重点练习的课后题

第一章：1、2、4 题
第二章：全做
第三章：1、2、3、4
第四章：所有的计算题基本都在这章里面出了。
4、10、11、12、13、14、15、16、17、18、19、20
第五章：不做 4
第六章：1、2
第七章：无

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 $A=\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}=\begin{pmatrix} 10 & 13 \\ 9 & 23 \end{pmatrix}$

第二章作业参考答案

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 $f(a_1,a_2,a_3)=a_1\oplus c_2a_2\oplus c_1a_3$

当 $c_1=0$，$c_2=0$ 时，$f(a_1,a_2,a_3)=a_1\oplus c_2a_2\oplus c_1a_3=a_1$，

输出序列为 101101…，　　周期＝3

当 $c_1=0$，$c_2=1$ 时，$f(a_1,a_2,a_3)=a_1\oplus c_2a_2\oplus c_1a_3=a_1\oplus a_2$，

输出序列为 10111001011100…，周期＝7

当 $c_1=1$，$c_2=0$ 时，$f(a_1,a_2,a_3)=a_1\oplus c_2a_2\oplus c_1a_3=a_1\oplus a_3$，

输出序列为 10100111010011…，周期＝7

当 $c_1=1$，$c_2=1$ 时，$f(a_1,a_2,a_3)=a_1\oplus c_2a_2\oplus c_1a_3=a_1\oplus a_2\oplus a_3$，

有输出序列为 1010…，　　周期＝2

2．设 n 级线性反馈移位寄存器的特征多项式为 $p(x)$，初始状态为$(a_1,a_2,\ldots,a_{n-1},a_n)=(00\ldots01)$，证明输出序列的周期等于 $p(x)$的阶

证：设 $p(x)$的阶为 p，由定理 2-3，由 $r|p$，所以 $r\le p$

设 $A(x)$为序列$\{a_i\}$的生成函数，并设序列$\{a_i\}$的周期为 r，则显然有 $A(x)p(x)=\phi(x)$

又 $A(x)=a_1+a_2x+\ldots+a_rx^{r-1}+x^r(a_1+a_2x+\ldots+a_rx^{r-1})+(x^r)^2(a_1+a_2x+\ldots+a_rx^{r-1})+\cdots$

$=a_1+a_2x+\ldots+a_rx^{r-1}/(1-x^r)=a_1+a_2x+\ldots+a_rx^{r-1}/(x^r-1)$

于是 $A(x)=(a_1+a_2x+\ldots+a_rx^{r-1})/(x^r-1)=\phi(x)/p(x)$

又$(a_1,a_2,\ldots,a_{n-1},a_n)=(00\ldots01)$

所以 $p(x)(a_nx^{n-1}+\ldots+a_rx^{r-1})=\phi(x)(x^r-1)$　即 $p(x)x^{n-1}(a_n+\ldots+a_rx^{r-n})=\phi(x)(x^r-1)$

由于 x^{n-1} 不能整除 x^r-1，所以必有 $x^{n-1}|\phi(x)$，而$\phi(x)$的次数小于 n，所以必有$\phi(x)=x^{n-1}$

所以必有 $p(x)|(x^r-1)$，由 $p(x)$的阶的定义知，阶 $p\le r$

综上所述：$p=r$　#

3．设 n＝4，$f(a_1,a_2,a_3,a_4)=a_1\oplus a_4\oplus 1\oplus a_2a_3$，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

4．设密钥流是由 $m=2s$ 级 LFSR 产生，其前 m+2 个比特是$(01)^{s+1}$，即 s＋1 个 01。问第 m+3 个比特有无可能是 1，为什么？

解：不能是 1。

可通过状态考察的方法证明以上结论。

首先 m 级 LFSR 的状态是一个 m 维的向量，则前 m 个比特构成一个状态 S_0，可表示为$(01)^s$，

第 m＋1 个比特是 0，所以 S_0 的下一个状态是 $S_1=(10)^s$，

第 m＋2 个比特是 1，所以 S_1 的下一个状态是 $S_2=(01)^s=S_0$，回到状态 S_0，

所以下一个状态应是 $S_3=S_1=(10)^s$，也即第 m+3 个比特应该为 0。

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

$$(S_i, S_{i+1}), (S_{i+1}, S_{i+2}), \ldots, (S_{i+2^n-3}, S_{i+2^n-2}), (S_{i+2^n-2}, S_{i+2^n-1}),$$

