

# 实验一 古典密码算法及攻击方法

## 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、实验原理

### 1、移位密码

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）。

### 2、对移位密码的攻击

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。

### 3、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。

### 4、对单表置换密码的攻击方法

在单表置换密码中，由于置换表字母组合方式有 $26!$ 种，约为 $4.03 \times 10^{26}$ 。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有短单词，常用单词，字母频率。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。

## 三、实验环境

运行Windows操作系统的PC机，具有VC等语言编译环境

## 四、实验内容和步骤

(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。

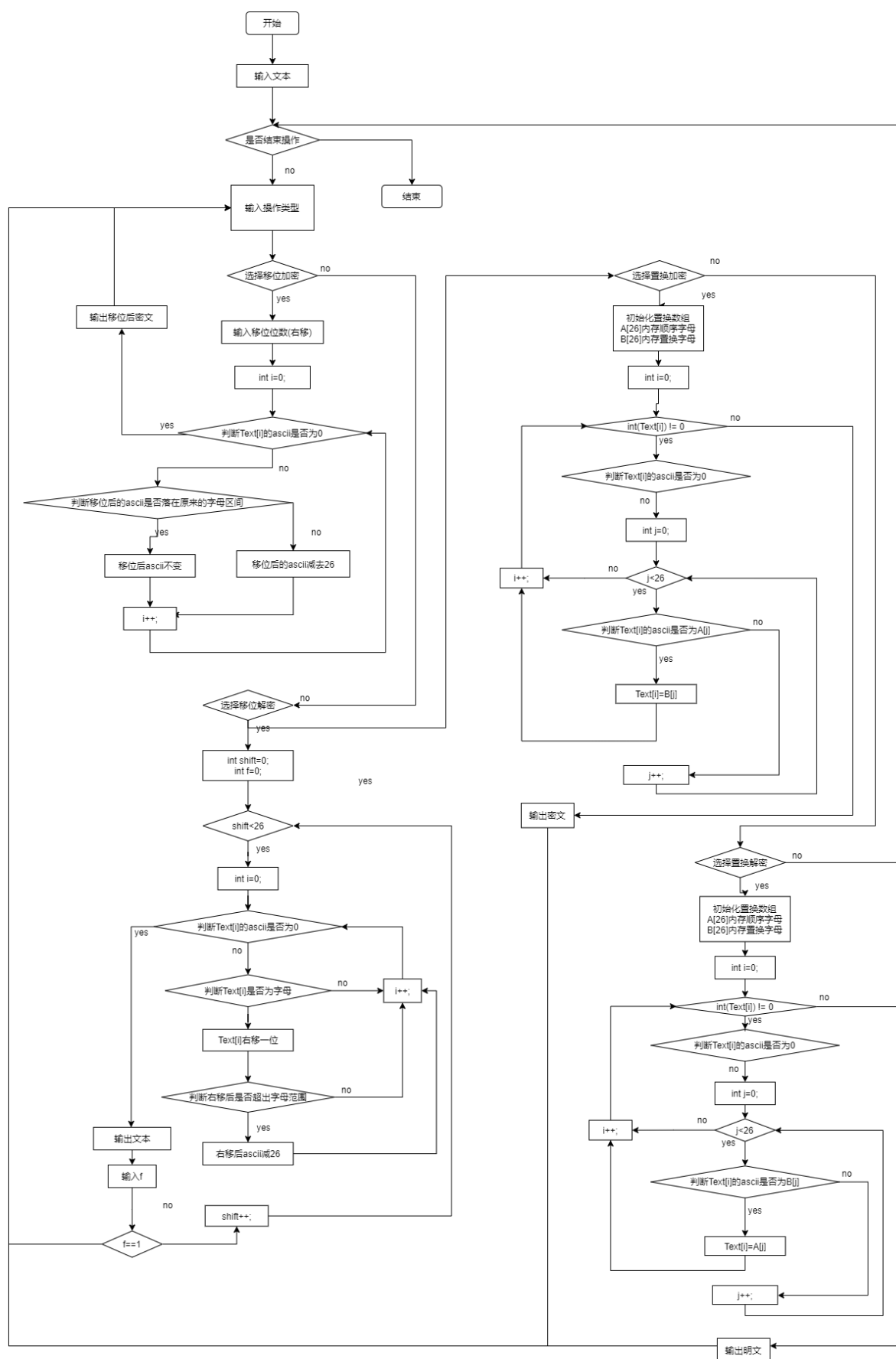
(3) 自己创建明文信息，并选择一个密钥，构建置换表。编写置换密码的加解密实现程序，实现加密和解密操作。

(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 JBRGZPC GINBBCA JB RZGI N VNY SINS SIC  
MPJEJBNQ QRRNEC GNB MBAY HC PCGMTCPD HY SIC PJEISFZA PCGJXJCSR SIC XNPSJGJXNBSR  
JB SIC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QRRNEC HMH SIC PCGCJTCP NBD

写出获得的明文消息和置换表。

下面是移位加密，移位解密，置换加密，置换解密的算法流程图。



## 六、加密解密结果

### (一) 移位加密

选择下面这段话进行移位加密

The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export.

