密码学实验报告

实验一移位密码

算法流程图

主函数，根据输入提供三种不同功能



输入1，进行加密

需要提供秘钥以及明文，然后使用for循环，先判断是否是字母，再判断字母的大小写，然后按照秘钥进行移位。

输入2，进行加密

需要提供秘钥以及密文，然后使用for循环，先判断是否是字母，再判断字母的大小写，然后按照秘钥进行反向移位解密。

输入3，进行攻击

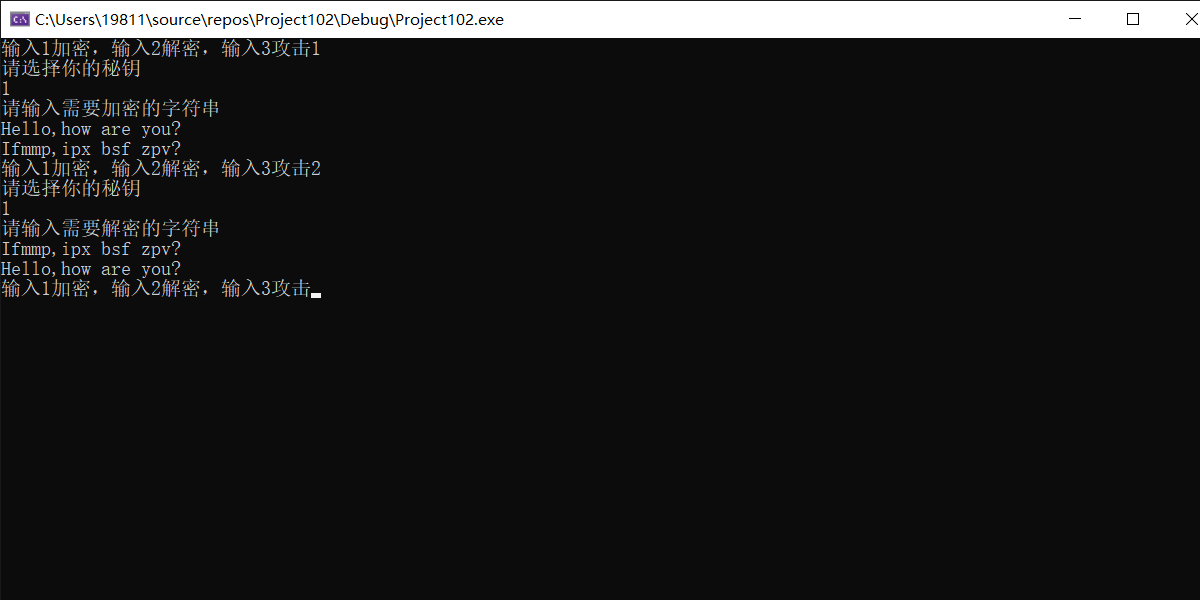
只需要提供密文，然后使用for循环，先判断是否是字母，再判断字母的大小写，然后移位1位，输出结果，此步骤共重复25次，得到25个结果，然后人工判断正确的明文

明文 Hello,how are you?

