第一章部分课后题参考答案

1．设仿射变换的加密是 $E_{11,23}(m)=11m+23 \pmod{26}$，对明文“THE NATIONAL SECURITY AGENCY”加密，并使用解密变换 $D_{11,23}(c)=11^{-1}(c-23) \pmod{26}$验证你的加密结果。

解：T=19，11・19+23(mod 26)=24，T⇒Y　　H=7，11・7+23(mod 26)=22，H⇒W

E=4，11・4+23(mod 26)=15，E⇒P　　N=13，11・13+23(mod 26)=10，N⇒K

A=0，11・0+23(mod 26)=23，A⇒X　　I=8，11・8+23(mod 26)=7，I⇒H

O=14，11・14+23(mod 26)=21，O⇒V　　L=11，11・11+23(mod 26)=14，L⇒O

S=18，11・18+23(mod 26)=13，S⇒N　　C=2，11・2+23(mod 26)=19，C⇒T

U=20，11・20+23(mod 26)=9，U⇒J　　R=17，11・17+23(mod 26)=2，R⇒C

Y=24，11・24+23(mod 26)=1，Y⇒B　　G=6，11・6+23(mod 26)=11，G⇒L

所得密文为“YWPKXYHVKXONPTJCHYBXLPKTB”

验证如下：11^{-1}（mod 26）＝19

Y=24，19・(24-23) (mod 26)=19，Y⇒T　　W=22，19・(22-23) (mod 26)=7，W⇒H

P=15，19・(15-23) (mod 26)=4，P⇒E　　K=10，19・(10-23) (mod 26)=13，K⇒N

X=23，19・(23-23) (mod 26)=0，X⇒A　　H=7，19・(7-23) (mod 26)=8，H⇒I

V=21，19・(21-23) (mod 26)=14，V⇒O　　O=14，19・(14-23) (mod 26)=11，O⇒L

N=13，19・(13-23) (mod 26)=18，N⇒S　　T=19，19・(19-23) (mod 26)=2，T⇒C

J=9，19・(9-23) (mod 26)=20，J⇒U　　C=2，19・(2-23) (mod 26)=17，C⇒R

B=1，19・(1-23) (mod 26)=24，B⇒Y　　L=11，19・(11-23) (mod 26)=6，L⇒G

译文与明文相同。

2. 设由仿射变换对一个明文加密得到密文为 edsgickxhuklzveqzvkxwkzukvcuh 又已知明文的前两个字符是“if”。对该密文解密。

解：密文对应数字 4,3,18,6,8,2,10,23,7,20,10,11,25,*21*,4,16,25,21, 10,23,*22*,10,25,20,10,21,2,20,7

if 所对应的数字为　8,5

设仿射变换为 $c=am+b \bmod 26$ 则由前两个字符的对应明文可得如下方程

4＝a*8+b mod 26　(1)

3＝a*5+b mod 26　(2)

联立（1）和（2）解方程组可得 a=9,b=10

所以解密算法为：$m=a^{-1}(c-b) \bmod 26=9^{-1}(c-10) \bmod 26=3(c-10) \bmod 26$

于是可得密文数字对应的明文数字依次为：

8,5,24,14,20,2,0,13,17,4,0,3,19,7,8,18,19,7,0,13,10,0,19,4,0,7,2,4,17

相应的明文为：if you can read this thank a teahcer

4. 设多表代换密码 $C_i=AM_i+B \pmod{26}$中，A 是 2×2 矩阵，B 是 0 矩阵，又知明文“dont”被加密为“elni”，求矩阵 A。

解：明文对应数字为：3，14，13，19；密文对应数字为 4，11，13，8

设 A 为$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$，则由名密文对应关系可得：

$a_{11}\times 3+a_{12}\times 14=4 \pmod{26}$

$a_{21}\times 3+a_{22}\times 14=11 \pmod{26}$

$a_{11}\times 13+a_{12}\times 19=13 \pmod{26}$

$a_{21}\times 13+a_{22}\times 19=8 \pmod{26}$

解以上四元一次方程组可得矩阵 $A=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}=\begin{pmatrix} 10 & 13 \\ 9 & 23 \end{pmatrix}$