密码学实验一报告

1. 移位密码

移位密码的原理是将英文字母向前或向后移动一个固定位置。设置密钥key为5，即加密表示：

明文：m=m1m2**…**mi**…,** 则有

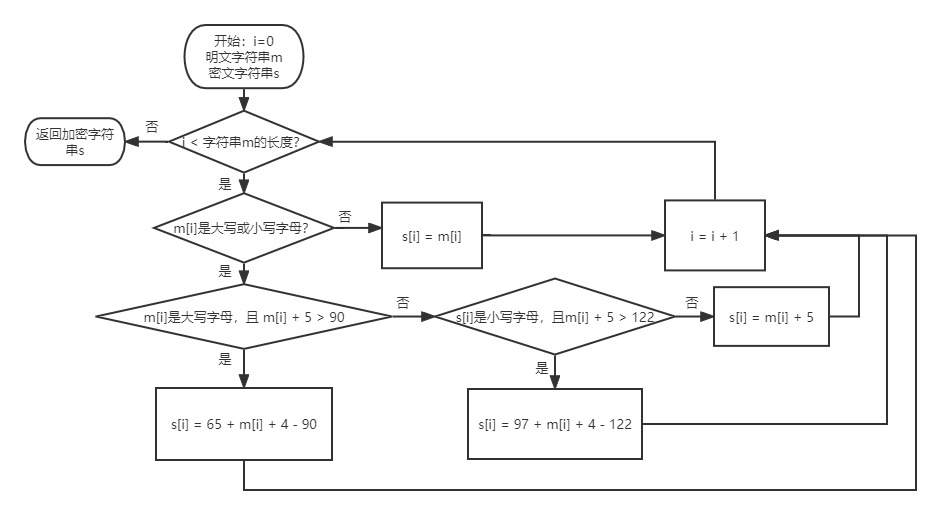
密文：c=c1c2**…**ci**…,** 其中 ci=(mi+5 mod26)，i＝1，2，**…**。