选择密钥为23，下面是移位23位后得到的结果

Qeb doltqe lc zovmqldoxmefz qbzekliildv exp oxfpba x krjybo lc ibdxi fpprbp fk qeb fkclojxqflk xdb. Zovmqldoxmefz'p mlqbkqfxi clo rpb xp x qlli clo bpmflkxdb xka pbaqfqlk exp iba jxkv dlsbokjbkqp ql zixppfcv fq xp x tbxmlk xka ql ifjq lo bsbk molefyfq fqp rpb xka bumloq.

```
请输入你的文本
The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export.
请输入操作类型
移位加密1
移位解密2
单表置换加密3
单表置换解密4
退出0
1
Please input your shift:23
密文为:
Qeb doltqe lc zovmqldoxmefz qbzekliildv exp oxfpba x krjybo lc ibdxi fpprbp fk qeb fkclojxqflk xdb. Zovmqldoxmefz'p mlqbkqfxi clo rpb xp x qlli clo bpmflkxdb xka pbaqfqlk exp iba jxkv dlsbokjbkqp ql zixppfcv fq xp x tbxmlk xka ql ifjq lo bsbk molefyfq fqp rpb xka bumloq.
-----
请输入操作类型
移位加密1
移位解密2
单表置换加密3
单表置换解密4
退出0
2
明文为:
Rfc epmurf md apwnrmepynfga rcaflmjmw fyq pygqcb y lskzcp md jceyj gqqsq gl rfc gldmpkyrgml yec. Apwnrmepynfw'q nmrlrgyj dmp sqc yq y rnmj dmp cqnsmlyec ylb qcbgrgml fyq jcb kylw emtcplkclrq rm ayyqagdw gr yq y ucynml ylb rm jekgr mp ctcl nmpfgzgr grq sqc ylb cvnmpr.
找到了吗? 找到请输入1, 没有的话输入0:0
明文为:
Sgd fqnvsg ne bqxsnsfzqoghb sdbgmknfx gzer qzhrdc z mtladq ne kdfzk hrrtdr hm sgd hmenqlzshnm zfd. Bqxsnsfzqogx'r onsdmshzk enq trd zr z snnk enq drohnmzfd zmc rdchshnm gzer kdc lzmz fnudqldmsr sn bkzrrhex hs zr z vdzonm zmc sn khlhs nq dudm oqngahs hsr trd zmc dwonqs.
找到了吗? 找到请输入1, 没有的话输入0:0
明文为:
The growth of cryptographic technology has raised a number of legal issues in the information age. Cryptography's potential for use as a tool for espionage and sedition has led many governments to classify it as a weapon and to limit or even prohibit its use and export.
找到了吗? 找到请输入1, 没有的话输入0:1
-----
请输入操作类型
移位加密1
移位解密2
单表置换加密3
单表置换解密4
退出0
0
C:\Users\86158\source\repos\密码实验一\Release\密码实验一.exe (进程 17296)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。...
```

### (二) 移位解密

从一位同学那里获得了加密后的密文

GUR PNG VF FB PHGR! V ERNYL JNAG GB UNIR BAR.

解密后得到如下结果

THE CAT IS SO CUTE! I REALLY WANT TO HAVE ONE.

```

请输入你的文本
GUR PNG VF FB PHGR! V ERNYL JNAG GB UNIR BAR.
请输入操作类型
移位加密1
移位解密2
单表置换加密3
单表置换解密4
退出0
2
明文为:
HVS QOH WG GC QIHS! W FSOZZM KOBH HC VOJS CBS.
找到了吗? 找到请输入1, 没有的话输0:0
明文为:
IWT RPI XH HD RJIT! X GTPAAN LPCI ID WPKT DCT.
找到了吗? 找到请输入1, 没有的话输0:0
明文为:
JXU SQJ YI IE SKJU! Y HUQBBO MQDJ JE XQLU EDU.
找到了吗? 找到请输入1, 没有的话输0:0
明文为:
KYV TRK ZJ JF TLKV! Z IVRCCP NREK KF YRMV FEV.
找到了吗? 找到请输入1, 没有的话输0:0
明文为:
LZW USL AK KG UMLW! A JWSDDQ OSFL LG ZSNW GFW.
找到了吗? 找到请输入1, 没有的话输0:0
明文为:
MAX VTM BL LH VNMX! B KXTEER PTGM MH ATOX HGX.
找到了吗? 找到请输入1, 没有的话输0:0
明文为:
NBY WUN CM MI WONY! C LYUFFS QUHN NI BUPY IHY.
找到了吗? 找到请输入1, 没有的话输0:0
明文为:
OCZ XVO DN NJ XPOZ! D MZVGGT RVIO OJ CVQZ JIZ.
找到了吗? 找到请输入1, 没有的话输0:0
明文为:
PDA YWP EO OK YQPA! E NAWHHU SWJP PK DWRA KJA.
找到了吗? 找到请输入1, 没有的话输0:0
明文为:
QEB ZXQ FP PL ZRQB! F OBXIIV TXKQ QL EXSB LKB.
找到了吗? 找到请输入1, 没有的话输0:0
明文为:
RFC AYR GQ QM ASRC! G PCYJJW UYLR RM FYTC MLC.
找到了吗? 找到请输入1, 没有的话输0:0
明文为:
SGD BZS HR RN BTSD! H QDZKKX VZMS SN GZUD NMD.
找到了吗? 找到请输入1, 没有的话输0:0
明文为:
THE CAT IS SO CUTE! I REALLY WANT TO HAVE ONE.
找到了吗? 找到请输入1, 没有的话输0:1

```

### (三) 置换加密及解密

选择下面这段话进行加密解密

THE GROWTH OF CRYPTOGRAPHIC TECHNOLOGY HAS RAISED A NUMBER OF LEGAL ISSUES IN THE INFORMATION AGE. CRYPTOGRAPHY'S POTENTIAL FOR USE AS A TOOL FOR ESPIONAGE AND SEDITION HAS LED MANY GOVERNMENTS TO CLASSIFY IT AS A WEAPON AND TO LIMIT OR EVEN PROHIBIT ITS USE AND EXPORT.

