第一章

4．设多表代换密码*Ci*=*AMi*＋*B* (mod 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，则由名密文对应关系可得：

a11×3＋a12×14＝4(mod 26)

a21×3＋a22×14＝11(mod 26)

a11×13＋a12×19＝13(mod 26)

a21×13＋a22×19＝8(mod 26)

解以上四元一次方程组可得矩阵*A*＝＝

第二章

1．3级线性反馈移位寄存器在*c*3＝1时可有4种线性反馈函数，设其初始状态为(*a*1,*a*2,*a*3)=(1,0,1)，求各线性反馈函数的输出序列及周期。

解：此时线性反馈函数可表示为*f*(*a*1,*a*2,*a*3)=*a*1⊕*c*2*a*2⊕*c*1*a*3

当*c*1＝0，*c*2＝0时，*f*(*a*1,*a*2,*a*3)=*a*1⊕*c*2*a*2⊕*c*1*a*3＝*a*1，

输出序列为101101…， 周期＝3

当*c*1＝0，*c*2＝1时，*f*(*a*1,*a*2,*a*3)=*a*1⊕*c*2*a*2⊕*c*1*a*3＝*a*1⊕*a*2，

输出序列为10111001011100…，周期＝7

当*c*1＝1，*c*2＝0时，*f*(*a*1,*a*2,*a*3)=*a*1⊕*c*2*a*2⊕*c*1*a*3＝*a*1⊕*a*3，

输出序列为10100111010011…，周期＝7

当*c*1＝1，*c*2＝1时，*f*(*a*1,*a*2,*a*3)=*a*1⊕*c*2*a*2⊕*c*1*a*3＝*a*1⊕*a*2⊕*a*3，

有输出序列为1010…， 周期＝2

3．设n＝4，*f*(*a*1,*a*2,*a*3,*a*4)=*a*1⊕*a*4⊕1⊕*a*2*a*3，初始状态为(*a*1,*a*2,*a*3,*a*4)＝(1,1,0,1)，求此非线性反馈移位寄存器的输出序列及周期。

解：由反馈函数和初始状态得状态输出表为

(*a*4 *a*3 *a*2 *a*1) 输出 (*a*4 *a*3 *a*2 *a*1) 输出

1 0 1 1 1 1 1 1 1 1

1 1 0 1 1 0 1 1 1 1

1 1 1 0 0 1 0 1 1 1（回到初始状态）

所以此反馈序列输出为：11011…周期为5

5．设密钥流是由*n*级LFSR产生，其周期为2*n*－1，*i*是任一正整数，在密钥流中考虑以下比特对

(*Si*, *Si*+1), (*Si*+1, *Si*+2), …, (*Si*+2n－3, *S i*+2n－2), (*Si*+2n－2, *S i*+2n－1),

问有多少形如(*Sj*, *Sj*+1)＝(1,1)的比特对？证明你的结论。

答：共有2(n-2)

证明：

证明方法一：由于产生的密钥流周期为2*n*－1，且LFSR的级数为n，所以是m序列

以上比特对刚好是1个周期上，两两相邻的所有比特对，其中等于(1,1)的比特对包含在所有大于等于2的1游程中。由m序列的性质，所有长为*i*的1游程(1≤ i ≤n-2)有2*n*-*i*-1/2个，没有长为n－1的1游程，有1个长为n的1游程。

长为i (i>1)的1游程可以产生i-1个(1,1)比特对，

所以共有(1,1)比特对的数目*N*＝2*n*-2-2×(2－1)＋2*n*-3-2×(3－1)＋…＋2*n*-i-2×(i－1)＋…＋2*n*-(*n*－2)－2×(n－2－1)＋n－1＝＋n－1＝2(n-2)

证明方法2：考察形如11\*…\*的状态的数目，共有2(n-2)个

6．已知流密码得密文串为1010110110和相应明文串0100010001，而且还已知密钥流是使用3级线性反馈移位寄存器产生的，试破译该密码系统。

解：由二元加法流密码的加密算法可知，将密文串和相应的明文串对应位模2加可得连续的密钥流比特为1110100111

设该三级线性反馈移位寄存器的反馈函数为*f*(*a*1,*a*2,*a*3)=*c*3*a*1⊕*c*2*a*2⊕*c*1*a*3

取其前6比特可建立如下方程

(*a*4*a*5*a*6)＝(*c*3,*c*2,*c*1)，

即(*c*3,*c*2,*c*1)＝(*a*4*a*5*a*6)＝(0 1 0) =(0 1 0) =(1 0 1)

