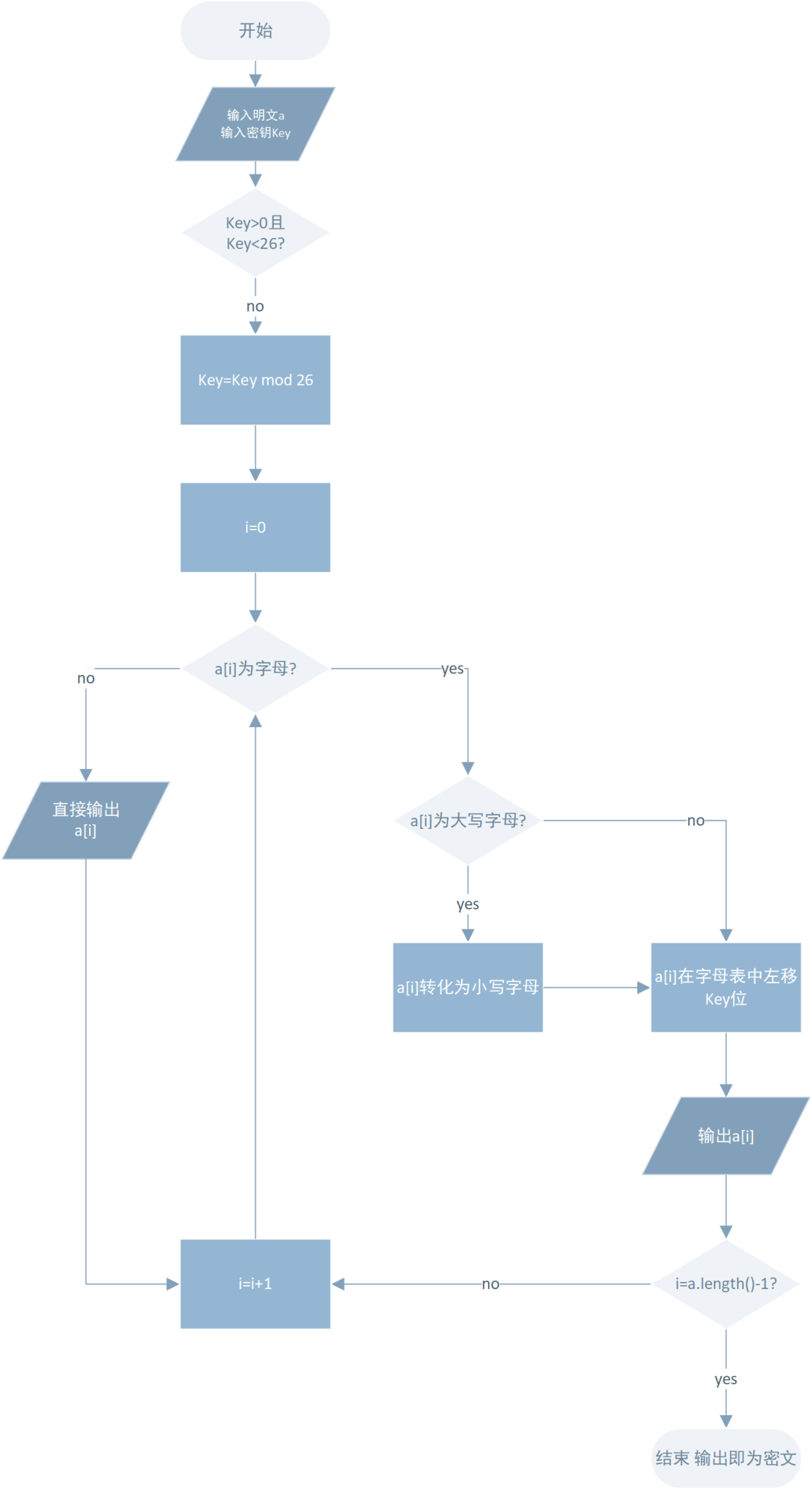


图 1: 移位密码加密算法流程图

解密

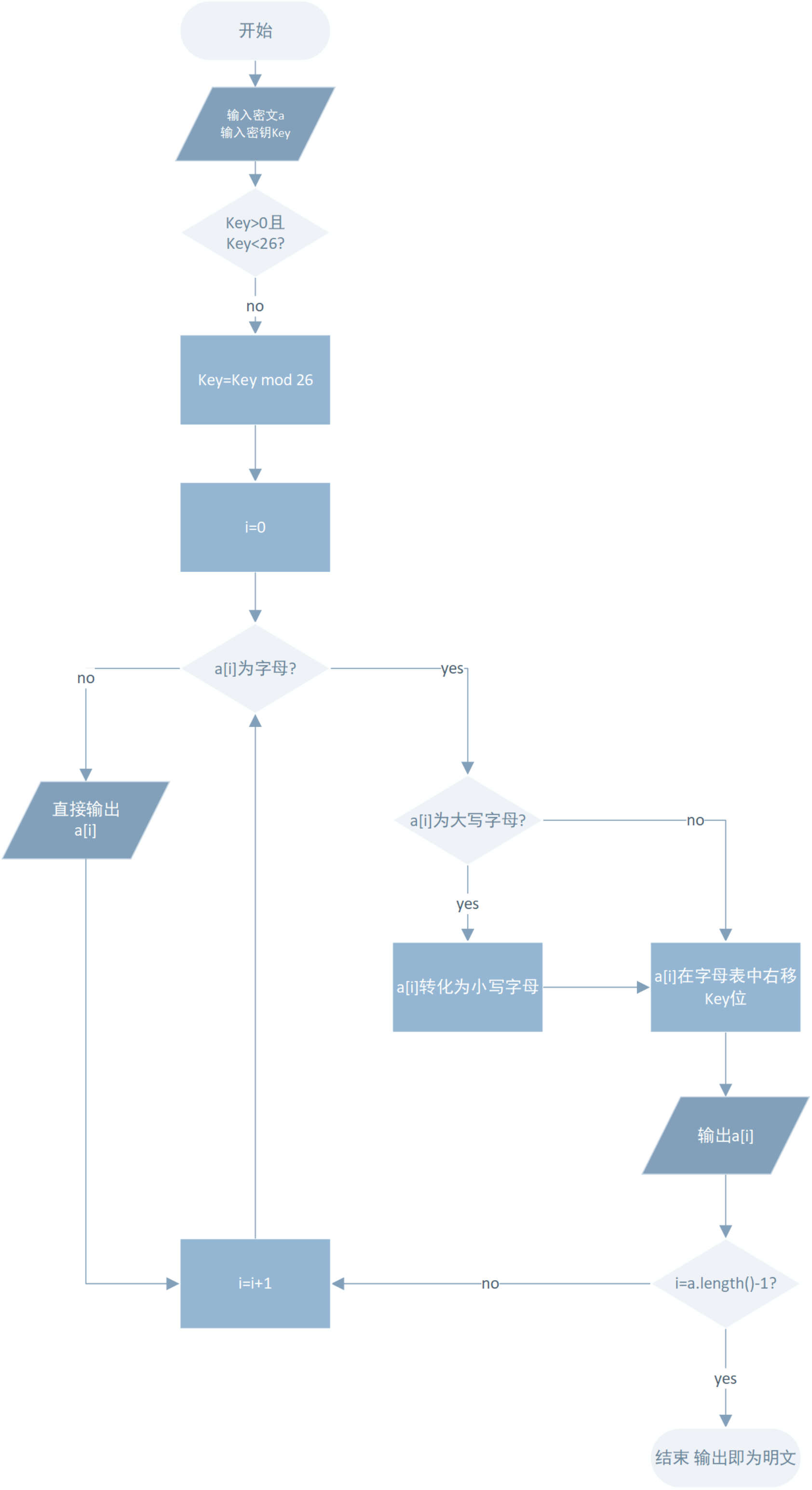


图 2: 移位密码解密算法流程图

3. 实验代码

加密代码

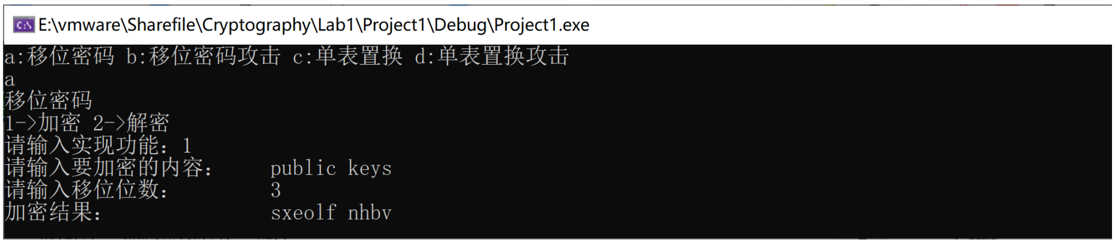
```cpp
cout << "请输入要加密的内容：\t";
string a;
getline(cin, a);
getline(cin, a);
//cout<<typeid(a[0]).name()<<endl;
int len = a.length();
int n1;//左移n位
cout << "请输入移位位数：\t";
cin >> n1;
if (n1 >= 26) { n1 %= 26; }
string* key1 = new string[len];
cout << "加密结果：\t\t";
for (int i = 0; i < len; i++) {
	if (a[i] < 65 || (a[i] > 90 && a[i] < 97) || a[i]>122) { cout << a[i]; continue; }
	if (a[i] >= 65 && a[i] <= 90) { a[i] += 32; }
	if (a[i] + n1 > 122) { a[i] -= 26; }
	key1[i] = char(int(a[i]) + n1);
	cout << key1[i];
}
cout << endl;
```

