## 第2章 古典密码

**1．运用凯撒密码算法，解密"RPQLD JDOOLD HVW GLYLVD LQ SDUWHV WUHV"。**

答案：omniagalliaestdivisainpartestres(拉丁语omnia Gallia est divisa in partest res 高卢全境分为三个部分)

**2.利用列置换密码算法，密钥用对换表示为加密下列消息：xiandaimimaxue。**

答案：密文：aidnxmimiauxea

**3.用Vigenere算法加密明文“We are discovered save yourself”，密钥是：deceptive。**

答案：将字母变换成对应的数字，然后利用公式计算，可得密文应为：ZICVTWQNGRZGVTWAVZHCQYGLMGJ

**4.根据以下两个置换*σ*1与*σ*2，按*d*=2的周期置换密码体制加密以下明文：transposi tionisare和arrangeme ntofthesy。其中*σ*1=（7 3 4 1 6 8 9 5 2），*σ*2=（4 1 2 7 9 8 5 6 3）。**

答案：将明文字母串分成9个字母连在一起的字母段，分别为：

transposi tionisare和arrangeme ntofthesy，再分别用置换*σ*1和*σ*2对字母段进行加密，得到经过置换后的密文：

OANTPSISR NTIAERISO和ERAAGMENR FNTEYSTHO。

**5.设*d*=4，*n*=9的周期置换密码的四个置换和密文如下，求明文？**

*σ*1 = (6 9 4 8 3 7 1 2 5) *σ*2 = (1 3 5 4 7 2 6 8 9)

*σ*3 = (5 9 6 4 7 8 2 1 3) *σ*4 = (2 5 1 6 3 9 4 7 8)

密文：pinsaotrs toinaisre negaemrar ttnhoyfes omlaofmbs esgaxsexx

答案：先求逆置换为：

(*σ*1)-1= (7 8 5 3 9 1 6 4 2) (*σ*2)-1= (1 6 2 4 3 7 5 8 9)

(*σ*3 )-1= (8 7 9 4 1 3 5 6 2) (*σ*4 )-1= (3 1 5 7 2 4 8 9 6)

密文经过逆置换后的明文为：transposi tionisare arrangeme ntofthesy mbolsofam essagexxx（transposition is are arrangement of the symbol sofa message xxx ）。

**6.密文CRWWZ是用模26的某仿射密码加密的，明文开头是ha；试对该密文解密？**

答案：明文*ha*对应密文*CR*，即有(7,0)加密后为(2,17)，将这两对明密文带入仿射加密算法，得到方程组



解这个方程组，得

所以有：

解密算法为：

对密文CRWWZ解密后的明文：happy。

**7.求模27的仿射密码可能的密钥有多少？用模29呢？**

答案：用模27的仿射密码代替模26的仿射密码，，其中，，且，所以*k*0的个数为φ(27)，其中*φ*为欧拉（Euler）函数，明显φ(27)=18。

密钥量：φ(27) ×27-1=485，其中减去一个恒等变换。

同理，用模29的仿射密码代替模26的仿射密码，密钥量：

φ(29) ×29-1=28×29-1=811。

**8.设英文字母*A*，*B*，…，*Z*分别编码为0，1，…，25。已知单表仿射加密变换为，其中*m*表示明文，***C***表示密文，试对明文*HELPME*加密？**

答案：将明文和密文的26个英文字母对应变换为0-25之间的数字，然后带入公式得：



所以*HELPME*加密后为*QBKEPB*。

**9.设英文字母*A*，*B*，…，*Z*分别编码为0,1，…，25。已知*m*表示明文，*C*表示密文，单表仿射加密变换为，试对密文*VMWZ*解密？**

答案：得，

而11-1=19mod26，故。

V=21，M=12，W=22，Z=25









所以，

**10.已知密码体制为Vigenere体制，明文为nankaiuniversity，密文为NRGKRBUEBVVKSZMY求该密码体制的密钥？**

答案：Vigenere体制加密：，其中*m*为明文，*C*为密文，*k*为密钥。因此，。

将明文和密文的26个英文字母对应变换为0-25之间的数字，因为Vigenere体制中，将明文和密文对应的数字代数公式得：密钥*k*=*aeturjorjqzbkhfw*