所以*f*(*a*1,*a*2,*a*3)=*a*1⊕*a*3，即流密码的递推关系式为*ai*+3=*ai*+2⊕*ai*

8.设J-K触发器中{*ak*}和{*bk*}分别为3级和4级m序列，且

{*ak*}＝11101001110100…

{*bk*}＝001011011011000 001011011011000…

求输出序列{*ck*}及周期。

解：由于gcd(3，4)=1且*a*0＋*b*0＝1所以序列{*ck*}的周期为(23-1)(24-1)=105

又由J-K触发器序列的递推式*ck*=( *ak*+*bk*+1) )*ck*-1+*ak*，令*c*-1=0可得输出序列为：

{*ck*}=11001001…

9．设基本钟控序列产生器中{*ak*}和{*bk*}分别为2级和3级m序列，且

{*ak*}＝101101…

{*bk*}＝10011011001101…

求输出序列{*ck*}及周期。

解：序列{*ak*}的周期*p*1＝22－1＝3，序列{*bk*}的周期*p*2＝23－1＝7，*w*1＝*a*0＋*a*1＋*a*2＝2

而gcd(*w*1, *p*2)=1。所以序列{*ck*}的周期*p*＝*p*1*p*2＝3×7＝21

记LFSR2(产生序列{*bk*})的状态向量为*σk*，则*σ*0＝(100)，在LFSR1(产生序列{*ak*})的控制下，状态转移为：

{*ak*} 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1

(100),(001),(001),(011),(110),(110),(101),(011),(011),(110),(100),(100),(001),(011),(011),(110)

1 0 0 0 1 1 1 0 0 1 1 1 0 0 0 1

{*ak*} 1 0 1 1 0 1 1 0 1

(101),(101),(011),(110),(110),(100),(001), (001),(011)

1 1 0 1 1 1 0 0 0

所以输出序列为100011100111000111011 1000…

第三章

3．在DES的CBC模式中C1的一个错误明显地将影响P1和P2的结果

（1）P2以后的分组不受影响，这是因为C1以后的密文都是正确的，而恢复明文主要看对应密文分组和其前一个密文分组的正确性。

（2）加密前的明文分组P1有1比特错误，则这一错误将在所有后续密文分组中传播，但接受者能够正确解密，除了P1的一个错误比特之外。这是因为相当于发送者将明文改变了1比特得到一个新明文，而该明文的对应密文正确的传送给了接受方。

4．在8bitCFB中密文字符中出现1比特错误，该错误将影响包括该密文的连续9组密文的解密。

第四章

10．设通信双方使用RSA加密体制，接收方的公开钥是(*e*，*n*)＝(5,35)，接收到的密文是C＝10，求明文M。

解：由n＝35，易知35＝5×7，进而*ϕ*(*n*)= *ϕ*(35)=24，

由RSA加密体制可知，*ed*≡1 mod *ϕ*(*n*)，即5*d*≡1 mod 24，所以*d*＝5

∴*M*=*Cd* mod *n*＝105 mod 35＝5

Ps：*ϕ*(*n*)=(p-1)(q-1)

13．在ElGamal体制中，设素数*p*＝71，本原根*g*＝7，

（1）如果接收方B的公开钥是*yB*＝3，发送方A选择的随机整数k＝3，求明文M＝30所对应的密文。

解：*C*1=*gk* mod *p*＝73 mod 71＝59

*C*2=*yBkM* mod *p*＝33×30 mod 71＝29

所以密文为(59，29)