解密代码

```cpp
cout << "请输入要解密的内容：\t";
string a;
getline(cin, a);
getline(cin, a);
int len = a.length();
int n1;//右移n位
cout << "请输入移位位数：\t";
cin >> n1;
if (n1 >= 26) { n1 %= 26; }
string* key1 = new string[len];
cout << "解密结果：\t\t";
for (int i = 0; i < len; i++) {
	if (a[i] < 65 || (a[i] > 90 && a[i] < 97) || a[i]>122) { cout << a[i]; continue; }
	if (a[i] >= 65 && a[i] <= 90) { a[i] += 32; }
	if (a[i] - n1 < 97) { a[i] += 26; }
	key1[i] = char(int(a[i]) - n1);
	cout << key1[i];
}
cout << endl;
```

4. 实验结果

加密：输入明文为 public keys，密钥为 3（即凯撒密码），输出结果应为 sxeolf nhbv。

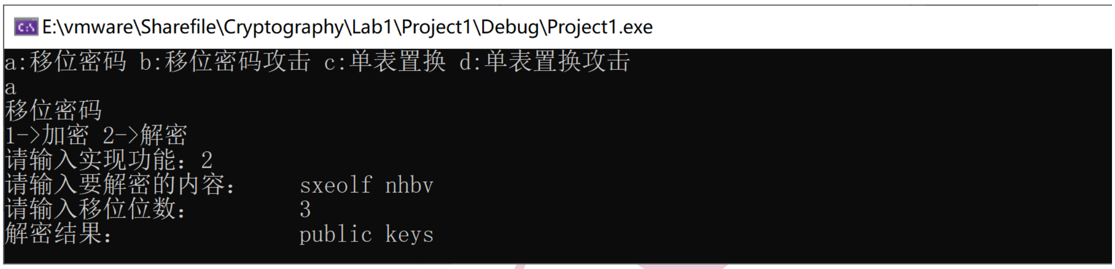


E:\vmware\Sharefile\Cryptography\Lab1\Project1\Debug\Project1.exe

```
a:移位密码 b:移位密码攻击 c:单表置换 d:单表置换攻击
a
移位密码
1->加密 2->解密
请输入实现功能: 1
请输入要加密的内容:      public keys
请输入移位位数:          3
加密结果:                sxeolf nhbv
```

图 3: 明文加密结果

解密：将上述得到的结果进行解密，输出结果应为 public keys:



E:\vmware\Sharefile\Cryptography\Lab1\Project1\Debug\Project1.exe

```
a:移位密码 b:移位密码攻击 c:单表置换 d:单表置换攻击
a
移位密码
1->加密 2->解密
请输入实现功能: 2
请输入要解密的内容:      sxeolf nhbv
请输入移位位数:          3
解密结果:                public keys
```

图 4: 密文解密结果

（二） 对移位密码的攻击

1. 实验原理

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. 算法流程图

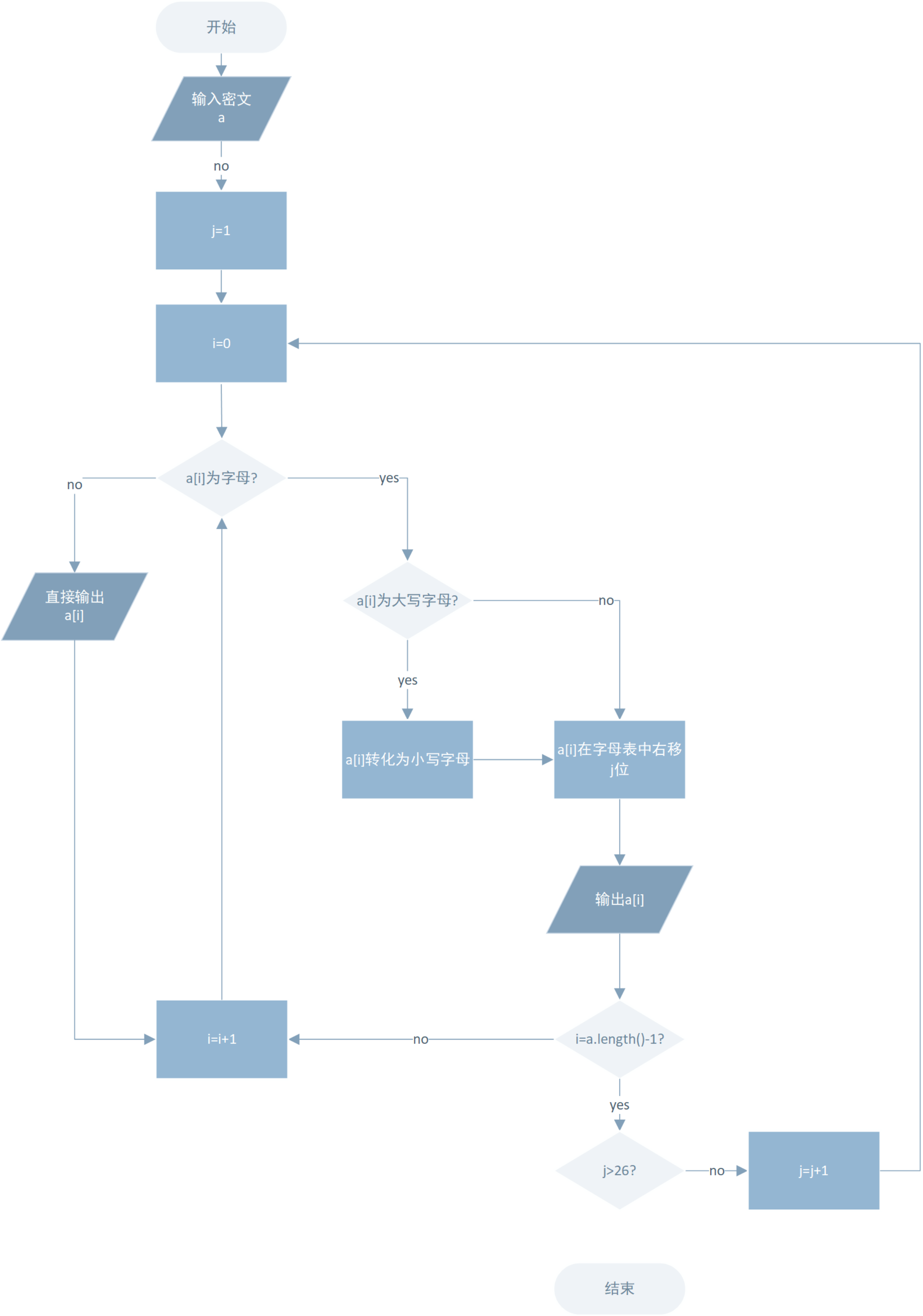


图 5: 对移位密码的攻击算法流程图

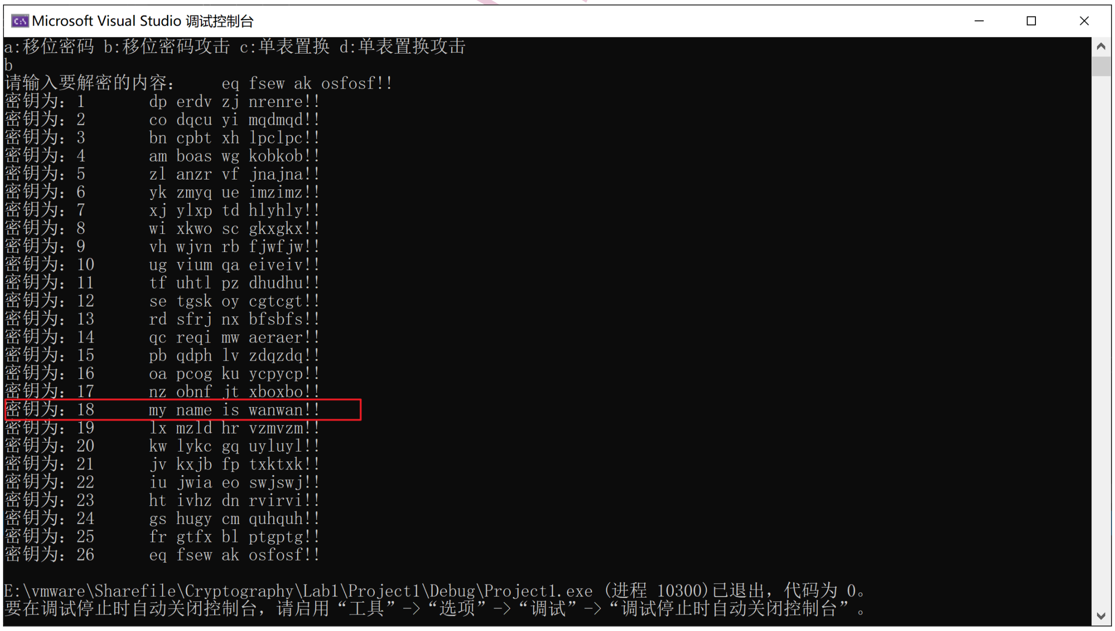
3. 实验代码

移位密码攻击

```
cout << "请输入要解密的内容: \t";
string b;
getline(cin, b);
getline(cin, b);
int len = b.length();
string* key1 = new string[len];
for (int j = 1; j <= 26; j++) {
        cout << "密钥为: " << j << "\t";
        for (int i = 0; i < len; i++) {
                string a = b;
                if (a[i] < 65 || (a[i] > 90 && a[i] < 97) || a[i]>122) { cout << a[i]; continue; }
                if (a[i] >= 65 && a[i] <= 90) { a[i] += 32; }
                if (a[i] - j < 97) { a[i] += 26; }
                key1[i] = char(int(a[i]) - j);
                cout << key1[i];
        }
        cout << endl;
}
```