加密后得到如下密文

FGX SNZDFG ZY WNUMFZSNHMG BW FXWGAZEZSU GH O NHBOXT H ACJKXN ZY EXSHE BOOCXO BA FGX BAYZNJHFBZA HSX. WNUMFZSNHMGU'O MZFXAFBHE YZN COX HO H FZZE YZN XOMBZAH SX HAT OXTBFBZA GH O EXT JHAU SZIXNAJXAFO FZ WEHOOBYU BF HO H DXHMZA HAT FZ EBJBF ZN XIXA MNZGBKBF BFO COX HAT XVMZNF.

解密后得到和明文相同的文本

THE GROWTH OF CRYPTOGRAPHIC TECHNOLOGY HAS RAISED A NUMBER OF LEGAL ISSUES IN THE INFORMATION AGE. CRYPTOGRAPHY'S POTENTIAL FOR USE AS A TOOL FOR ESPIONAGE AND SEDITION HAS LED MANY GOVERNMENTS TO CLASSIFY IT AS A WEAPON AND TO LIMIT OR EVEN PROHIBIT ITS USE AND EXPORT.

```

请输入你的文本
THE GROWTH OF CRYPTOGRAPHIC TECHNOLOGY HAS RAISED A NUMBER OF LEGAL ISSUES IN THE INFORMATION AGE. CRYPTOGRAPHY'S POTENTIAL FOR USE AS A
TOOL FOR ESPIONAGE AND SEDITION HAS LED MANY GOVERNMENTS TO CLASSIFY IT AS A WEAPON AND TO LIMIT OR EVEN PROHIBIT ITS USE AND EXPORT.
请输入操作类型
移位加密1
移位解密2
单表置换加密3
单表置换解密4
退出0
3
密文为：
FGX SNZDFG ZY WNUMFZSNHMGW FXWGAZEZSU GHQ NHBOXI H ACJKXN ZY EXSHE BOOCXO BA FGX BAYZNJHFBZA HSX. WNUMFZSNHMGU'O MZFXAFBHE YZN COX HO H
FZZE YZN XOMBZAHSX HAT OXTBFBZA GHQ EXT JHAU SZIXNAJXAFO FZ WEHOBYU BF HO H DXHMA HAT FZ EBJBF ZN XIXA MNZGBKBF BFO COX HAT XVMZNF.
-----
请输入操作类型
移位加密1
移位解密2
单表置换加密3
单表置换解密4
退出0
4
明文为：
THE GROWTH OF CRYPTOGRAPHIC TECHNOLOGY HAS RAISED A NUMBER OF LEGAL ISSUES IN THE INFORMATION AGE. CRYPTOGRAPHY'S POTENTIAL FOR USE AS A
TOOL FOR ESPIONAGE AND SEDITION HAS LED MANY GOVERNMENTS TO CLASSIFY IT AS A WEAPON AND TO LIMIT OR EVEN PROHIBIT ITS USE AND EXPORT.
-----
请输入操作类型
移位加密1
移位解密2
单表置换加密3
单表置换解密4
退出0
0
C:\Users\86158\source\repos\密码实验一\Release\密码实验一.exe (进程 7384)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。 . .