秘钥 1

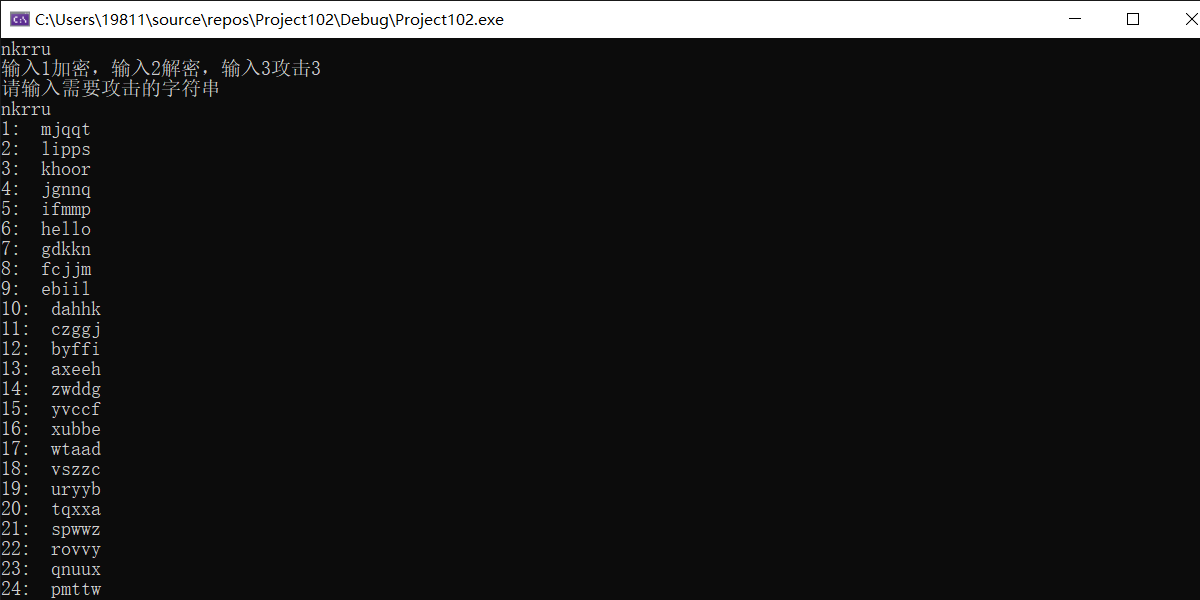
密文Ifmmp,ipx bsf zpv?

加密解密结果



攻击过程

例如我们得到密文nkrru，使用程序进行攻击



我们可以判断明文为hello，秘钥为6

实验二单标置换密码

程序流程图

主函数，根据输入提供三

两种不同功能

输入2，进行加密

用户输入置换密码表

输入1，进行加密

用户输入置换密码表

Get\_secret()

程序根据用户的输入构造完整的置换密码表。系统顺序的遍历用户输入的字符串,若遇到的是字母，首先判断是否是大写字母，如果不是则转换成大写字母，然后判断已构造的密码表中是否有这个字母，如果没有，则把它添加到密码表中，当遍历完后，如果还有字母没有添加到表中，则按照英语字母顺序添加到密码表中。

Get\_secret()

程序根据用户的输入构造完整的置换密码表。系统顺序的遍历用户输入的字符串,若遇到的是字母，首先判断是否是大写字母，如果不是则转换成大写字母，然后判断已构造的密码表中是否有这个字母，如果没有，则把它添加到密码表中，当遍历完后，如果还有字母没有添加到表中，则按照英语字母顺序添加到密码表中。

用户输入需要解密的密文

用户输入需要加密的明文

解密时我们需要先把小写字母转换为大写字母查表，然后再转换成小写字母替换，大写字母则直接查找替换即可

由于加密查找的时候，密码表是按照abcdefg正常顺序排列的，所以我们只需要判断段字母大小写，大写字母减去65（A的ascii）小写字母减去97（a的 ascii），然后根据下标替换即可

秘钥：Hello,how are you?