4. 实验结果

比如截获密文为：eq fsew ak osfosf!!



```
a:移位密码 b:移位密码攻击 c:单表置换 d:单表置换攻击
b
请输入要解密的内容:      eq fsew ak osfosf!!
密钥为: 1        dp erdv zj nrenre!!
密钥为: 2        co dqcu yi mqdmqd!!
密钥为: 3        bn cpbt xh lpclpc!!
密钥为: 4        am boas wg kobkob!!
密钥为: 5        zl anzr vf jnajna!!
密钥为: 6        yk zmyq ue imzimz!!
密钥为: 7        xj ylxp td hlyhly!!
密钥为: 8        wi xkwo sc gkxgkx!!
密钥为: 9        vh wjvn rb fjwfjw!!
密钥为: 10       ug vium qa eiveiv!!
密钥为: 11       tf uhtl pz dhudhu!!
密钥为: 12       se tgsk oy cgtcgt!!
密钥为: 13       rd sfrj nx bfsbfs!!
密钥为: 14       qc reqi mw aeraer!!
密钥为: 15       pb qdph lv zdqzdq!!
密钥为: 16       oa pcog ku ycpycp!!
密钥为: 17       nz obnf jt xboxbo!!
密钥为: 18       my name is wanwan!!
密钥为: 19       lx mzld hr vzmvzm!!
密钥为: 20       kw lykc gq uyluyl!!
密钥为: 21       jv kxjb fp txktxk!!
密钥为: 22       iu jwia eo swjswj!!
密钥为: 23       ht ivhz dn rvirvi!!
密钥为: 24       gs hugy cm quhquh!!
密钥为: 25       fr gtfx bl ptgptg!!
密钥为: 26       eq fsew ak osfosf!!

E:\vmware\Sharefile\Cryptography\Lab1\Project1\Debug\Project1.exe (进程 10300)已退出，代码为 0。
要在调试停止时自动关闭控制台，请启用“工具”->“选项”->“调试”->“调试停止时自动关闭控制台”。
```

图 6: 移位密码攻击

根据实验结果可以解出明文：my name is wanwan!! 密钥为 18

（三） 单表置换密码

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。

2. 算法流程图

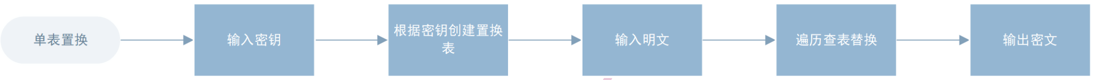


图 7: 单表置换密码算法流程图

3. 实验代码

加密代码

```
map<string, string>mp_str;
map<char, char>mp_ch;
string str1 = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";
string str2 ;
string key1="";
cout << "输入密钥：\t";
getline(cin, str2);
getline(cin, str2);
map<char, int>mp_is;
//将字母表所有字母出现标志位设置为0
for (int i = 0; i < 26; i++) {
        mp_is[str1[i]] = 0;
}
//如果在输入中出现过 标志位设置为1 在ley中添加
for (int i = 0; i < str2.length(); i++) {
        if (str2[i] >= 97 && str2[i] <= 122) { str2[i] -= 32; }
        else if (str2[i] < 65 || str2[i]>90) { continue; }
        if (mp_is[str2[i]] == 0) { key1 += str2[i]; }
        mp_is[str2[i]] = 1;
}
//没出现过的按顺序添入key中
for (int i = 0; i < 26; i++) {
        if (mp_is[str1[i]] == 0) { key1 += str1[i]; }
}
cout << "密钥为：\t" << key1 << endl;
```

```
str2 = key1;
//建立映射表
for (int i = 0; i < 26; i++) {
        mp_ch[str1[i]] = str2[i];
}
cout << "输入明文：\t";
string a;
getline(cin, a);
int len = a.length();
string b = "";
cout << "加密为：\t";
for (int i = 0; i < len; i++) {
        if (a[i] >= 97 && a[i] <= 122) { a[i] -= 32; cout << char((mp_ch[a[i]] + 32)); }
        else if (a[i] < 65 || a[i]>90) { cout << a[i]; }
        else { cout << mp_ch[a[i]]; }
}
```

解密代码

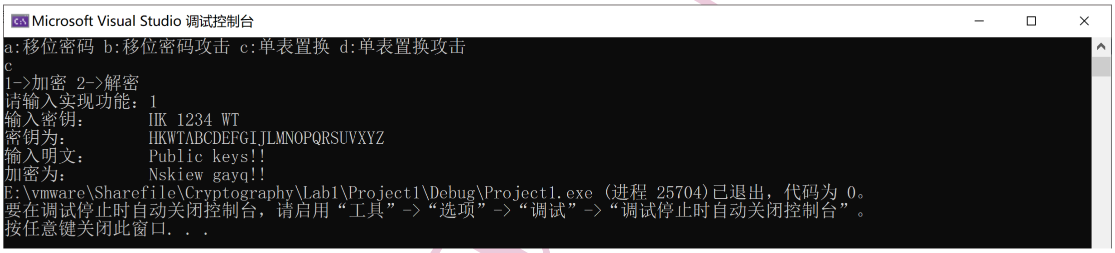
```
map<string, string>mp_str;
map<char, char>mp_ch;
string str1 = "ABCDEFGHIJKLMNOPQRSTUVWXYZ";
string str2;
string key1 = "";
cout << "输入密钥：\t";
getline(cin, str2);
getline(cin, str2);
map<char, int>mp_is;
for (int i = 0; i < 26; i++) {
        mp_is[str1[i]] = 0;
}
for (int i = 0; i < str2.length(); i++) {
        if (str2[i] >= 97 && str2[i] <= 122) { str2[i] -= 32; }
        else if (str2[i] < 65 || str2[i]>90) { continue; }
        if (mp_is[str2[i]] == 0) { key1 += str2[i]; }
        mp_is[str2[i]] = 1;

for (int i = 0; i < 26; i++) {
        if (mp_is[str1[i]] == 0) { key1 += str1[i]; }
}
cout << "密钥为：\t" << key1 << endl;
str2 = key
for (int i = 0; i < 26; i++) {
        mp_ch[str2[i]] = str1[i];
}
cout << "输入密文：\t";
string a;
getline(cin, a);
```

```
int len = a.length();
string b = "";
cout << "解密为: \t";
for (int i = 0; i < len; i++) {
        if (a[i] >= 97 && a[i] <= 122) { a[i] -= 32; cout << char((mp_ch[a[i
            ]] + 32)); }
        else if (a[i] < 65 || a[i]>90) { cout << a[i]; }
        else { cout << mp_ch[a[i]]; }
}
```

在单表置换的加解密中,考虑了输入字符串的大小写､是否为字母问题,通过 cout « char((mp_ch[a[i]] + 32)); 来实现小写字母的置换表替换, 之后通过 (a[i] < 65 || a[i]>90) cout « a[i]; 过滤非字母元素。

4. 实验结果

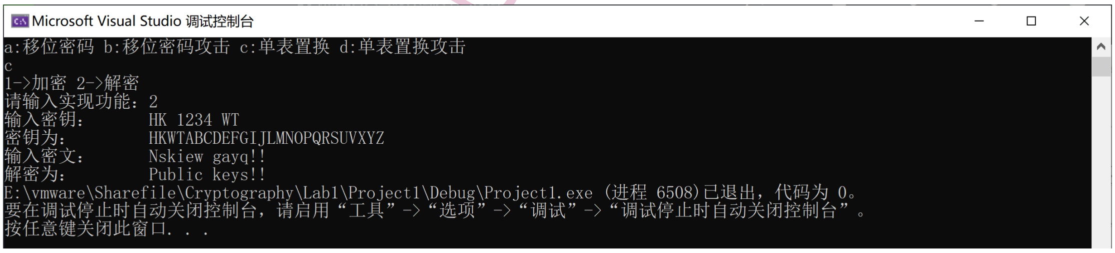
加密：例如明文为 Public keys!!，输入为“HK 1234 WT”，得到密钥为：“HKWTABCDEFGIJLMNOPQRSUVXYZ”，那么密文应为 Nskiew gayq!!;



```
a:移位密码 b:移位密码攻击 c:单表置换 d:单表置换攻击
c
1->加密 2->解密
请输入实现功能: 1
输入密钥:       HK 1234 WT
密钥为:         HKWTABCDEFGIJLMNOPQRSUVXYZ
输入明文:       Public keys!!
加密为:         Nskiew gayq!!
E:\vmware\Sharefile\Cryptography\Lab1\Project1\Debug\Project1.exe (进程 25704)已退出，代码为 0。
要在调试停止时自动关闭控制台，请启用“工具”->“选项”->“调试”->“调试停止时自动关闭控制台”。
按任意键关闭此窗口. . .
```