（2）如果A选择另一个随机数k，使得明文M=30，加密后的密文是C＝（59，C2），求C2

解：由*C*1=*gk* mod *p*得59＝*gk* mod *p*＝7*k* mod 71，即k＝3

而*C*2=*yBkM* mod *p*＝33×30 mod 71＝29

14．设背包密码系统得超递增序列为（3，4，9，17，35），乘数为t＝19，模数k＝73，试对good night加密。

解：由*A*=（3，4，9，17，35），乘数为*t*＝19，模数*k*＝73，

得*B*=*t*×*A* mod *k*＝(57，3，25，31，8）

名文“good night”的编码为“00111”，“01111”，“01111”，“00100”，“00000”，“01110”“01001”“00111”“01000”“10100”

*f*(00111)=25+31+8=64，*f*(01111)=3+25+31+8=67，*f*(01111)=3+25+31+8=67，*f*(00100)=25

*f*(00000)=0，*f*(01110)=3+25+31=59，*f*(01001)=3+8=11，*f*(00111)=25+31+8=64，

*f*(01000)=3，*f*(10100)=57＋25=82＝9 mod 73

相应的密文为（64，67，67，25，0，59，11，64，3，9）

15．设背包密码系统的超递增序列为（3，4，8，17，33），乘数为t＝17，模数k＝67，试对密文25，2，72，92解密。

解：*t*－1mod *k*＝17－1 mod 67＝4 mod 67

所以4×(25，2，72，92)mod 67＝(33,8,20,33)

从而可得4个明文分组为(00001,00100,10010,00001)，所以由表4－5明文为：“ADRA”

19．已知点G=（2，7）在椭圆曲线E11(1,6)上，求2G和3G

解：求2G:

λ=(3×22＋1)/(2×7) mod11＝13×4 mod11＝8

x3＝82－2－2 mod 11＝5，y3＝8(2－5)－7 mod 11＝2

所以2G＝（5，2）

求3G＝2G＋G＝（5，2）＋（2，7）

λ=(7－2)/(2－5) mod11＝5×7 mod11＝2

x3＝22－5－2 mod 11＝8，y3＝2(5－8)－2 mod 11＝3

所以3G＝（8，3）

20．利用椭圆曲线实现ElGamal密码体制，设椭圆曲线是E11(1,6)，生成元G=（2，7），接收方A的秘密钥*nA*＝7

（1）求A的公开钥*PA*

解：*PA*＝7G＝2×2G＋3G

先求2×2G

λ=(3×52＋1)/2×2 mod11＝10×3 mod11＝8

x3＝82－5－5 mod 11＝10，y3＝8(5－10)－2 mod 11＝2

所以2×2G＝2×(5，2)＝(10，2)

*PA*＝(10，2)＋(8，3）

由于λ=(3－2)/(8－10) mod11＝1×5 mod11＝5

x3＝52－10－8 mod 11＝7，y3＝5(10－7)－2 mod 11＝2

所以*PA*＝(7，2)

（2）发送方B欲发送*Pm*＝(10，9)，选择随机数k＝3，求密文C

解：C=(*kG*，*Pm*＋*kPA*)，*kG*＝3G＝（8，3），*kPA*＝2*PA*＋*PA*＝3G+7G＝(2，7)＋(7，2)

由于λ=(2－7)/(7－2) mod11＝－1

x3＝(－1)2－2－7 mod 11＝3，y3＝－1(2－3)－7 mod 11＝5

*Pm*＋*kPA*＝(10，9)＋(3，5)

由于λ=(5－9)/(3－10) mod11＝－1

x3＝(－1)2－10－3 mod 11＝10，y3＝－1(10－10)－9 mod 11＝2

所以C=(*kG*，*Pm*＋*kPA*)＝（（8，3），（10，2））

（3）显示接收方*A*从密文*Cm*恢复消息*Pm*的过程

解：*Pm*＝（*Pm*＋*kPA*）－*nA*(*kG*)＝（10，2）－7（8，3）＝（10，2）－（3，5）

＝（10，2）＋（3，6）＝(10，9)

第五章

2．Diffie-Hellman密钥交换协议易受中间人攻击，即攻击者截获通信双方通信的内容后可分别冒充通信双方，以获得通信双方协商的密钥。详细分析攻击者如何实施攻击。