```

## 七、字母频率统计攻击

### 确定E,T(字母频率)

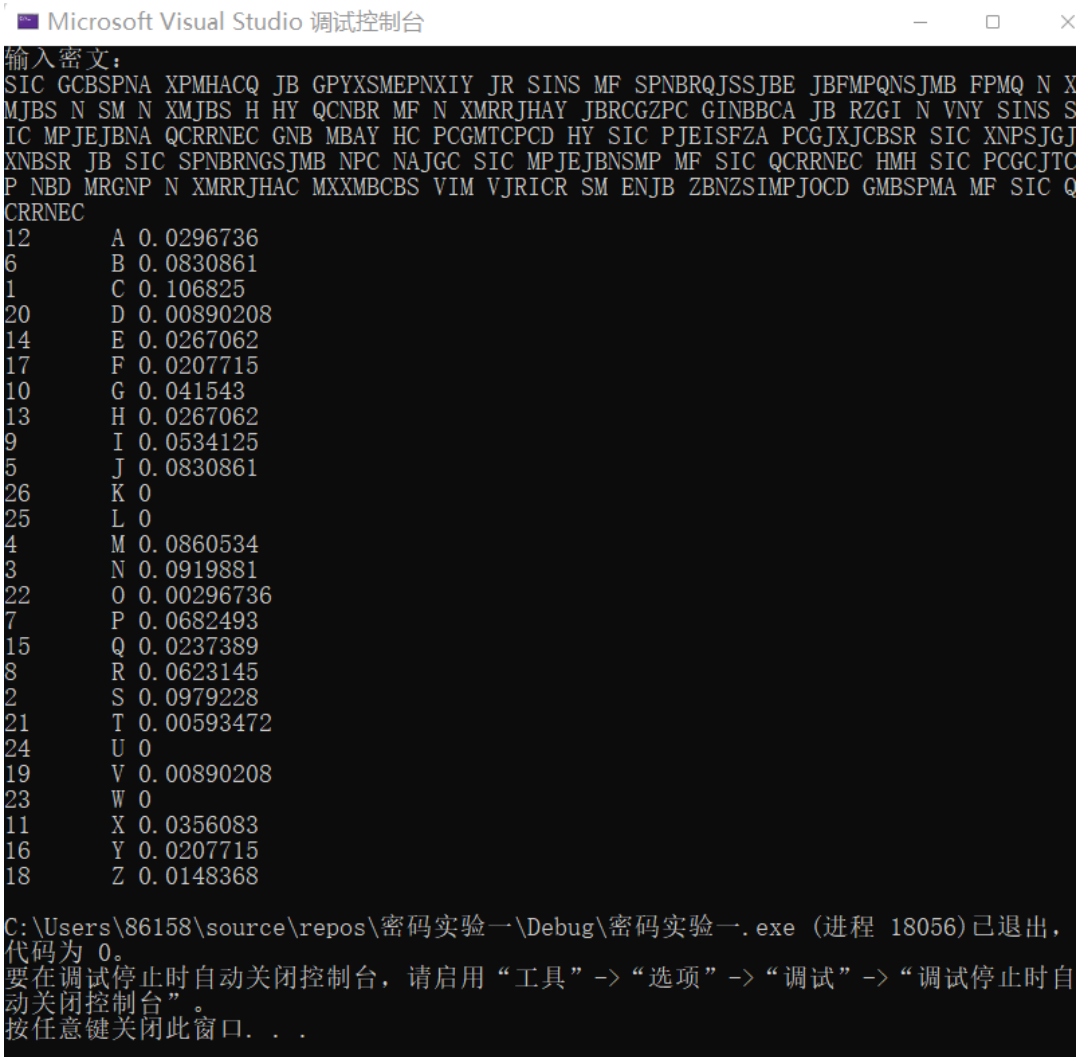
```

1  #include<iostream>
2  using namespace std;
3  int main()
4  {
5      char Cipher[1000];
6      int A[26],C[26];
7      double B[26];
8      for (int i = 0; i < 26; i++)
9      {
10         A[i] = 0;
11     }
12     cout << "输入密文: " << endl;
13     cin.getline(Cipher, 1000);
14     for (int i = 0; int(Cipher[i]) != 0; i++)
15     {
16         if (int(Cipher[i]) < 65 || int(Cipher[i]) > 90)
17             continue;
18         A[int(Cipher[i]) - 65]++;
19     }
20     double sum = 0.0;
21     for (int i = 0; i < 26; i++)sum += A[i];
22     for (int i = 0; i < 26; i++)
23     {
24         B[i] = A[i] / sum;
25         C[i] = 1;
26     }
27     for (int i = 1; i < 26; i++)
28     {
29         for (int j = 0; j < i; j++)
30         {
31             if (B[i] >= B[j])C[j]++;
32             else C[i]++;
33         }
34     }
35     for (int i = 0; i < 26; i++)
36     {

```

```
37     cout << C[i] << "\t" << char(i + 65) << " " << B[i] << endl;
38 }
39 }
```

结果如图



得到频率最高的字母为C，其次为S。

置换表

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
		E		C														T	S						

确定A,I(单字母单词)

由于这里密文量不大，所以不计算频率，直接判断

```
1  #include<iostream>
2  using namespace std;
3  int main()
4  {
5      char cipher[1000];
6      cout << "输入密文: " << endl;
7      cin.getline(cipher, 1000);
8      int A[26], C[26];
9      double B[26];
10     for (int i = 1; int(cipher[i + 1]) != 0; i++)
11     {
12         if (int(cipher[i - 1]) == 32 && int(cipher[i + 1]) == 32)
```

```

13     {
14         cout << Cipher[i] << " ";
15     }
16 }
17 }

```

输入密文：  
SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFMPQNSJMB FPMQ N X  
MJBS N SM N XMJBS H HY QCNR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SINS S  
IC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJ  
XNBSR JB SIC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTC  
P NBD MRGNP N XMRRJHAC MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOC D GMBSPMA MF SIC Q  
CRRNEC  
N N N H N N N  
C:\Users\86158\source\repos\密码实验一\Debug\密码实验一.exe (进程 16640) 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。 . . .

得到单字母单词为6个N和1个H。由于具有偶然性，所以先将N对应A，H对应I，后续出现错误再修改。

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		E		C			I	H					A					T	S						

按照上述置换表进行替换，下面为替换代码

```

1  #include<iostream>
2  using namespace std;
3  int main()
4  {
5      char Cipher[1000];
6      cout << "输入密文: " << endl;
7      cin.getline(Cipher, 1000);
8      for (int i = 0; int(Cipher[i]) != 0; i++)
9      {
10         if (Cipher[i] == 'A')Cipher[i] = 'N';
11         else
12         if (Cipher[i] == 'I')Cipher[i] = 'H';
13         else
14         if (Cipher[i] == 'C')Cipher[i] = 'E';
15         else
16         if (Cipher[i] == 'S')Cipher[i] = 'T';
17         else
18         if (Cipher[i] == 'N')Cipher[i] = 'A';
19         else
20         if (Cipher[i] == 'H')Cipher[i] = 'I';
21         else
22         if (Cipher[i] == 'E')Cipher[i] = 'C';
23         else
24         if (Cipher[i] == 'T')Cipher[i] = 'S';
25     }
26     cout << Cipher;
27 }