图 8: 加密实验结果

解密: 同理, 密文为 Nskiew gayq!! 时, 输入为“HK 1234 WT”, 得到密钥为:“HKWTABCDEFGIJLMNOPQRSUVXYZ”, 解密得到明文 Public keys!!



```
a:移位密码 b:移位密码攻击 c:单表置换 d:单表置换攻击
c
1->加密 2->解密
请输入实现功能: 2
输入密钥:       HK 1234 WT
密钥为:         HKWTABCDEFGIJLMNOPQRSUVXYZ
输入密文:       Nskiew gayq!!
解密为:         Public keys!!
E:\vmware\Sharefile\Cryptography\Lab1\Project1\Debug\Project1.exe (进程 6508)已退出，代码为 0。
要在调试停止时自动关闭控制台，请启用“工具”->“选项”->“调试”->“调试停止时自动关闭控制台”。
按任意键关闭此窗口. . .
```

图 9: 解密实验结果

（四） 对单表置换密码的攻击

1. 实验原理

在单表置换密码中，由于置换表字母组合方式有 26! 种，约为 4.03×1026。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 [1]:

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 26×26 = 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 26×26×26 = 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。

2. 算法流程图

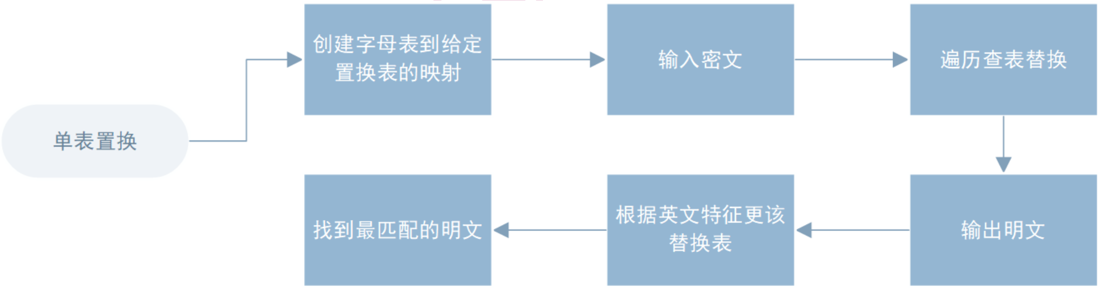


图 10: 对置换密码攻击的流程图

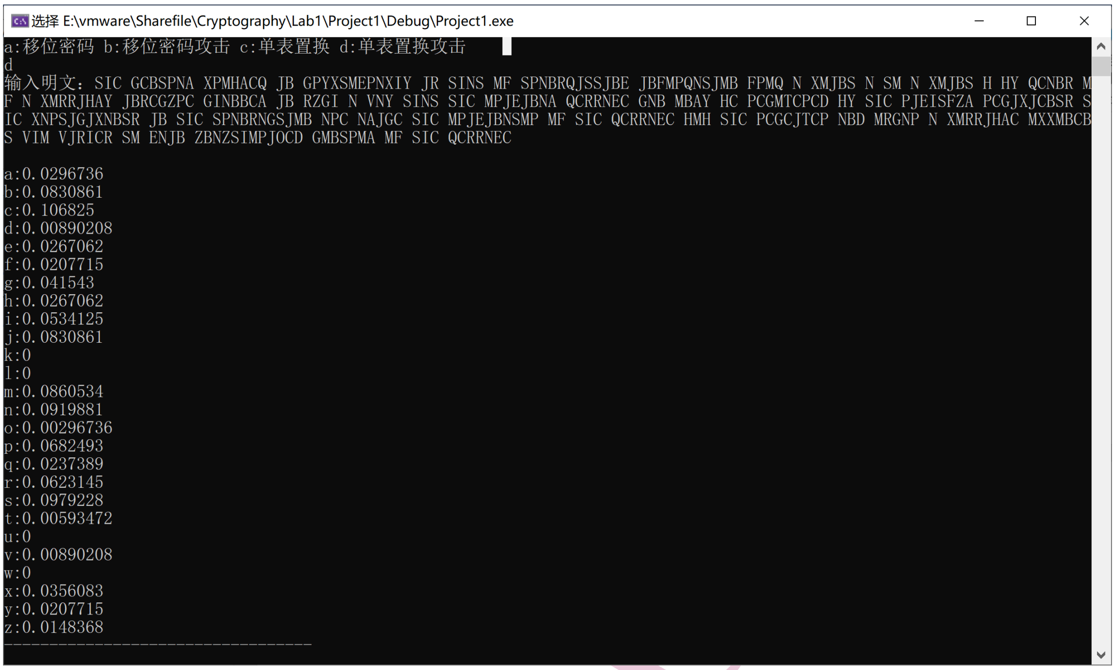
3. 实验代码

置换密码攻击代码

```
cout << "输入明文：";
string a;
getline(cin, a);
getline(cin, a);
string a_copy = a;
int len = a.length();
int sum = len;
map<char, float>mp_cf;
string str = "abcdefghijklmnopqrstuvwxyz";
string str_c = str;
//初始化
for (int i = 0; i < 26; i++) {
        mp_cf[str[i]] = 0;
}
for (int i = 0; i < len; i++) {
        //cout << "a[i]" << a[i] << endl;
        if (a[i] == 32) { cout << " "; sum--; continue; }
        if (a[i] >= 65 && a[i] <= 90) { a[i] += 32; }
        mp_cf[a[i]] += 1;
}
cout << endl;
//统计出现频率
for (char i = 0; i < 26; i++) {
        mp_cf[str[i]] /= sum;
        cout << str[i] << ":" << mp_cf[str[i]] << endl;
}
//排序
for (int i = 0; i < 26 - 1; i++) {
        for (int j = 0; j < 26 - i -1; j++) {
                if (mp_cf[str[j]] < mp_cf[str[j + 1]]) {
                        float temp_f= mp_cf[str[j]];
                        char temp_c=str[j];
                        str[j] = str[j + 1];
                        mp_cf[str[j]] = mp_cf[str[j + 1]];

                        str[j + 1] = temp_c;
                        mp_cf[str[j + 1]] = temp_f;
                }
        }
}
cout << "-----------------------------------"<<endl;
for (char i = 0; i < 26; i++) {
        cout << str[i] << ":" << mp_cf[str[i]] << endl;
}
//电子文本字母频率映射
map<char, char> map_stos;
string net_str = "etoiansrhlducmpyfgwbvkxjqz";
for (char i = 0; i < 26; i++) {
        map_stos[str[i]] = net_str[i];
}
cout << "置换表为: " << endl;
for (char i = 0; i < 26; i++) {
        cout << str_c[i] << " ";
}
cout << endl;
for (char i = 0; i < 26; i++) {
        cout << map_stos[str_c[i]] << " ";
}
cout << endl << "解密结果: " << endl;
//首次破译
a = a_copy;
for (int i = 0; i < len; i++) {
        if (a[i] == 32) { cout << " "; sum--; continue; }
        if (a[i] >= 65 && a[i] <= 90) { a[i] += 32; }
        cout << map_stos[a[i]];
}
//根据英文特征继续破译
while (1) {
        char old1;
        char new1;
        cout <<endl<<"--------------------------------------------------" << endl;
        cout << "the first letter:";
        cin >> old1;
        cout << "the second letter:";
        cin >> new1;
        cout << "--------------" << endl;
        for (int i = 0; i < 26; i++) {
                if (map_stos[str[i]] == old1) { map_stos[str[i]] = new1; continue; }
                if (map_stos[str[i]] == new1) { map_stos[str[i]] = old1; continue; }
        }
        cout << "置换表为: " << endl;
        for (char i = 0; i < 26; i++) {
                cout << str_c[i] << " ";
        }
        cout << endl;
        for (char i = 0; i < 26; i++) {
                cout << map_stos[str_c[i]] << " ";
        }
        cout << endl << "解密结果: " << endl;
        for (int i = 0; i < len; i++) {
                //cout << "a[i]" << a[i] << endl;
                if (a[i] == 32) { cout << " "; sum--; continue; }
                if (a[i] >= 65 && a[i] <= 90) { a[i] += 32; }
                cout << map_stos[a[i]];
        }
}
```