问有多少形如$(S_j, S_{j+1})=(1,1)$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($1\le i\le n-2$)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 $N=2^{n-2-2}\times(2-1)+2^{n-3-2}\times(3-1)+\ldots+2^{n-i-2}\times(i-1)+\ldots+2^{n-(n-2)-2}\times(n-2-1)+n-1=\sum_{i=2}^{n-2}2^{n-i-2}(i-1)+n-1=2^{(n-2)}$

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 $f(a_1,a_2,a_3)=c_3a_1\oplus c_2a_2\oplus c_1a_3$

取其前 6 比特可建立如下方程

$$(a_4a_5a_6)=(c_3,c_2,c_1)\begin{bmatrix}a_1&a_2&a_3\\a_2&a_3&a_4\\a_3&a_4&a_5\end{bmatrix},$$

$$\text{即}(c_3,c_2,c_1)=(a_4a_5a_6)\begin{bmatrix}a_1&a_2&a_3\\a_2&a_3&a_4\\a_3&a_4&a_5\end{bmatrix}^{-1}=(0\ 1\ 0)\begin{bmatrix}1&1&1\\1&1&0\\1&0&1\end{bmatrix}^{-1}=(0\ 1\ 0)\begin{bmatrix}1&1&1\\1&0&1\\1&1&0\end{bmatrix}=(1\ 0\ 1)$$

所以 $f(a_1,a_2,a_3)=a_1\oplus a_3$，即流密码的递推关系式为 $a_{i+3}=a_{i+2}\oplus a_i$

7．若 GF(2)上的二元加法流密码的密钥生成器是 n 级线性反馈移位寄存器，产生的密钥是 m 序列。2.5 节已知，敌手若知道一段长为 2n 的明密文对就可破译密钥流生成器。如果敌手仅知道长为 2n－2 的明密文对，问如何破译密钥流生成器。

解：破译 n－LFSR 所产生的 m 序列，需要 2n 个连续比特，现在仅有 2n－2 个连续的密钥比特(由长为 2n－2 的明密文对逐位异或得到)，因此需要猜测后两个比特。这有 00，01，10，11 四种情况，对这些情况按下式逐一试破译

$$(a_{n+1}a_{n+2}..a_{2n})=(c_nc_{n-1}..c_1)\begin{pmatrix}a_1&a_2&\cdots&a_n\\a_2&a_3&\cdots&a_{n+1}\\\vdots&&&\\a_n&a_{n+1}&\cdots&a_{2n-1}\end{pmatrix}=(c_nc_{n-1}..c_1)\boldsymbol{X}$$

首先验证矩阵 $\boldsymbol{X}$ 的可逆性，如果不可逆则可直接排除此情况

其次对于可逆的情况，求解出$(c_nc_{n-1}..c_1)$，然后验证多项式 $p(x)=1+c_1x+\ldots+c_nx^n$ 是否是本原多项式，如果是，则是一解。