```

```

输入密文：
SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFMPQNSJMB FPMQ N X
MJBS N SM N XMJBS H HY QCNR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SINS S
IC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJ
XNBSR JB SIC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTC
P NBD MRGNP N XMRRJHAC MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOCD GMBSPMA MF SIC Q
CRRNEC
THE GEBTPAN XPMINEQ JB GPYXTMCPAXHY JR THAT MF TPABRQJTTJBC JBFMPQATJMB FPMQ A X
MJBT A TM A XMJBT I IY QEABR MF A XMRRJINY JBREGZPE GHABEN JB RZGH A VAY THAT T
HE MPJCJBAN QERRACE GAB MBNY IE PEGMSEPED IY THE PJCHTFZN PEGJXJEBTR THE XAPTJGJ
XABTR JB THE TPABRAGTJMB APE ANJGE THE MPJCJBATMP MF THE QERRACE IMI THE PEGEJSE
P ABD MRGAP A XMRRJINE MXXMBEBT VHM VJRHER TM CAJB ZBAZTHMPJOED GMBTPMN MF THE Q
ERRACE

```

## 确定H(三字母单词the)

由于这里单词量很少，所以直接看

出现the这个单词

```

MICROSOFT VISUAL STUDIO 调试控制台
输入密文：
THE GEBTPAN XPMINEQ JB GPYXTMCPAXHY JR THAT MF TPABRQJTTJBC JBFMPQATJMB FPMQ A X
MJBT A TM A XMJBT I IY QEABR MF A XMRRJINY JBREGZPE GHABEN JB RZGH A VAY THAT T
HE MPJCJBAN QERRACE GAB MBNY IE PEGMSEPED IY THE PJCHTFZN PEGJXJEBTR THE XAPTJGJ
XABTR JB THE TPABRAGTJMB APE ANJGE THE MPJCJBATMP MF THE QERRACE IMI THE PEGEJSE
P ABD MRGAP A XMRRJINE MXXMBEBT VHM VJRHER TM CAJB ZBAZTHMPJOED GMBTPMN MF THE Q
ERRACE
THE VAY THE GAB THE THE THE APE THE THE IMI THE ABD VHM THE
C:\Users\86158\source\repos\密码实验一\Debug\密码实验一.exe (进程 13244) 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。 . . .

```

置换表

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		E		C			I	H					A					T	S						

## 确定O,F(两字母单词to,of)

```

输入密文：
THE GEBTPAN XPMINEQ JB GPYXTMCPAXHY JR THAT MF TPABRQJTTJBC JBFMPQATJMB FPMQ A X
MJBT A TM A XMJBT I IY QEABR MF A XMRRJINY JBREGZPE GHABEN JB RZGH A VAY THAT T
HE MPJCJBAN QERRACE GAB MBNY IE PEGMSEPED IY THE PJCHTFZN PEGJXJEBTR THE XAPTJGJ
XABTR JB THE TPABRAGTJMB APE ANJGE THE MPJCJBATMP MF THE QERRACE IMI THE PEGEJSE
P ABD MRGAP A XMRRJINE MXXMBEBT VHM VJRHER TM CAJB ZBAZTHMPJOED GMBTPMN MF THE Q
ERRACE
JB JR MF TM IY MF JB IE IY JB MF TM MF
C:\Users\86158\source\repos\密码实验一\Debug\密码实验一.exe (进程 20448) 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。 . . .

```

MF出现4次，JB出现3次，TM出现2次，IY出现2次，JR和IE分别出现1次

按照频率，因为T已经确定，所以根据to, of, is, in这几个单词，将M确定为O，F确定为F

置换表

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		E		C	F		I	H				O	A	M				T	S						

下面是代换后的结果



```

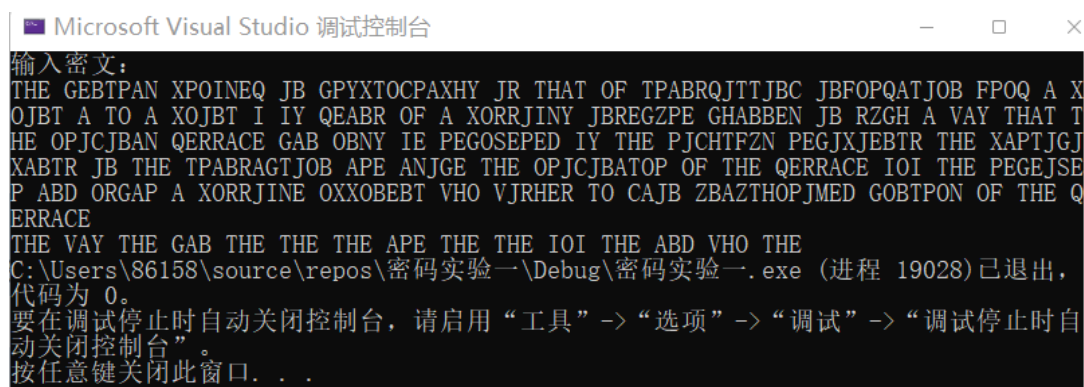
输入密文：
SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFMPQNSJMB FPMQ N X
MJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SINS S
IC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJ
XNBSR JB SIC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTC
P NBD MRGNP N XMRRJHAC MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOC D GMBSPMA MF SIC Q
CRRNEC
THE GEBTPAN XPOINEQ JB GPYXTOCPAXHY JR THAT OF TPABRQJTTJBC JBFOPQATJOB FPOQ A X
OJBT A TO A XOJBT I IY QEABR OF A XORRJINY JBREGZPE GHABEN JB RZGH A VAY THAT T
HE OPJCBAN QERRACE GAB OBNY IE PEGOSEPED IY THE PJCHTFZN PEGJXJEBTR THE XAPTJGJ
XABTR JB THE TPABRAGTJOB APE ANJGE THE OPJCBATOP OF THE QERRACE IOI THE PEGEJSE
P ABD ORGAP A XORRJINE OXXOBEBT VHO VJRHER TO CAJB ZBAZTHOPJMED GOBTPON OF THE Q
ERRACE