4. 实验步骤与结果

1. 输入明文，统计输入明文字母出现频率

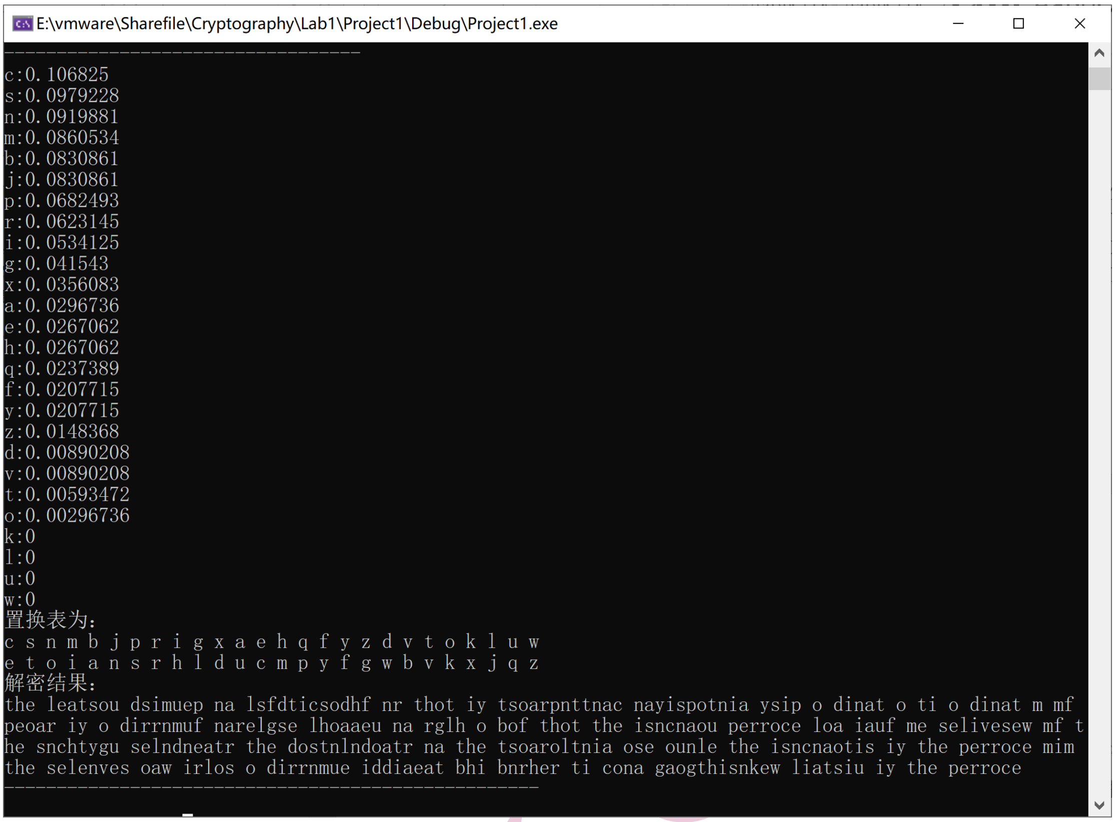


选择 E:\vmware\Sharefile\Cryptography\Lab1\Project1\Debug\Project1.exe

```
a:移位密码 b:移位密码攻击 c:单表置换 d:单表置换攻击
d
输入明文：SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFMPQNSJMB FPMQ N XMJBS N SM N XMJBS H HY QCNBR M
F N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SINS SIC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPCD HY SIC PJEISFZA PCGJXJCBSR S
IC XNPSJGJXNBSR JB SIC SPNBRNGSJMB NPC NAJGC SIC MPJEJBSMP MF SIC QCRRNEC HMH SIC PCGCJTCP NBD MRGNP N XMRRJHAC MXXMBCB
S VIM VJRICR SM ENJB ZBNZSIMPJOCD GMBSPMA MF SIC QCRRNEC

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
----------------------------------
```

图 11: 明文字母出现频率

2. 将字母出现频率排序，然后根据电子文本中的字母频率进行简单置换表构建，执行第一次解密：



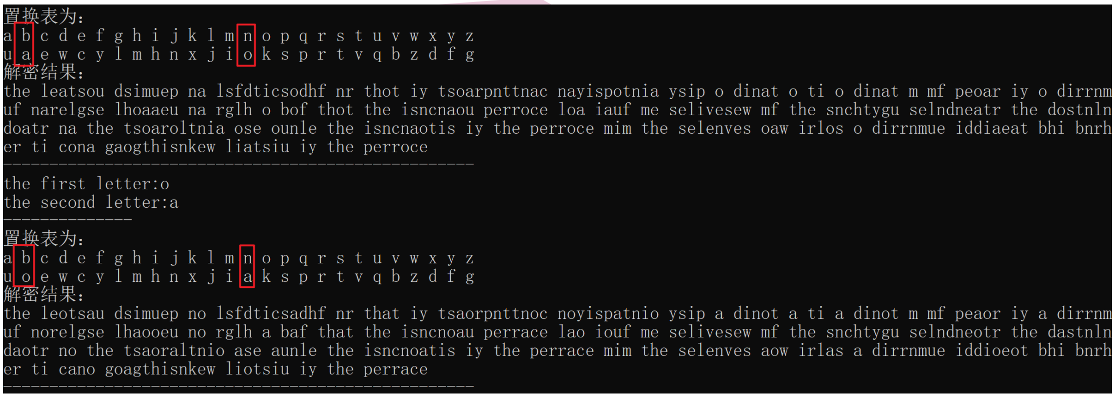
E:\vmware\Sharefile\Cryptography\Lab1\Project1\Debug\Project1.exe

```
----------------------------------
c:0.106825
s:0.0979228
n:0.0919881
m:0.0860534
b:0.0830861
j:0.0830861
p:0.0682493
r:0.0623145
i:0.0534125
g:0.041543
x:0.0356083
a:0.0296736
e:0.0267062
h:0.0267062
q:0.0237389
f:0.0207715
y:0.0207715
z:0.0148368
d:0.00890208
v:0.00890208
t:0.00593472
o:0.00296736
k:0
l:0
u:0
w:0
置换表为:
c s n m b j p r i g x a e h q f y z d v t o k l u w
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
解密结果:
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 t
he snchtygu selndneatr the dostnlndoatr na the tsoaroltnia ose ounle the isncnaotis iy the perroce mim
the selenves oaw irlos o dirrnmue iddiaeat bhi bnrher ti cona gaogthisnkew liatsiu iy the perroce
---------------------------------------------------
```

图 12: 明文字母出现频率

3. 观察解密后的文本，根据英文特征修改置换表：

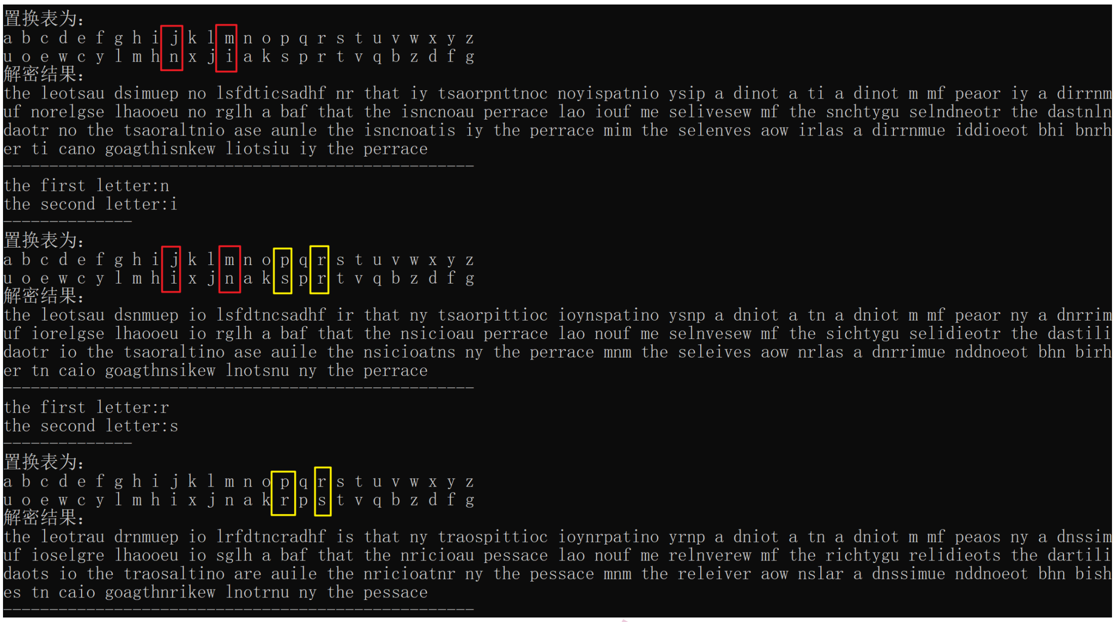
（1）在第一次解密后，发现文本中单个字母 “o” 的出现频率非常高，由此可以推测 “o” 实际应该为 “a”：



```
置换表为:
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
u a e w c y l m h n x j i o k s p r t v q b z d f g
解密结果:
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
---------------------------------------------------
the first letter:o
the second letter:a
--------------
置换表为:
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
u o e w c y l m h n x j i a k s p r t v q b z d f g
解密结果:
the leotsau dsimuep no lsfdticsadhf nr that iy tsaorpnttnoc noyispatnio ysip a dinot a ti a dinot m mf peaor iy a dirrnm
uf norelgse lhaooeu no rglh a baf that the isncnoau perrace lao iouf me selivesew mf the snchtygu selndneotr the dastnln
daotr no the tsaoraltnio ase aunle the isncnoatis iy the perrace mim the selenves aow irlas a dirrnmue iddioeot bhi bnrh
er ti cano goagthisnkew liotsiu iy the perrace
---------------------------------------------------
```