结果可能会多余 1 个。

8.设 J-K 触发器中$\{a_k\}$和$\{b_k\}$分别为 3 级和 4 级 m 序列，且

$\{a_k\}$＝11101001110100…

$\{b_k\}$＝001011011011000 001011011011000…

求输出序列$\{c_k\}$及周期。

解：由于 gcd(3，4)=1 且 $a_0+b_0=1$ 所以序列$\{c_k\}$的周期为$(2^3-1)(2^4-1)=105$

又由 J-K 触发器序列的递推式 $c_k=(a_k+b_k+1)c_{k-1}+a_k$，令 $c_{-1}=0$ 可得输出序列为：

$\{c_k\}$=11001001…

9．设基本钟控序列产生器中$\{a_k\}$和$\{b_k\}$分别为 2 级和 3 级 m 序列，且

$\{a_k\}$＝101101…

$\{b_k\}$＝10011011001101…

求输出序列$\{c_k\}$及周期。

解：序列$\{a_k\}$的周期 $p_1=2^2-1=3$，序列$\{b_k\}$的周期 $p_2=2^3-1=7$，$w_1=a_0+a_1+a_2=2$

而 gcd(w_1, p_2)=1。所以序列$\{c_k\}$的周期 $p=p_1p_2=3\times7=21$

记 LFSR2(产生序列$\{b_k\}$)的状态向量为σ_k，则σ_0＝(100)，在 LFSR1(产生序列$\{a_k\}$)的控制下，状态转移为：

$\{a_k\}$ 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

$\{a_k\}$ 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…

第三章作业

1．(1)设 M'是 M 的逐比特取反，证明：若 $Y=\mathrm{DES}_K(X)$则 $Y'=\mathrm{DES}_{K'}(X')$

证：①以 P_D 记 DES 中的所有置换，包括循环移位、左右交换，则 P_D 满足如下性质：

若 $T=P_D(Z)$，则 $T'=P_D(Z')$

在 DES 中，异或运算显然满足性质 $a'\oplus b'=a\oplus b$，及 $a'\oplus b=(a\oplus b)'$

因而 DES 中的函数 $F(R_{i-1}, K_i)$在 S 盒前是异或运算，所以 $F(R'_{i-1}, K'_i)=F(R_{i-1}, K_i)$

②由密钥编排方案中的运算部件知，

若 K 的子密钥为 $K_1,K_2,\ldots,K_{16}$，那么 K′的子密钥为 $K'_1,K'_2,\ldots,K'_{16}$

③若 X 经初始置换 IP 后记为 $L_0\|R_0$，则 X′经初始置换 IP 后记为 $L'_0\|R'_0$，

用 K 对 X 加密的第 i 轮输入为 $L_{i-1}\|R_{i-1}$，输出为 $L_i\|R_i$，

其中，$L_i=R_{i-1}$，$R_i=L_{i-1}\oplus F(R_{i-1}, K_i)$

设用 K′对 X′加密的第 i 轮输入为 $L'_{i-1}\|R'_{i-1}$，则其第 i 轮的输出满足

左半部分$=R'_{i-1}=L'_i$

右半部分$=L'_{i-1}\oplus F(R'_{i-1}, K'_i)=L'_{i-1}\oplus F(R_{i-1}, K_i)=(L_{i-1}\oplus F(R_{i-1}, K_i))'=R'_i$

即 $L'_i\|R'_i$，

④由归纳法知，前 16 轮的输出均满足逐比特取反的关系，在经过左右交换盒 IP^{-1} 两个置换运算，输出密文也满足取反关系　　#

(2)由(1)的结论，在对 DES 进行穷搜索攻击时，选择两个明密文对(M,C_1)和(M',C_2)，然后选择 $K\in F_2^{56}$，对 M 加密 $C=\mathrm{DES}_K(M)$，判断 $C=C_1$ 或 $C'=C_2$ 则分别说明 K 或 K′为正确密钥，否则 K 和 K′都不是密钥，从而一次加密运算可同时验证一对互反密钥，使搜索量减少一半

2．证明：DES 的解密变换是加密变换的逆

证：DES 的加密变换由 IP，16 轮迭代，左右交换，IP^{-1} 四部分构成，注意到解密时子密钥逆续使用，16 轮迭代与左右交换一起刚好构成 Feistel 网络，若 Feistel 网络输入为 X，输出为 Y，即 Y＝Feistel(X,K)，其中 K 为密钥，如果 K 的子密钥逆续使用则记为 Inv(K)，那么由 Feistel 网络的性质有 X=Feistel(Y,Inv(K))。

对任意的明文消息 M 加密可表示为 $C=IP^{-1}[\mathrm{Feistel}(IP(M),K)]$

即 IP(C)=Feistel(IP(M),K)

由 Feistel 网络的性质有 IP(M)=Feistel(IP(C),Inv(K))

而对密文 C 解密，即为明文$=IP^{-1}[\mathrm{Feistel}(IP(C),\mathrm{Inv}(K))]=IP^{-1}[IP(M)]=M$，所以解密变换是加密变换的逆　　#

3．在 DES 的 CBC 模式中 C_1 的一个错误明显地将影响 P_1 和 P_2 的结果

（1）P_2 以后的分组不受影响，这是因为 C_1 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 P_1 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 P_1 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。

5．在实现 IDEA 时，最困难的部分是模 $2^{16}+1$ 乘法运算，设 a 和 b 是两个 n 比特的非 0 整数，记$(ab \bmod 2^n)$为 ab 的 n 个最低有效位，$(ab \operatorname{div} 2^n)$为 ab 右移 n 位