解密表示：

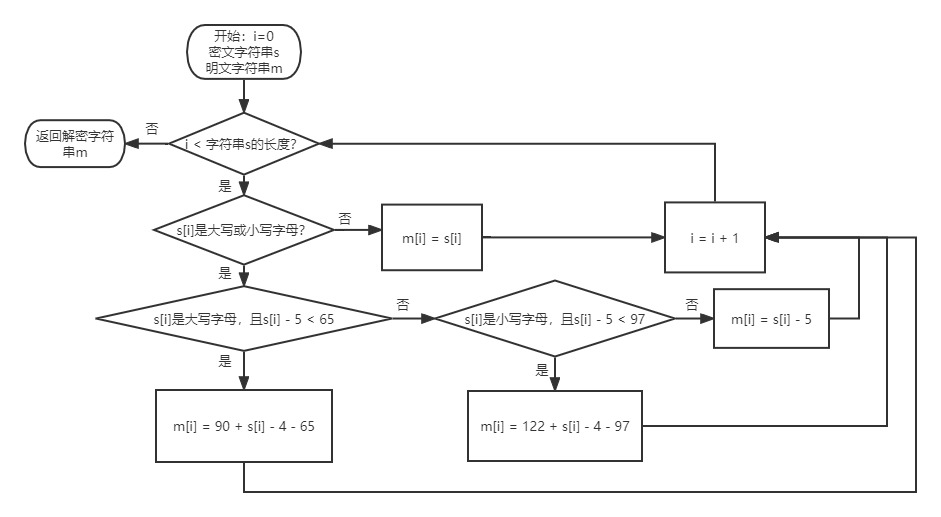
密文：c=c1c2**…**ci**…,** 则有

明文：m=m1m2**…**mi**…,**其中mi=(ci-5 mod26)，i＝1，2，**…**。

加密算法流程图：

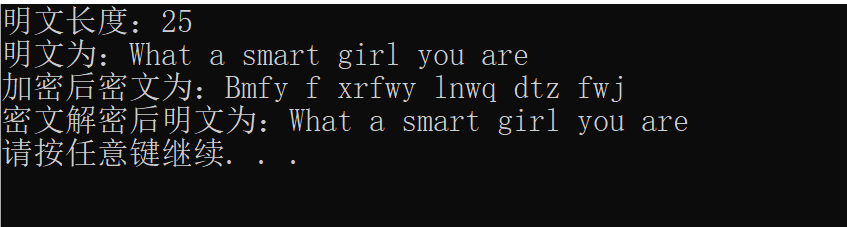


解密算法流程图：



设明文为：What a smart girl you are

运行程序结果如下：



因此加密后，密文为：Bmfy f xrfwy lnwq dtz fwj

密文解密后，明文为：What a smart girl you are

因此，检验加解密算法正确。

1. 攻击别人的移位密码算法

两人小组另一位成员：马羽潇

密文为：OHCL H UPJL KHF

首先，发现有一个单个字母H，可以猜测可能明文是A，因此：

密文字母 = 明文字母 + 7

经过尝试，解密得到明文：HAVE A NICE DAY

1. 单表置换密码

首先，使用”you are superman”为原始句子，构建置换密钥表：

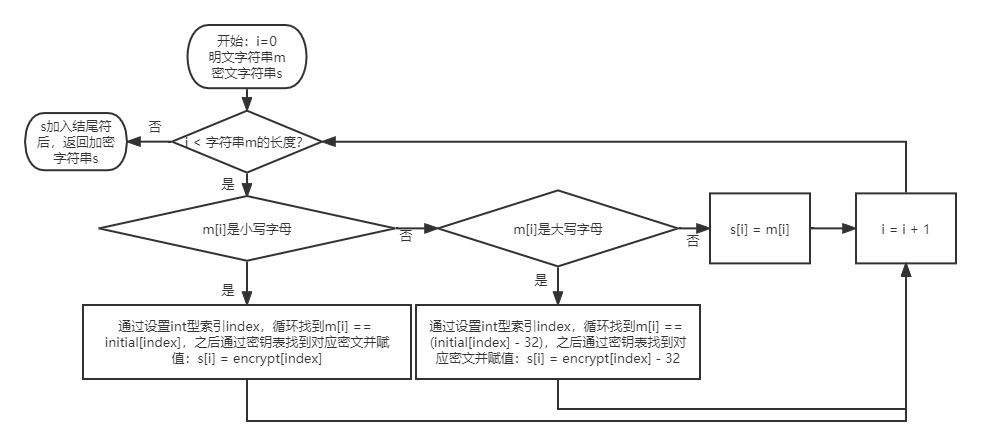
原始表：initial[26]

'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'

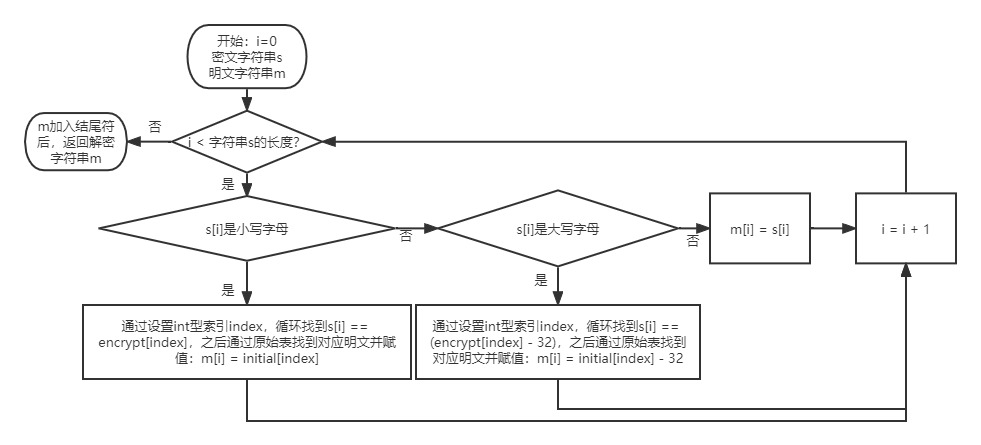
密钥表：encrypt[26]

'y','o','u','a','r','e','s','p','m','n','b','c','d','f','g','h','i','j','k','l','q','t','v','w','x','z'