虽然Diffie-Hellman密钥交换算法十分巧妙，但由于**没有认证功能**，**存在中间人攻击**。当Alice和Bob交换数据时，Trudy拦截通信信息，并冒充Alice欺骗Bob，冒充Bob欺骗Alice。其过程如下：

(1)Alice选取大的随机数*x*，并计算*X*=*gx* (mod *P*)，Alice将*g*、*P*、*X*传送给Bob，但被Trudy拦截。

(2)Trudy冒充Alice选取大的随机数z，并计算*Z*=*gz*(mod *P*)，Trudy将Z传送给Bob。

(3)Trudy冒充Bob，再将*Z*=*gz*(mod *P*)传送给Alice。

(4)Bob选取大的随机数y，并计算*Y* =*gy*(mod *P*)，Bob将*Y*传送给Alice，但被Trudy拦截。

由(1)、(3)Alice与Trudy共享了一个秘密密钥*gxz*，由(2)、(4)Trudy与Bob共享了一个秘密密钥*gyz*。

以后在通信过程中，只要Trudy作中间人，Alice和Bob不会发现通信的异常，但Trudy可以获取所有通信内容。

3．Diffie-Hellman密钥交换过程中，设大素数*p*＝11，*a*＝2是*p*的本原根，

(1) 用户A的公开钥*YA*＝9，求其秘密钥*XA*

解：*XA*满足*YA*＝*aXA* mod *p* 即9＝2*XA* mod 11，所以由*XA*＝6

(2)设用户B的公开钥*YB*＝3，求A和B的共享密钥K

解：由Diffie-Hellman协议可知*K*= *YB XA* mod *p*＝36 mod 11＝3

4．线性同余算法*Xn*＋1＝(*aXn*) mod 24，问：

(1)该算法产生的数列的最大周期是多少？

解：由于模m＝24因此它没有原根，又由递推式不难得知*Xn*＝*anX*0 mod 24

因此该算法产生的序列的最大周期为*a* mod 24的最大阶*l*，而*l*|*ϕ*(24)，但*l*≠*ϕ*(24)＝8

若*l*＝4，则不难验证，*X*0=1,*a*＝3时，数列周期为4，因此该算法产生数列的最大周期是4

(2) *a*的值是多少？

解：a必须满足gcd(a,24)=1，所以a在{1,3,5,…,15}中取值。

周期为4的有{3，5，11，13}，即为a的取值

(3) 对种子有何限制？

答：种子*X*0必须满足gcd(*X*0,24)=1。

5．在Shamir秘密分割门限方案中，设k＝3，n＝5，q＝17，5个子密钥分别是8、7、10、0、11，从中任选3个，构造插值多项式并求秘密数据s

解：取*f*(1)=8, *f*(2)=7, *f*(4)=0,构造插值多项式

*f*(*x*)=8(x-2)(x-4)/(1-2)(1-4)+7(x-1)(x-4)/(2-1)(2-4)＋0(x-1)(x-2)/(4-1)(4-2)

=8(x-2)(x-4)6+7(x-1)(x-4)8 mod 17

=2*x*2+10*x*+13

*s*= *f*(0)=13

第七章

1．在DSS数字签名标准中，取p=83=2×41+1，q＝41，h＝2，于是g≡22≡4 mod 83，若取x＝57，则*y*≡*gx*≡457＝77 mod 83。在对消息M=56签名时选择k＝23,计算签名并进行验证。

解：这里忽略对消息M求杂凑值的处理

计算*r*＝(*gk* mod *p*) mod *q*＝(423 mod 83) mod 41=51 mod 41=10

*k*-1mod q=23-1 mod 41=25

*s*=*k*-1(*M*+*xr*) mod *q*=25(56+57\*10) mod 41=29

所以签名为(*r*,*s*)=(10,29)

接收者对签名(*r*′,*s*′)=(10,29)做如下验证：

计算w＝(*s*′)-1 mod *q*=29-1 mod 41=17

u1＝[*M*′w] mod *q*=56\*17 mod 41=9

u2＝*r*′w mod *q*＝10×17 mod 41＝6

v＝(*gu*1*y*u2 mod *p*) mod *q*=(49×776 mod 83) mod 41＝10

所以有v＝*r*′，即验证通过。