(1) 证明存在惟一的非负整数 q 和 r，使得 $ab=q(2^n+1)+r$

证：令 q 为 $ab/(2^n+1)$的商，r 为 $ab/(2^n+1)$的余数，均非负，则 $ab=q(2^n+1)+r$

若存在另一对数 q_1，r_1 满足 $ab=q_1(2^n+1)+r_1$

两式相减的$(r_1-r)=(q-q_1)(2^n+1)$

由于$|(r_1-r)|\le 2^n$，所以当且仅当 $r_1=r$，$q_1=q$ 时上式才成立　#

(2) 求 q 和 r 的上下界

解：由(1)知，r 为余数，所以有 $0\le r\le 2^n$

又 a 和 b 的最大值为 2^n-1，所以 $0\le q\le [ab/(2^n+1)]\le [(2^n-1)^2/(2^n-1)]=[2^n-3+4/(2^n+1)]=2^n-3$ 对于 $n\ge 2$ 时都成立，当 n＝1 时，q＝0

所以，q 的上下界为 $0\le q\le 2^n-3$ （$n\ge 2$）n＝1 时，q＝0

(3) 证明 $q+r<2^{n+1}$

证：$q+r\le 2^n-3+2^n=2^{n+1}-3<2^{n+1}$

(4)，(5) 求(ab div 2^n)关于 q 的表达式和(ab mod 2^n)关于 q 和 r 的表达式

解：设 $ab=q_1 2^n+r_1$，则显然有 $q_1=(ab \text{ div } 2^n)$，$r_1=(ab \bmod 2^n)$

又 $ab=q(2^n+1)+r$，记为(a)式

当 $q_1\le r_1$ 时，$ab=q_1 2^n+r_1=q_1(2^n+1)+(r_1-q_1)$　记为(b)式

此时 $0\le (r_1-q_1)\le r_1\le 2^n-1$

由(1)的唯一性结论,比较(a),(b)两式知，$q_1=q$，$r_1-q_1=r$

即 $q_1=(ab \text{ div } 2^n)=q$，$r_1=(ab \bmod 2^n)=r+q_1=r+q$

当 $q_1>r_1$ 时，$ab=q_1 2^n+r_1=(q_1-1)(2^n+1)+(r_1-q_1)+(2^n+1)$　记为(c)式

此时，由假设 $q_1>r_1$，知$(r_1-q_1)<0$，及$(q_1-1)\ge 0$ 所以

$0<(r_1-q_1)+(2^n+1)\le 2^n$

即$(r_1-q_1)+(2^n+1)$为 $ab/(2^n+1)$的余数

所以比较两式(a),(c)两式知$(q_1-1)=q$，$(r_1-q_1)+(2^n+1)=r$

即 $q_1=(ab \text{ div } 2^n)=q+1$，$r_1=(ab \bmod 2^n)=r+q_1-(2^n+1)=r+(q+1)-(2^n+1)$

综上所述有

$$q_1=(ab \text{ div } 2^n)=\begin{cases} q, & q_1\le r_1 \\ q+1, & q_1\le r_1 \end{cases}=\begin{cases} q, & (ab\ div\ 2^n)\le (ab \bmod 2^n) \\ q+1, & (ab\ div\ 2^n)\ge (ab \bmod 2^n) \end{cases}$$

$$r_1=(ab \bmod 2^n)=\begin{cases} q+r, & q_1\le r_1 \\ q+r-2^n, & q_1\le r_1 \end{cases}=\begin{cases} q+r, & (ab\ div\ 2^n)\le (ab \bmod 2^n) \\ q+r-2^n, & (ab\ div\ 2^n)\ge (ab \bmod 2^n) \end{cases}$$

(6) 用(4)和(5)的结果求 r 的表达式，说明 r 的含义

当 $q_1\le r_1$ 时，$r=(r+q)-q=(r_1-q_1)=(ab \bmod 2^n)-(ab \text{ div } 2^n)$

当 $q_1>r_1$ 时，　$r=(r+q-2^n)-(q+1)+(2^n+1)=(r_1-q_1)+(2^n+1)=(ab \bmod 2^n)-(ab \text{ div } 2^n)+(2^n+1)$