```

在这里出现了一些我们认识的单词，比如the,that,of,a,to。

## 确定N,D(三字母单词and)

现在重新进行三个字母单词的检测



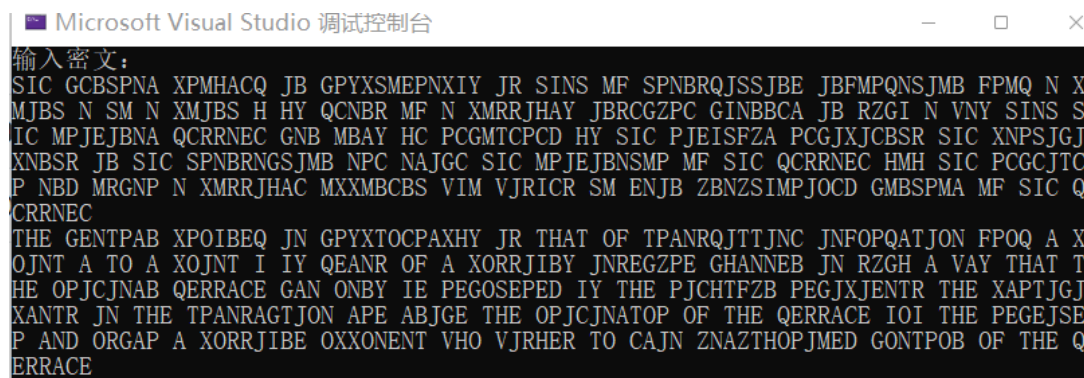
```

Microsoft Visual Studio 调试控制台
输入密文：
THE GEBTPAN XPOINEQ JB GPYXTOCPAXHY JR THAT OF TPABRQJTTJBC JBFOPQATJOB FPOQ A X
OJBT A TO A XOJBT I IY QEABR OF A XORRJINY JBREGZPE GHABEN JB RZGH A VAY THAT T
HE OPJCBAN QERRACE GAB OBNY IE PEGOSEPED IY THE PJCHTFZN PEGJXJEBTR THE XAPTJGJ
XABTR JB THE TPABRAGTJOB APE ANJGE THE OPJCBATOP OF THE QERRACE IOI THE PEGEJSE
P ABD ORGAP A XORRJINE OXXOBEBT VHO VJRHER TO CAJB ZBAZTHOPJMED GOBTPON OF THE Q
ERRACE
THE VAY THE GAB THE THE THE APE THE THE IOI THE ABD VHO THE
C:\Users\86158\source\repos\密码实验一\Debug\密码实验一.exe (进程 19028) 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。 . . .

```

想确定and这一使用频率较高的单词

以上符合条件的只有ABD，所以N-B，D-D



```

Microsoft Visual Studio 调试控制台
输入密文：
SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFMPQNSJMB FPMQ N X
MJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SINS S
IC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJ
XNBSR JB SIC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTC
P NBD MRGNP N XMRRJHAC MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOC D GMBSPMA MF SIC Q
CRRNEC
THE GENTPAB XPOIBEQ JN GPYXTOCPAXHY JR THAT OF TPANRQJTTJNC JNFOPQATJON FPOQ A X
OJNT A TO A XOJNT I IY QEANR OF A XORRJIBY JNREGZPE GHANNEB JN RZGH A VAY THAT T
HE OPJCNAB QERRACE GAN ONBY IE PEGOSEPED IY THE PJCHTFZB PEGJXJENTR THE XAPTJGJ
XANTR JN THE TPANRAGTJON APE ABJGE THE OPJCNATOR OF THE QERRACE IOI THE PEGEJSE
P AND ORGAP A XORRJIBE OXXONENT VHO VJRHER TO CAJN ZNAZTHOPJMED GONTPOB OF THE Q
ERRACE

```

## 确定R,M(单词from)

出现FPOQ，猜测是from，所以P-R，Q-M

置换表

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	N	E	D	C	F		I	H				O	A	Q	R	M		T	S						

```

输入密文：
SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFMPQNSJMB FPMQ N X
MJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SINS S
IC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJ
XNBSR JB SIC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTC
P NBD MRGNP N XMRRJHAC MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOC D GMBSPMA MF SIC Q
CRRNEC
THE GENTRAB XROIBEM JN GRYXTOCRAXHY JR THAT OF TRANRMJTTJNC JNFORMATJON FROM A X
OJNT A TO A XOJNT I IY MEANR OF A XORRJIBY JNREGZRE GHANNEB JN RZGH A VAY THAT T
HE ORJCJNAB MERRACE GAN ONBY IE REGOSERED IY THE RJCHTFZB REGJXJENTR THE XARTJGJ
XANTR JN THE TRANRAGTJON ARE ABJGE THE ORJCJNATOR OF THE MERRACE IOI THE REGEJSE
R AND ORGAR A XORRJIBE OXXONENT VHO VJRHER TO CAJN ZNAZTHORJQED GONTROB OF THE M
ERRACE