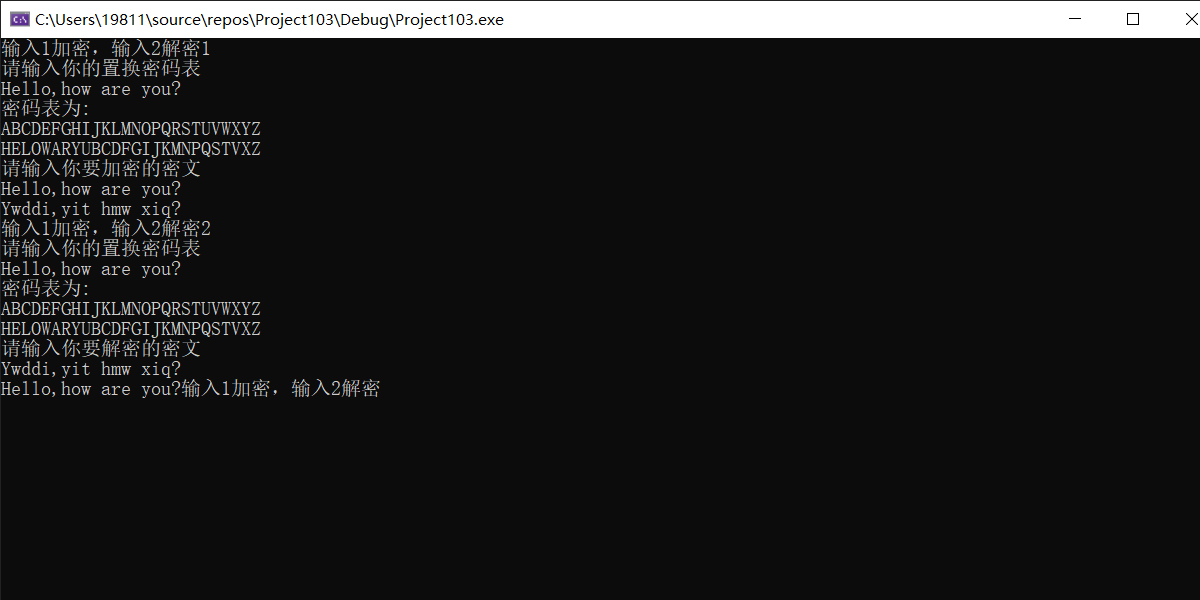
密码表：  
ABCDEFGHIJKLMNOPQRSTUVWXYZ

HELOWARYUBCDFGIJKMNPQSTVXZ

明文：Hello,how are you?

密文：Ywddi,yit hmw xiq?

加密解密结果



实验三 单表置换密码攻击

|  |
| --- |
| 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 |

c s i n p m v f j b r q x h y a e g d

e t h a r o w f i n s m p b y l g c d

我们可以看到图中单独出现的字母是N和H

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

而字母正常出现的概率为

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

我们尝试对密码进行攻击

第一步：首先我们对表中的单个单词做分析，在英语中，可以单个出现的只有I、A，对应题目中的单词H、N

第二步：接着我们尝试找到密文中出现频率最高的两个字母，我们可以看到分别是C:36次，S:33次，他们可能对应的是e、t

c s

e t

第三步：接着我们观察单词SIC，其在句子里出现的频率极高，推测其对应单词the

c s i

e t h

第四步：我们观察的单词SINS，由于已知S和I，所以我们可以推断出这个单词为that，即N对应字母a

c s i n

e t h a

第五步：我们观察单词NPC 则我们可以判断P对应字母r

c s i n p

e t h a r

第六步：我们观察SM，很容易判断它对应单词to

c s i n p m

e t h a r o

第七步：我们来查看VIM，他的对应的是who

c s i n p m v

e t h a r o w

第八步：我们观察MF多次出现，判断其为of

c s i n p m v f

e t h a r o w f

第九步：接着我们观察JB多次出现，同时也有JR出现，我们再观察频率，可以判断JB为in，JR为is

c s i n p m v f j b r

e t h a r o w f i n s

第十步：我们观察FPMQ，很容易判断他为from

c s i n p m v f j b r q

e t h a r o w f i n s m

第十一步：我们观察XMJBS，很容易判断他为point

c s i n p m v f j b r q x

e t h a r o w f i n s m p

第十二步：我们将FPMQ N XMJBS N SM N XMJBS H翻译过来，

from a point a to a point H,这样我们很容易判断H为b，同时后面的HY为by

c s i n p m v f j b r q x h y

e t h a r o w f i n s m p b y

第十三步：我们很容易判断XPMHACQ为problem

c s i n p m v f j b r q x h y a

e t h a r o w f i n s m p b y l

第十四步：观察ENJB，我们很容易判断段为gain

c s i n p m v f j b r q x h y a e

e t h a r o w f i n s m p b y l g

第十五步：观察GNB我们很容易判断其为can

c s i n p m v f j b r q x h y a e g

e t h a r o w f i n s m p b y l g c

第十六步：观察NBD，我们很容易判断为and

c s i n p m v f j b r q x h y a e g d

e t h a r o w f i n s m p b y l g c d

第十七步：观察PCGCJTCP，很容易判断为receiver

c s i n p m v f j b r q x h y a e g d t

e t h a r o w f i n s m p b y l g c d v

第十八步：观察RZGI，很容易判断为such

c s i n p m v f j b r q x h y a e g d t z

e t h a r o w f i n s m p b y l g c d v u

第十九步：最后我们观察ZBNZSIMPJOCD，很容易判断为unauthorized

c s i n p m v f j b r q x h y a e g d t z o

e t h a r o w f i n s m p b y l g c d v u z

于是我们便可根据以上关系进行解密：得到原文

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.