所以 $r=ab \bmod (2^n+1)=\begin{cases} ab \bmod 2^n-ab\ div\ 2^n, & (ab\ div\ 2^n)\le (ab \bmod 2^n) \\ ab \bmod 2^n-ab\ div\ 2^n+2^n+1, & (ab\ div\ 2^n)\ge (ab \bmod 2^n) \end{cases}$

6. （1）在 IDEA 模乘运算中，将模数取为 $2^{16}+1$，是因为它是素数，从而所有非 0 元都有逆元

(2) 在 IDEA 的模加运算中，模数取为 2^{16} 使所有元素都有逆元，构成群运算，同时刚好在 16 位子段上运算，求模运算易于实现，而取为 $2^{16}+1$ 时则必须做额外处理

第四章部分课后题参考答案

4. 用推广的 Euclid 算法求 67 mod 119 的逆元

解：初始化：(1,0,119), (0,1,67)

1：Q=119/67=1，(0,1,67) , (1,-1,52)

2：Q=67/52=1，(1,-1,52), (-1,2,15)

3：Q=52/15=3，(-1,2,15), (4,-7,7)

4：Q=15/7=2，(4,-7,7), (-9,16,1)

所以 $67^{-1} \bmod 119 = 16$

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$\varphi(n)= \varphi(35)=24$，

由 RSA 加密体制可知，$ed \equiv 1 \bmod \varphi(n)$，即 $5d \equiv 1 \bmod 24$，所以 $d=5$

$\therefore M=C^d \bmod n = 10^5 \bmod 35 = 5$

11. 已知 $c^d \bmod n$ 的运行时间是 $O(\log^3 n)$，用中国剩余定理改进 RSA 的解密运算。如果不考虑中国剩余定理的计算代价，证明改进后的解密运算速度是原解密运算速度的 4 倍。

证明：RSA 的两个大素因子 p，q 的长度近似相等，约为模数 n 的比特长度 log$n$ 的一半，即 (log$n$)/2，而在中国剩余定理中要计算模 p 和模 q 两个模指数运算，与 $c^d \bmod n$ 的运行时间规律相似，每一个模指数运算的运行时间仍然是其模长的三次幂，即 $O[((\log n)/2)^3]= O(\log^3 n)/8$，这样在不考虑中国剩余定理计算代价的情况下，总的运行时间为两个模指数的运行时间之和，即 $O(\log^3 n)/8+O(\log^3 n)/8=O(\log^3 n)/4$，得证。

12. 设 RSA 加密体制的公开钥是(e，n)=(77，221)。

(1) 用重复平方法加密明文 160，得中间结果为

$160^2 \pmod{221}=185$，$160^4 \pmod{221}=191$，$160^8 \pmod{221}=16$，$160^{16} \pmod{221}=35$，

$160^{32} \pmod{221}=120$，$160^{64} \pmod{221}=35$，$160^{72} \pmod{221}=118$，$160^{76} \pmod{221}=217$，

$160^{77} \pmod{221}=23$，

若敌手得到以上中间结果就很容易分解 n，问敌手如何分解 n

解：由以上中间结果得 $160^{16} \pmod{221}=35=160^{64} \pmod{221}$，

此即 $160^{64}-160^{16} \equiv 0 \pmod{221}$

即 $(160^{32}-160^8)(160^{32}+160^8) \equiv 0 \pmod{221}$

$(120-16)(120+16) \equiv 0 \pmod{221}$

$104 \times 136 \equiv 0 \pmod{221}$

由 gcd(104,221)=13 及 gcd(136,221)=17，可知 221 的分解为 221=13×17

(2) 求解密密钥 d

$d=e^{-1} \bmod \varphi(221)=77^{-1} \bmod 12 \times 16$

由扩展 Eucild 算法可得 d=5。

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 y_B=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：$C_1=g^k \bmod p = 7^3 \bmod 71 = 59$

$C_2=y_B^k M \bmod p = 3^3 \times 30 \bmod 71 = 29$

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，C_2），求 C_2

解：由 $C_1=g^k \bmod p$ 得 $59=g^k \bmod p=7^k \bmod 71$，即 k=3

而 $C_2=y_B^k M \bmod p = 3^3 \times 30 \bmod 71 = 29$

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 $B=t\times A \bmod k=(57，3，25，31，8)$