图 13: o<->a

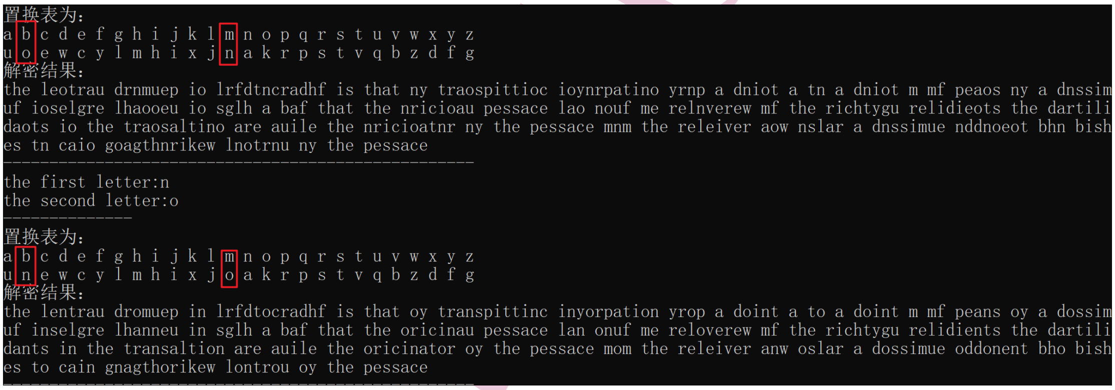
（2）”nr” 跟在 “that” 前，推测 “nr” 实际为 “is”：



```
置换表为:
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
u o e w c y l m h n x j i a k s p r t v q b z d f g
解密结果:
the leotsau dsimuep no lsfdticsadhf nr that iy tsaorpnttnoc noyispatnio ysip a dinot a ti a dinot m mf peaor iy a dirrnm
uf norelgse lhaooeu no rglh a baf that the isncnoau perrace lao iouf me selivesew mf the snchtygu selndneotr the dastnln
daotr no the tsaoraltnio ase aunle the isncnoatis iy the perrace mim the selenves aow irlas a dirrnmue iddioeot bhi bnrh
er ti cano goagthisnkew liotsiu iy the perrace
------------------------------------------------
the first letter:n
the second letter:i
--------------
置换表为:
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
u o e w c y l m h i x j n a k s p r t v q b z d f g
解密结果:
the leotsau dsnmuep io lsfdtncsadhf ir that ny tsaorpittioc ioynspatino ysnp a dniot a tn a dniot m mf peaor ny a dnrrim
uf iorelgse lhaooeu io rglh a baf that the nsicioau perrace lao nouf me selnvesew mf the sichtygu selidieotr the dastili
daotr io the tsaoraltino ase auile the nsicioatns ny the perrace mnm the seleives aow nrlas a dnrrimue nddnoeot bhn birh
er tn caio goagthnsikew lnotsnu ny the perrace
------------------------------------------------
the first letter:r
the second letter:s
--------------
置换表为:
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
u o e w c y l m h i x j n a k r p s t v q b z d f g
解密结果:
the leotrau drnmuep io lrfdtncradhf is that ny traospittioc ioynrpatino yrnp a dniot a tn a dniot m mf peaos ny a dnssim
uf ioselgre lhaooeu io sglh a baf that the nricioau pessace lao nouf me relnverew mf the richtygu relidieots the dartili
daots io the traosaltino are auile the nricioatnr ny the pessace mnm the releiver aow nslar a dnssimue nddnoeot bhn bish
es tn caio goagthnrikew lnotrnu ny the pessace
------------------------------------------------
```

图 14: n<->i,r<->s

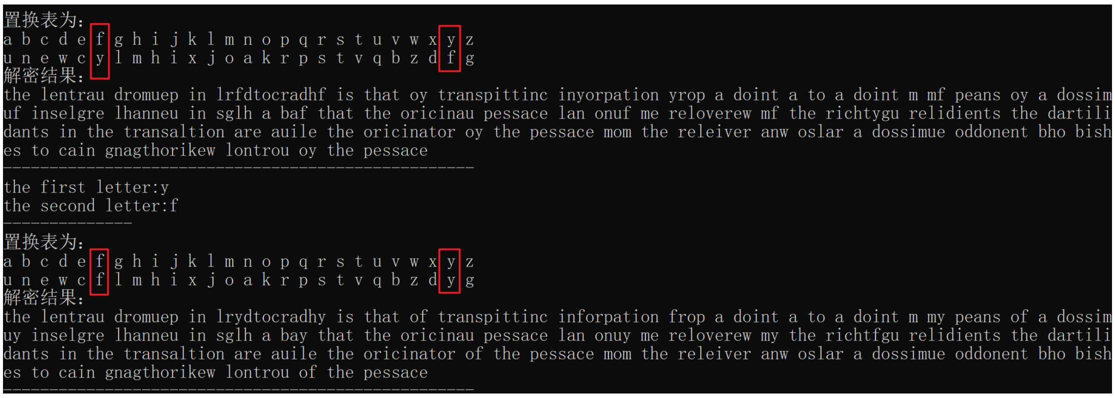
（3）新解密出的明文中有”a doint a tn a doint m”，推测”tn” 应该为”to”



```
置换表为:
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
u o e w c y l m h i x j n a k r p s t v q b z d f g
解密结果:
the leotrau drnmuep io lrfdtncradhf is that ny traospittioc ioynrpatino yrnp a dniot a tn a dniot m mf peaos ny a dnssim
uf ioselgre lhaooeu io sglh a baf that the nricioau pessace lao nouf me relnverew mf the richtygu relidieots the dartili
daots io the traosaltino are auile the nricioatnr ny the pessace mnm the releiver aow nslar a dnssimue nddnoeot bhn bish
es tn caio goagthnrikew lnotrnu ny the pessace
------------------------------------------------
the first letter:n
the second letter:o
--------------
置换表为:
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
u n e w c y l m h i x j o a k r p s t v q b z d f g
解密结果:
the lentrau dromuep in lrfdtocradhf is that oy transpittinc inyorpation yrop a doint a to a doint m mf peans oy a dossim
uf inselgre lhanneu in sglh a baf that the oricinau pessace lan onuf me reloverew mf the richtygu relidients the dartili
dants in the transaltion are auile the oricinator oy the pessace mom the releiver anw oslar a dossimue oddonent bho bish
es to cain gnagthorikew lontrou oy the pessace
------------------------------------------------
```

图 15: n<->o

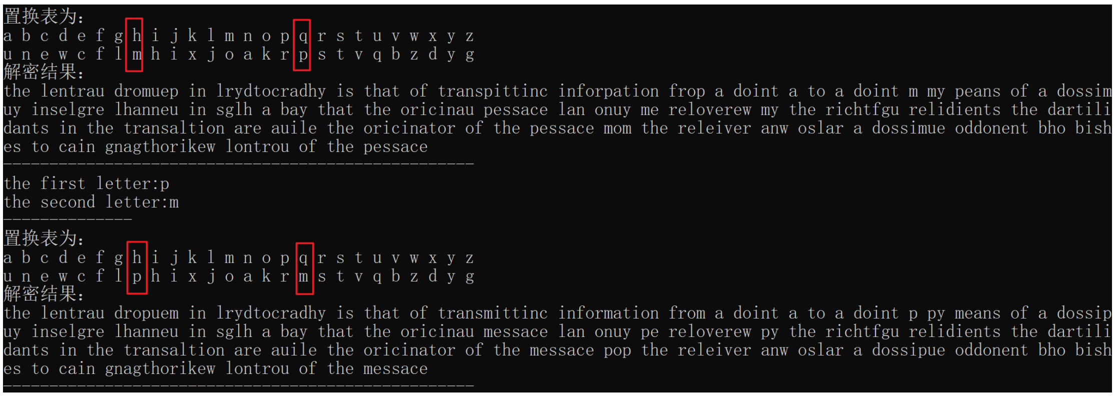
（4）存在”is that oy” 推测”oy” 应该为”of”：



```
置换表为:
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
u n e w c y l m h i x j o a k r p s t v q b z d f g
解密结果:
the lentrau dromuep in lrfdtocradhf is that oy transpittinc inyorpation yrop a doint a to a doint m mf peans oy a dossim
uf inselgre lhanneu in sglh a baf that the oricinau pessace lan onuf me reloverew mf the richtygu relidients the dartili
dants in the transaltion are auile the oricinator oy the pessace mom the releiver anw oslar a dossimue oddonent bho bish
es to cain gnagthorikew lontrou oy the pessace
------------------------------------------------
the first letter:y
the second letter:f
--------------
置换表为:
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
u n e w c f l m h i x j o a k r p s t v q b z d y g
解密结果:
the lentrau dromuep in lrydtocradhy is that of transpittinc inforpation frop a doint a to a doint m my peans of a dossim
uy inselgre lhanneu in sglh a bay that the oricinau pessace lan onuy me reloverew my the richtfgu relidients the dartili
dants in the transaltion are auile the oricinator of the pessace mom the releiver anw oslar a dossimue oddonent bho bish
es to cain gnagthorikew lontrou of the pessace
------------------------------------------------
```

