古典密码作业

(1)求置换的逆置换。

答：d(y1,y2,y3,y4,y5,y6,y7,y8)=(y2,y4,y8,y7,y1,y5,y3,y6)

(2)用维吉尼亚密码加密明文“please keep this message in secret”，其中使用的密钥为“computer”，试求其密文。

答：密钥对应的数字串为（2,14,12,15,20,19,4,17）

明文对应的数字串，八个一组进行分组的结果是：

（15,11,4,0,18,4,10,4）（4,15,19,7,8,18,12,4）(18,18,0,6,4,8,13,18)(4,2,17,4,19)

分别(2,14,12,15,20,19,4,17)+(mod26)得：

(17,25,16,15,12,23,14,21)(6,3,5,22,2,11,16,21)(20,6,12,21,24,1,17,9)(6,16,3,19,13)

所以密文为：RZQPMXOVGDFWCLQVUGMVYBRJGQDTN

(3)用Playfair密码加密明文“hide the gold in the tree stump”，密钥为“cryptography”，试求其密文。

(4)用Hill密码加密明文“hill”，使用的密钥是：

试求其密文。

答：hill=(7,8,11,11)

（7,8,11,11）×k=(269,268,268,258)=(9,9,8,24)

所以密文是JJIY

(5)已知以下密文是由仿射密码得到的，试求其明文。

“FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHVUFEDKAPRKDLYEVLRHHRH”

(6)已知下列密文是通过维吉尼亚密码加密得来的，试求其明文。

“CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBWRVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAKLXFPSKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELXVRVPRTULHDNQWTWDTYGBPHXTFALJHASVBFXNGLLCHRZBWELEKMSJIKNBGHWRJGNMGJSGLXFEYPHAGNRBIEQJTAMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQEBBIPEEWEVKAKOEWADREMXMTBHHCHRTKDNVRZCHRCLQOHPWQAIIWXNRMGWOIIFKEE” (Key: JANET)

1. 明文“friday”用n=2的Hill密码加密后得到密文“PQCFKU”，求Hill密码的密钥。

答：friday=