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

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

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

$f(01000)=3$，$f(10100)=57+25=82=9 \bmod 73$

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：$t^{-1} \bmod k=17^{-1} \bmod 67=4 \bmod 67$

所以 $4\times(25，2，72，92) \bmod 67=(33,8,20,33)$

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”

16.已知 n＝pq，p，q 都是素数，x，$y\in Z_n^*$，其 Jacobi 符号都是 1，其中 $Z_n^*=Z_n-\{0\}$,证明：

（1）xy(mod n)是模 n 的平方剩余，当且仅当 x，y 都是模 n 的平方剩余或 x，y 都是模 n 的非平方剩余。

证明：必要性：若 xy(mod n)是模 n 的平方剩余，即存在 t 使得 $xy=t^2 \bmod n$，

而 n＝pq，显然必有 $xy=t^2 \bmod p$ 及 ，$xy=t^2 \bmod q$，

所以 xy 也同时是模 p 和模 q 的平方剩余，即(xy/p)=1 且(xy/q)=1

也即(x/p)(y/p)=1 和(x/q)(y/q)=1，　　(a)

又由题设(x/n)＝1 和(y/n)＝1 由雅可比符号定义，此即

(x/p)(x/q)=1 和(y/p)(y/q)=1　　(b)

所以当(x/p)＝1 时由(a)中(x/p)(y/p)=1 知(y/p)=1，而由(b)中(y/p)(y/q)=1 知(y/q)=1，再由(a)中(x/q)(y/q)=1 知(x/q)=1，即 x 同时是 p 和 q 的平方剩余，y 也同时是 p 和 q 的平方剩余，所以 x 和 y 都是 n 的平方剩余。

若(x/p)＝－1 时由(a)中(x/p)(y/p)=1 知(y/p)=－1，而由(b)中(y/p)(y/q)=1 知(y/q)=－1，再由(a)中(x/q)(y/q)=1 知(x/q)=－1，即 x 同时是 p 和 q 的非平方剩余，y 也同时是 p 和 q 的非平方剩余，所以 x 和 y 都是 n 的非平方剩余。

充分性：若 x 和 y 都是模 n 的平方剩余，则 x 和 y 也都是模 p 和模 q 的平方剩余，则(x/p)＝(x/q)＝(y/p)＝(y/q)＝1，所以 xy 也是模 p 和模 q 的平方剩余，所以 xy 是模 n 的平方剩余

若 x 和 y 都是模 n 的非平方剩余,则它们对于模 p 和模 q 至少有一种情况是非平方剩余，不妨设(x/p)＝－1 和(y/p)＝－1 则由(b)式知(x/q)＝－1，且(y/q)＝－1，即 x 和 y 也都是模 p 和模 q 的非平方剩余。所以(x/p)(y/p)＝(xy/p)＝(－1)(－1)＝1 以及(xy/q)＝1，即 xy 同时是模 p 和模 q 的平方剩余。所以 xy 是模 n 的平方剩余。#

（2）x^3y^5(mod n)是模 n 的平方剩余，当且仅当 x，y 都是模 n 的平方剩余或 x，y 都是模 n 的非平方剩余。

证明：若 x^3y^5(mod n)是模 n 的平方剩余，则 x^3y^5 模 p 和模 q 也是平方剩余，所以 $(x^3y^5/p)=1=(x/p)^3(y/p)^5$,由于勒让得符号的偶数次方肯定为 1(p|x 情况除外) 即有 $1=(x/p)(y/p)$，以下证明如(1)。

17．在 Rabin 密码体制中，设 p＝47，q＝59

（1）确定 1 在模 n 下的四个平方根。

解：由 $x^2=1 \bmod 47$，得 $x_1=1 \bmod 47$，$x_2=p-1=46 \bmod 47$

由 $y^2=1 \bmod 59$，得 $y_1=1 \bmod 59$，$y_2=q-1=59 \bmod 47$

n=47*59=2773

由中国剩余定理 CRT，1 在模 n 下的四个平方根分别为

$U_1=CRT(x_1，y_1)=CRT(1，1)=1*59*[59^{-1}(\bmod 47)]+1*47*[47^{-1}(\bmod 59)] \ (\bmod n)$