图 16: y<->f

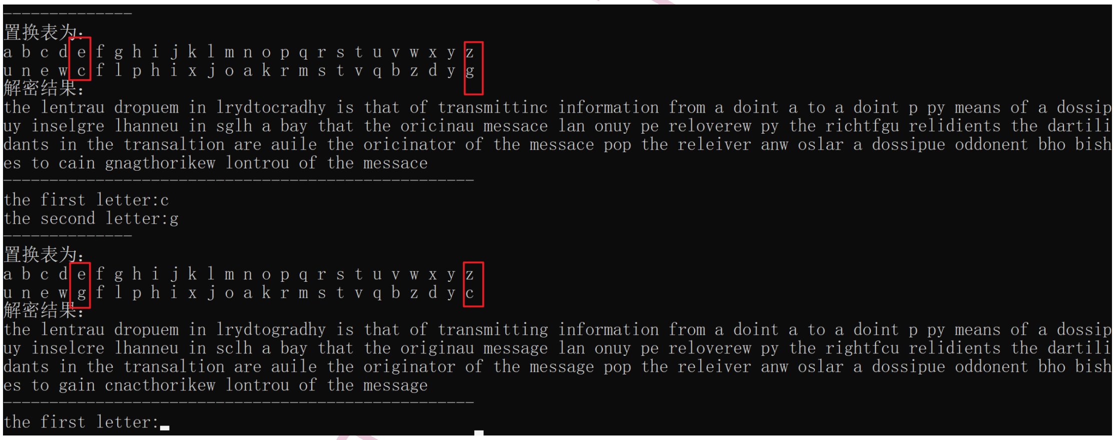
（5）继续分析在（3）中出现的语句“frop a doint a tn a doint m”，很明显这里是“from..to..”，所以将 p 与 m 对换：



```
置换表为:
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
u n e w c f l m h i x j o a k r p s t v q b z d y g
解密结果:
the lentrau dromuep in lrydtocradhy is that of transpittinc inforpation frop a doint a to a doint m my peans of a dossim
uy inselgre lhanneu in sglh a bay that the oricinau pessace lan onuy me reloverew my the richtfgu relidients the dartili
dants in the transaltion are auile the oricinator of the pessace mom the releiver anw oslar a dossimue oddonent bho bish
es to cain gnagthorikew lontrou of the pessace
---------------------------------------------------
the first letter:p
the second letter:m
--------------
置换表为:
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
u n e w c f l p h i x j o a k r m s t v q b z d y g
解密结果:
the lentrau dropuem in lrydtocradhy is that of transmittinc information from a doint a to a doint p py means of a dossip
uy inselgre lhanneu in sglh a bay that the oricinau messace lan onuy pe reloverew py the richtfgu relidients the dartili
dants in the transaltion are auile the oricinator of the messace pop the releiver anw oslar a dossipue oddonent bho bish
es to cain gnagthorikew lontrou of the messace
---------------------------------------------------
```

图 17: p<->m

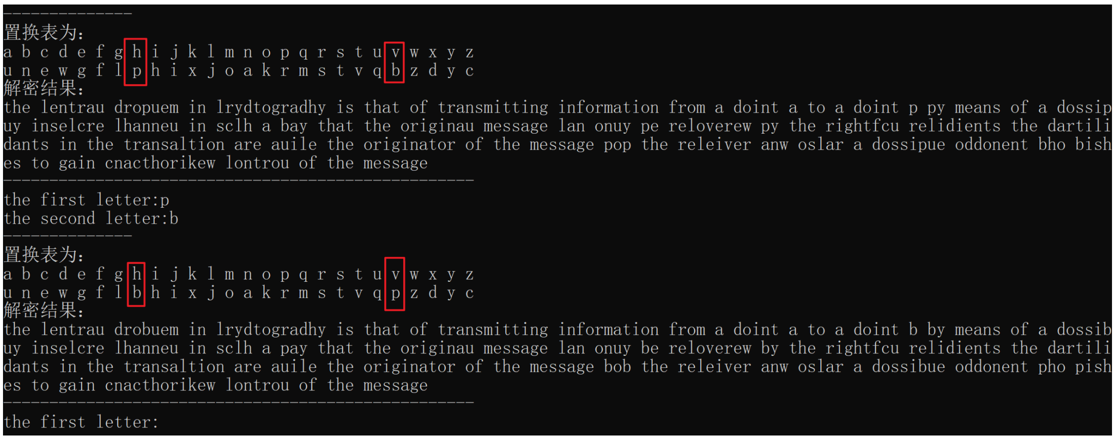
（6）文本结尾处有一个单词“messace”，推测应该为“message”，将 c 与 g 互换：



```
--------------
置换表为:
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
u n e w c f l p h i x j o a k r m s t v q b z d y g
解密结果:
the lentrau dropuem in lrydtocradhy is that of transmittinc information from a doint a to a doint p py means of a dossip
uy inselgre lhanneu in sglh a bay that the oricinau messace lan onuy pe reloverew py the richtfgu relidients the dartili
dants in the transaltion are auile the oricinator of the messace pop the releiver anw oslar a dossipue oddonent bho bish
es to cain gnagthorikew lontrou of the messace
---------------------------------------------------
the first letter:c
the second letter:g
--------------
置换表为:
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
u n e w g f l p h i x j o a k r m s t v q b z d y c
解密结果:
the lentrau dropuem in lrydtogradhy is that of transmitting information from a doint a to a doint p py means of a dossip
uy inselcre lhanneu in sclh a bay that the originau message lan onuy pe reloverew py the rightfcu relidients the dartili
dants in the transaltion are auile the originator of the message pop the releiver anw oslar a dossipue oddonent bho bish
es to gain cnacthorikew lontrou of the message
---------------------------------------------------
the first letter:_
```

图 18: c<->g

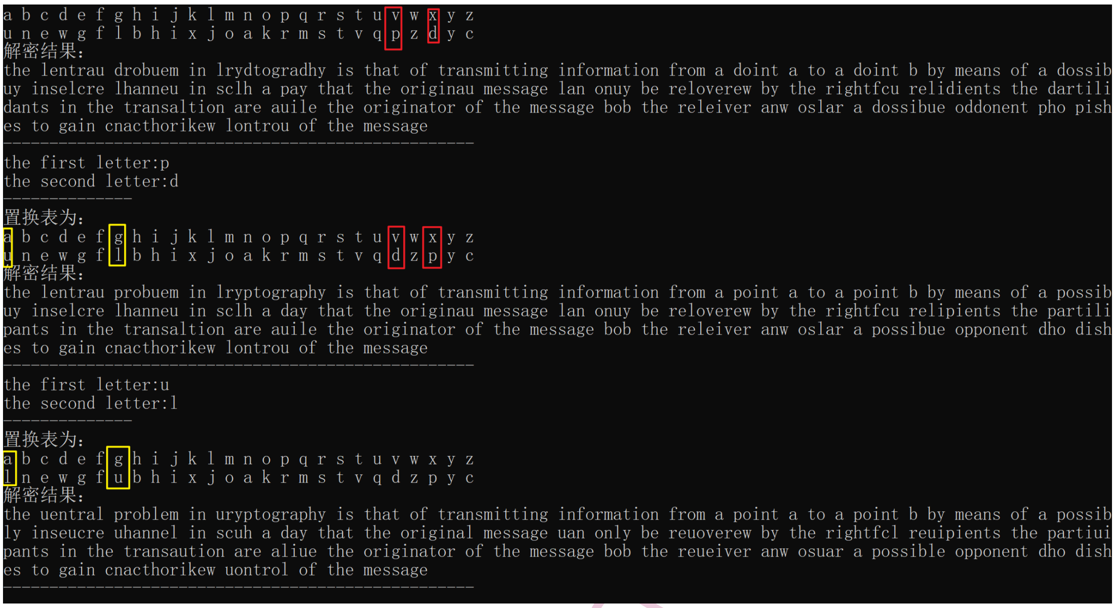
（7）存在短语“py means of”，并且文本中也出现了“py”，推测应该是“by means of”和“by”，所以将 p 与 b 对换：



```
--------------
置换表为:
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
u n e w g f l p h i x j o a k r m s t v q b z d y c
解密结果:
the lentrau dropuem in lrydtogradhy is that of transmitting information from a doint a to a doint p py means of a dossip
uy inselcre lhanneu in sclh a bay that the originau message lan onuy pe reloverew py the rightfcu relidients the dartili
dants in the transaltion are auile the originator of the message pop the releiver anw oslar a dossipue oddonent bho bish
es to gain cnacthorikew lontrou of the message
---------------------------------------------------
the first letter:p
the second letter:b
--------------
置换表为:
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
u n e w g f l b h i x j o a k r m s t v q p z d y c
解密结果:
the lentrau drobuem in lrydtogradhy is that of transmitting information from a doint a to a doint b by means of a dossib
uy inselcre lhanneu in sclh a pay that the originau message lan onuy be reloverew by the rightfcu relidients the dartili
dants in the transaltion are auile the originator of the message bob the releiver anw oslar a dossibue oddonent pho pish
es to gain cnacthorikew lontrou of the message
---------------------------------------------------
the first letter:
```