加密算法流程图：

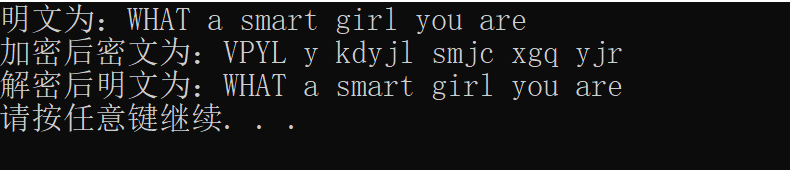


解密算法流程图：



设置明文为：WHAT a smart girl you are

运行程序加密解密的结果如下：



加密后密文为：VPYL y kdyjl smjc xgq yjr

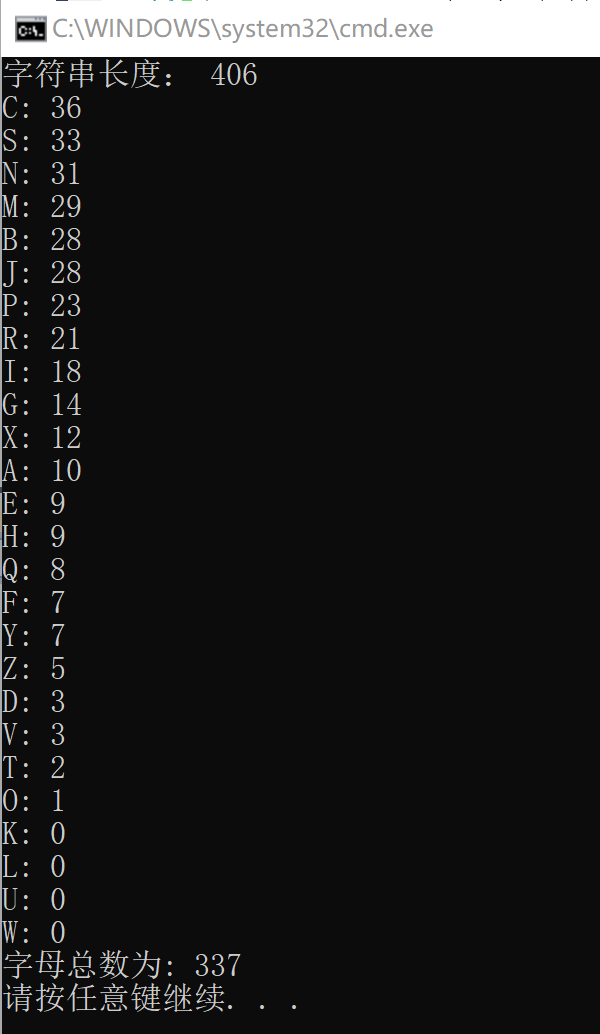
密文解密后明文为：WHAT a smart girl you are

1. 置换密码解密

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

对于这串密文的置换密码解密：

（1）首先编写代码统计总字母数量，以及每个字母在这个字符串中出现的次数，并按照频率排序（代码文件已经传在文件夹中）。



（2）根据字母频率，以及常用单词，进行猜测解密。

结果如上图所示，根据字母频率排序，我们首先猜测C为明文中的E，S为T。常用单词我们先统计2个或者3个字母的单词。发现SIC在字符串中出现9次，常用单词中的”the”出现频率很高，猜测SIC为单词”THE”，因此I为H。又根据常用单词，发现JB在字符串中出现4次，且JB的字母频率都是28次，比较高，因此猜测JB为单词”IN”，J为I，B为N。同时JR出现1次，根据常用单词，猜测为”IS”，R为S。之后继续统计，MF出现了4次，同时SM出现了2次，结合S为T，结合字母频率和常用单词，推测MF为”OF”，SM为”TO”，M为O，F为F。HY出现2次，HC出现1次，因为C已经猜出是E，猜测HY为”BY”，HC是”BE”。再看单个的字母，N出现6次，且在字母频率中也比较高，因此猜测N为A。VNY出现1次，VIM出现1次，结合已知的NY和IM，猜测V为W，因此，VNY表示”WAY”，VIM表示”WHO”。GNB出现1次，猜测为” CAN”，NBD出现1次，猜测为”AND”，NPC出现1次，根据N为A，C为E，猜测为”ARE”。SINS出现2次，四个字母已知为”THAT”。FPMQ出现1次，可能是”FROM”。

之后的猜测的单词比较长，可以根据多个单词进行猜测。ENJB出现1次，根据已知猜测这个单词是”\*AIN”,又根据SPNBRQJSSJBE根据已知是”TRANSMITTIN\*“，猜测E为G。XMJBS是”\*OINT”，之后XMRRJHAY为”\*OSSIBLY”，因此猜测X为P。RZGI是”S\*CH”，JBRCGZPC为”INSEC\*RE”，因此猜测Z为U。ZBNZSIMPJOCD是”UNAUTHORI\*ED”，通过单词猜测O为Z。PCGMTCPCD为”RECO\*ERED”，因此根据单词猜测T为V。

之后我们通过几个单词验证：MBAY是”ONLY”，NAJGC为”ALICE”，GCBSPNA为”CENTRAL“，MRGNP为”OSCAR”，发现我们的猜测得到了验证。

（3）最终我们可以得到置换表：

密文 明文 密文 明文 密文 明文 密文 明文 密文 明文

A L B N C E D D E G

F F G C H B I H J I

K / L / M O N A O Z

P R Q M R S S T T V

U / V W W / X P Y Y

Z U

通过程序编写进行解密，得到解密后的明文：

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