```

### 确定I(单词in)

发现好几个单词jn，猜测-I

替换表

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	N	E	D	C	F		J	H	I			O	A	Q	R	M	P	T	S						

输入密文：  
SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFMPQNSJMB FPMQ N X  
MJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SINS S  
IC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJ  
XNBSR JB SIC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTC  
P NBD MRGNP N XMRRJHAC MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOCD GMBSPMA MF SIC Q  
CRRNEC  
THE GENTRAB XROJBEM IN GRYXTOCRAXHY IP THAT OF TRANPMITTINC INFORMATION FROM A X  
OINT A TO A XOINT J JY MEANP OF A XOPPIJBY INPEGZRE GHANNEB IN PZGH A VAY THAT T  
HE ORICINAB MEPPACE GAN ONBY JE REGOSERED JY THE RICHTFZB REGIXIENTP THE XARTIGI  
XANTP IN THE TRANPAGTION ARE ABIGE THE ORICINATOR OF THE MEPPACE JOJ THE REGEISE  
R AND OPGAR A XOPPIJBE OXXONENT VHO VIPHEP TO CAIN ZNAZTHORIQUED GONTROB OF THE M  
EPPACE

### 确定P(单词point)

看到单词XOINT 猜测X-P

置换表

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	N	E	D	C	F		J	H	I			O	A	Q	R	M	X	T	S				P		

输入密文：  
SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFMPQNSJMB FPMQ N X  
MJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SINS S  
IC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJ  
XNBSR JB SIC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTC  
P NBD MRGNP N XMRRJHAC MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOCD GMBSPMA MF SIC Q  
CRRNEC  
THE GENTRAB PROJBEIN IN GRYPTOCRAHY IX THAT OF TRANXMITTINC INFORMATION FROM A P  
OINT A TO A POINT J JY MEANX OF A POXXIJBY INXEGZRE GHANNEB IN XZGH A VAY THAT T  
HE ORICINAB MEXXACE GAN ONBY JE REGOSERED JY THE RICHTFZB REGIPIENTX THE PARTIGI  
PANTX IN THE TRANXAGTION ARE ABIGE THE ORICINATOR OF THE MEXXACE JOJ THE REGEISE  
R AND OXGAR A POXXIJBE OPPONENT VHO VIXHEX TO CAIN ZNAZTHORIQUED GONTROB OF THE M  
EXXACE

### 确定S(单词is)

看到单词IX 猜测为is

置换表

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	N	E	D	C	F		J	H	I			O	A	Q	R	M	S	T	X				P		

输入密文：  
SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFMPQNSJMB FPMQ N X  
MJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SINS S  
IC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJ  
XNBSR JB SIC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTC  
P NBD MRGNP N XMRRJHAC MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOCD GMBSPMA MF SIC Q  
CRRNEC  
THE GENTRAB PROJBEIN IN GRYPTOCRAHY IS THAT OF TRANSMITTINC INFORMATION FROM A P  
OINT A TO A POINT J JY MEANS OF A POSSIJBY INSEZGRE GHANNEB IN SZGH A VAY THAT T  
HE ORICINAB MESSAGE GAN ONBY JE REGOXERED JY THE RICHTFZB REGIPIENTS THE PARTIGI  
PANTS IN THE TRANSAGTION ARE ABIGE THE ORICINATOR OF THE MESSAGE JOJ THE REGEIXE  
R AND OSGAR A POSSIJBE OPPONENT VHO VISHES TO CAIN ZNAZTHORIQUED GONTROB OF THE M  
ESSAGE

## 确定B,L(单词problem)

看到单词PROJBEM，猜测为problem

置换表

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	C	F		B	H	I		J	O	A	Q	R	M	S	T	X				P		

输入密文：  
SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFMPQNSJMB FPMQ N X  
MJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SINS S  
IC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJ  
XNBSR JB SIC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTC  
P NBD MRGNP N XMRRJHAC MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOC D GMBSPMA MF SIC Q  
CRRNEC  
THE GENERAL PROBLEM IN CRYPTOGRAPHY IS THAT OF TRANSMITTING INFORMATION FROM A P  
OINT A TO A POINT B BY MEANS OF A POSSIBLY INSEGRZ GHANNEL IN SZGH A VAY THAT T  
HE ORICINAL MESSAGE CAN ONLY BE REGOXERED BY THE RICHTFZL REGIPIENTS THE PARTIGI  
PANTS IN THE TRANSAGTION ARE ALIGE THE ORICINATOR OF THE MESSAGE BOB THE REGEIXE  
R AND OSGAR A POSSIBLE OPPONENT VHO VISHES TO CAIN ZNAZTHORIQUED CONTROL OF THE M  
ESSACE

## 确定C(单词channel)

看到单词GHANNEL，猜测为channel

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		J	O	A	Q	R	M	S	T	X				P		

输入密文：  
SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFMPQNSJMB FPMQ N X  
MJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SINS S  
IC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJ  
XNBSR JB SIC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTC  
P NBD MRGNP N XMRRJHAC MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOC D GMBSPMA MF SIC Q  
CRRNEC  
THE CENTRAL PROBLEM IN CRYPTOGRAPHY IS THAT OF TRANSMITTING INFORMATION FROM A P  
OINT A TO A POINT B BY MEANS OF A POSSIBLY INSECZRE CHANNEl IN SZCH A VAY THAT T  
HE ORIGINAL MESSAGE CAN ONLY BE RECOXERED BY THE RIGHTFZL RECIPIENTS THE PARTICI  
PANTS IN THE TRANSACTION ARE ALICE THE ORIGINATOR OF THE MESSAGE BOB THE RECEIXE  
R AND OSCAR A POSSIBLE OPPONENT VHO VISHES TO GAIN ZNAZTHORIQUED CONTROL OF THE M  
ESSAGE