图 19: b<->p

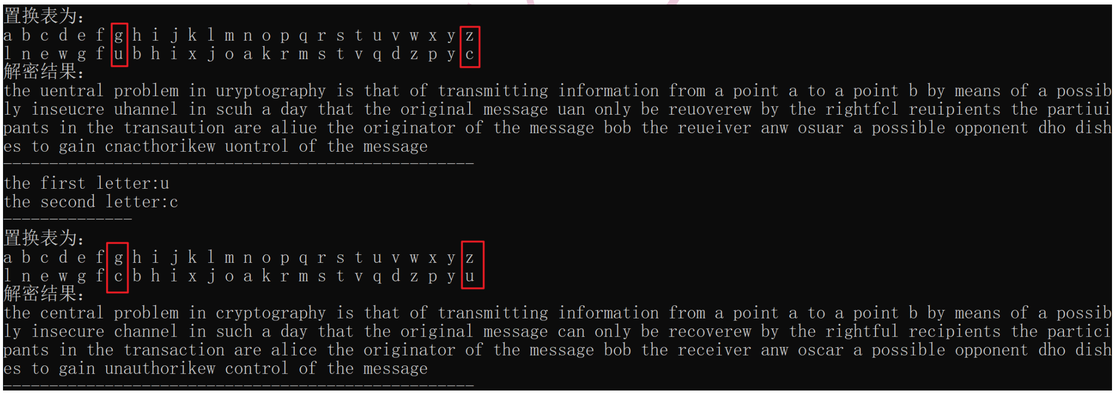
（8）文本中第三个单词为“drobuem”，推测是 problem，所以将 p 和 d 对换、u 和 l 对换:



```
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
u n e w g f l b h i x j o a k r m s t v q p z d y c
解密结果:
the lentrau drobuem in lrydtogradhy is that of transmitting information from a doint a to a doint b by means of a dossib
uy inselcre lhanneu in sclh a pay that the originau message lan onuy be reloverew by the rightfcu relidients the dartili
dants in the transaltion are auile the originator of the message bob the releiver anw oslar a dossibue oddonent pho pish
es to gain cnacthorikew lontrou of the message
-------------------------------------------------

the first letter:p
the second letter:d
-------------
置换表为:
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
u n e w g f l b h i x j o a k r m s t v q d z p y c
解密结果:
the lentrau probuem in lryptography is that of transmitting information from a point a to a point b by means of a possib
uy inselcre lhanneu in sclh a day that the originau message lan onuy be reloverew by the rightfcu relipients the partili
pants in the transaltion are auile the originator of the message bob the releiver anw oslar a possibue opponent dho dish
es to gain cnacthorikew lontrou of the message
-------------------------------------------------

the first letter:u
the second letter:l
-------------
置换表为:
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
l n e w g f u b h i x j o a k r m s t v q d z p y c
解密结果:
the uentral problem in uryptography is that of transmitting information from a point a to a point b by means of a possib
ly inseucre uhannel in scuh a day that the original message uan only be reuoverew by the rightfcl reuipients the partiui
pants in the transaution are aliue the originator of the message bob the reueiver anw osuar a possible opponent dho dish
es to gain cnacthorikew uontrol of the message
-------------------------------------------------
```

图 20: d<->p,u<->l

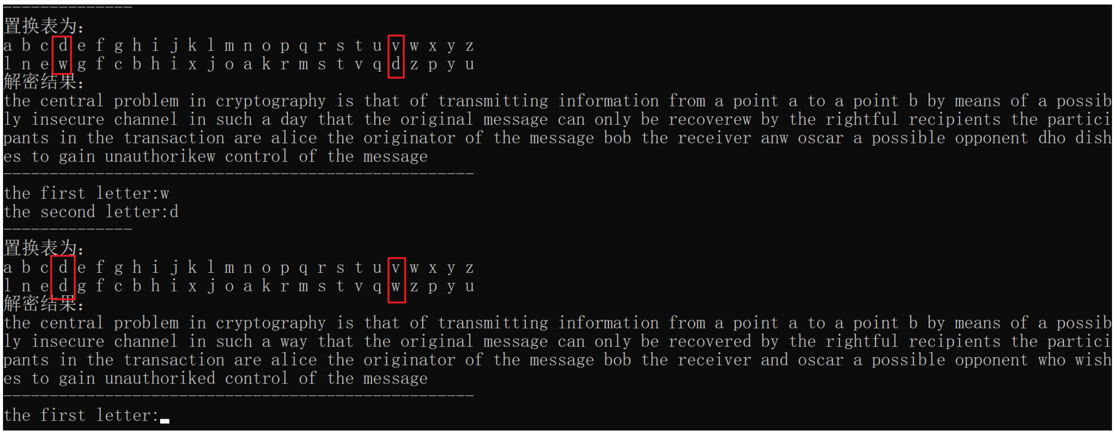
（9）文本中第二个单词为“uentral”，后面还出现了“uan”，推测是“central”和“can”，所以将 u 和 c 对换:



```
置换表为:
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
l n e w g f u b h i x j o a k r m s t v q d z p y c
解密结果:
the uentral problem in uryptography is that of transmitting information from a point a to a point b by means of a possib
ly inseucre uhannel in scuh a day that the original message uan only be reuoverew by the rightfcl reuipients the partiui
pants in the transaution are aliue the originator of the message bob the reueiver anw osuar a possible opponent dho dish
es to gain cnacthorikew uontrol of the message
-------------------------------------------------

the first letter:u
the second letter:c
-------------
置换表为:
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
l n e w g f c b h i x j o a k r m s t v q d z p y u
解密结果:
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 day that the original message can only be recoverew by the rightful recipients the partici
pants in the transaction are alice the originator of the message bob the receiver anw oscar a possible opponent dho dish
es to gain unauthorikew control of the message
-------------------------------------------------
```

图 21: u<->c

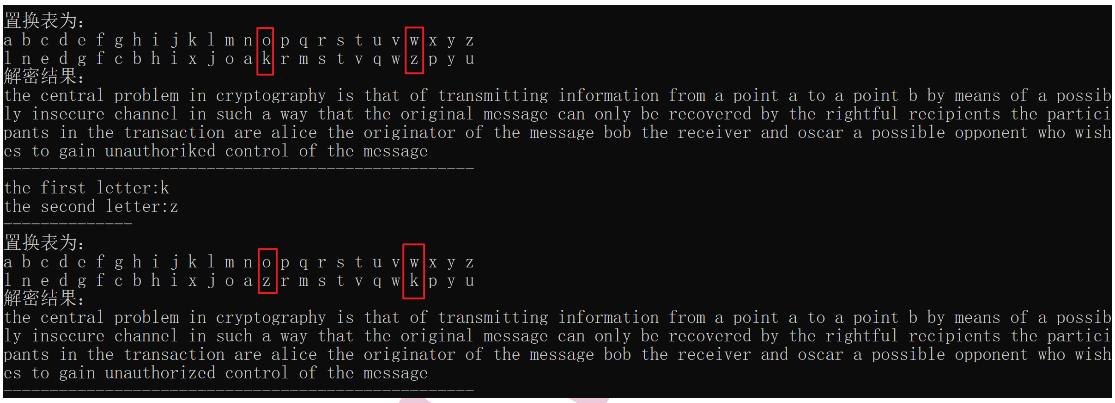
（10）文本中出现了“recoverew”和“anw”，推测应该为“recovered”和“and”，所以将 w 与 d 对换:



```
--------------
置换表为:
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
l n e w g f c b h i x j o a k r m s t v q d z p y u
解密结果:
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 day that the original message can only be recoverew by the rightful recipients the partici
pants in the transaction are alice the originator of the message bob the receiver anw oscar a possible opponent dho dish
es to gain unauthorikew control of the message
---------------------------------------------------
the first letter:w
the second letter:d
--------------
置换表为:
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
l n e d g f c b h i x j o a k r m s t v q w z p y u
解密结果:
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
---------------------------------------------------
the first letter:
```

图 22: w<->d

（11）在最后出现了单词“unauthoriked”，推测应该为“unauthorized”，所以将 k 和 z 对换：



```
置换表为:
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
l n e d g f c b h i x j o a k r m s t v q w z p y u
解密结果:
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
---------------------------------------------------
the first letter:k
the second letter:z
--------------
置换表为:
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
l n e d g f c b h i x j o a z r m s t v q w k p y u
解密结果:
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
---------------------------------------------------
```

图 23: k<->z

经过上述步骤之后，已经得到了通顺的语句，解密得到的明文为：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