此时的密文已经有了大致的内容

## 确定W(单词who)

仔细观察发现一个单词VHO，猜测为who

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		J	O	A	Q	R	M	S	T	X		W	V	P		

输入密文：  
SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFMPQNSJMB FPMQ N X  
MJBS N SM N XMJBS H HY QCNBR MF N XMRRJHAY JBRCGZPC GINBBCA JB RZGI N VNY SINS S  
IC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJ  
XNBSR JB SIC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTC  
P NBD MRGNP N XMRRJHAC MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOC D GMBSPMA MF SIC Q  
CRRNEC  
THE CENTRAL PROBLEM IN CRYPTOGRAPHY IS THAT OF TRANSMITTING INFORMATION FROM A P  
OINT A TO A POINT B BY MEANS OF A POSSIBLY INSECZRE CHANNEl IN SZCH A WAY THAT T  
HE ORIGINAL MESSAGE CAN ONLY BE RECOXERED BY THE RIGHTFZL RECIPIENTS THE PARTICI  
PANTS IN THE TRANSACTION ARE ALICE THE ORIGINATOR OF THE MESSAGE BOB THE RECEIXE  
R AND OSCAR A POSSIBLE OPPONENT WHO WISHES TO GAIN ZNAZTHORIQUED CONTROL OF THE M  
ESSAGE

6.1.5.1 解密过程 (解密实验) 6.1.5.2 解密实验 (进阶 16.15.2) 可退出



## 确定V(单词recovered)

仔细观察发现一个单词RECOXERED, 猜测为recovered

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		J	O	A	Q	R	M	S	T	V		W	X	P		

```
输入密文:
SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFMPQNSJMB FPMQ N X
MJBS N SM N XMJBS H HY QCNR MF N XMRRJHAY JBRGZPC GINBBCA JB RZGI N VNY SINS S
IC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJ
KNBSR JB SIC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTC
P NBD MRGNP N XMRRJHAC MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOC D GMBSPMA MF SIC Q
CRRNEC
THE CENTRAL PROBLEM IN CRYPTOGRAPHY IS THAT OF TRANSMITTING INFORMATION FROM A P
OINT A TO A POINT B BY MEANS OF A POSSIBLY INSECZRE CHANNEL IN SZCH A WAY THAT T
HE ORIGINAL MESSAGE CAN ONLY BE RECOVERED BY THE RIGHTFZL RECIPIENTS THE PARTICI
PANTS IN THE TRANSACTION ARE ALICE THE ORIGINATOR OF THE MESSAGE BOB THE RECEIVE
R AND OSCAR A POSSIBLE OPPONENT WHO WISHES TO GAIN ZNAZTHORIQED CONTROL OF THE M
ESSAGE
```

## 确定U(单词such)

仔细观察发现一个单词SZCH, 猜测为such

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		J	O	A	Q	R	M	S	T	V	Z	W	X	P		U

```
输入密文:
SIC GCBSPNA XPMHACQ JB GPYXSMEPNXIY JR SINS MF SPNBRQJSSJBE JBFMPQNSJMB FPMQ N X
MJBS N SM N XMJBS H HY QCNR MF N XMRRJHAY JBRGZPC GINBBCA JB RZGI N VNY SINS S
IC MPJEJBNA QCRRNEC GNB MBAY HC PCGMTCPD HY SIC PJEISFZA PCGJXJCBSR SIC XNPSJGJ
KNBSR JB SIC SPNBRNGSJMB NPC NAJGC SIC MPJEJBNSMP MF SIC QCRRNEC HMH SIC PCGCJTC
P NBD MRGNP N XMRRJHAC MXXMBCBS VIM VJRICR SM ENJB ZBNZSIMPJOC D GMBSPMA MF SIC Q
CRRNEC
THE CENTRAL PROBLEM IN CRYPTOGRAPHY IS THAT OF TRANSMITTING INFORMATION FROM A P
OINT A TO A POINT B BY MEANS OF A POSSIBLY INSECURE CHANNEL IN SUCH A WAY THAT T
HE 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 RECEIVE
R AND OSCAR A POSSIBLE OPPONENT WHO WISHES TO GAIN UNAUTHORIQED CONTROL OF THE M
ESSAGE
```

此时发现这段话已经是一段完整的话了, 所以最终的置换表为

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	K	J	O	A	Q	R	M	S	T	V	Z	W	X	P	Y	U

置换代码

```
1  #include<iostream>
2  using namespace std;
3  int main()
4  {
5      char cipher[1000];
6      cout << "输入密文: " << endl;
7      cin.getline(cipher, 1000);
8      char A[26] = {
9          'L', 'N', 'E', 'D', 'G', 'F', 'C', 'B', 'H', 'I', 'K', 'J', 'O', 'A', 'Q', 'R', 'M', 'S', 'T',
10         'V', 'Z', 'W', 'X', 'P', 'Y', 'U' };
11     for (int i = 0; int(cipher[i]) != 0; i++)
12     {
13         if (int(cipher[i]) > 64 && int(cipher[i]) < 91)
14             cipher[i] = A[int(cipher[i]) - 65];
15     }
16     cout << cipher;
```

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 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