$=1*59*4+1*47*54 \ (\bmod 2773)=1$

U_2=CRT(x_1，y_2)＝CRT(1，58)＝1*59*4+58*47*54 (mod 2773)=471

U_3=CRT(x_2，y_1)＝CRT(46，1)＝46*59*4+1*47*54 (mod 2773)=2302

U_4=CRT(x_2，y_2)＝CRT(46，58)＝2772

（2）求明文消息 2347 所对应的密文

解：2347^2(mod 2773)＝1231

（3）对上述密文确定可能的明文

解：由 x^2＝9 mod 47，得 x_1＝3 mod 47，x_2＝p－3＝44 mod 47

由 y^2＝51 mod 59，得 y_1＝46 mod 59，y_2＝59－46＝13 mod 59

由中国剩余定理 CRT，1231 在模 n 下的四个可能明文分别为

U_1=CRT(x_1，y_1)＝CRT(3，46)＝3*59*[59^{-1}(mod 47)]+46*47*[47^{-1}(mod 59)] (mod n)

＝3*59*4+46*47*54 (mod 2773)=990

U_2=CRT(x_1，y_2)＝CRT(3，13)＝3*59*4+13*47*54 (mod 2773)=426

U_3=CRT(x_2，y_1)＝CRT(44，46)＝44*59*4+46*47*54 (mod 2773)=2347

U_4=CRT(x_2，y_2)＝CRT(44，13)＝2773－990＝1783

18．椭圆曲线 E_{11}(1,6)表示 $y^2=x^3+x+6$ (mod 11)，求其上的所有点

解：模 11 的平方剩余有 1，4，9，5，3

x＝1，4，6 时，y^2＝8 (mod 11)，无解，x＝9 时，y^2＝7 (mod 11)，无解，x＝0 时无解

x＝2 时，y^2＝2 (mod 11)，y＝4 或 7，x＝3 时，y^2＝3 (mod 11)，y＝5 或 6

x＝5，7，10 时，y^2＝4 (mod 11)，y＝2 或 9，x＝8 时，y^2＝9 (mod 11)，y＝3 或 8

所以，E_{11}(1,6)上所有点为：

{（2，4），（2，7），（3，5），（3，6），（5，2），（5，9），（7，2），（7，9），（8，3），（8，8），（10，2），（10，9），O}

19．已知点 G=（2，7）在椭圆曲线 E_{11}(1,6)上，求 2G 和 3G

解：求 2G:

λ=(3×2^2＋1)/(2×7) mod11＝13×4 mod11＝8

x_3＝8^2－2－2 mod 11＝5，y_3＝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

x_3＝2^2－5－2 mod 11＝8，y_3＝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 E_{11}(1,6)，生成元 G=（2，7），接收方 A 的秘密钥 n_A＝7

（1）求 A 的公开钥 P_A

解：P_A＝7G＝2×2G＋3G

先求 2×2G

λ=(3×5^2＋1)/2×2 mod11＝10×3 mod11＝8

x_3＝8^2－5－5 mod 11＝10，y_3＝8(5－10)－2 mod 11＝2

所以 2×2G＝2×(5，2)＝(10，2)

P_A＝(10，2)＋(8，3）

由于 λ=(3－2)/(8－10) mod11＝1×5 mod11＝5

x_3＝5^2－10－8 mod 11＝7，y_3＝5(10－7)－2 mod 11＝2

所以 P_A＝(7，2)

（2）发送方 B 欲发送 P_m＝(10，9)，选择随机数 k＝3，求密文 C

解：C=(kG，P_m＋kP_A)，kG＝3G＝（8，3），kP_A＝$2P_A$＋P_A＝3G+7G＝(2，7)＋(7，2)

由于 λ=(2－7)/(7－2) mod11＝－1

x_3＝(－1)^2－2－7 mod 11＝3，y_3＝－1(2－3)－7 mod 11＝5

P_m+kP_A=(10，9)+(3，5)

由于λ=(5－9)/(3－10) mod11＝－1

$x_3=(-1)^2-10-3 \bmod 11=10$，$y_3=-1(10-10)-9 \bmod 11=2$

所以 C=(kG，P_m+kP_A)＝（（8，3），（10，2））

（3）显示接收方 A 从密文 C_m 恢复消息 P_m 的过程

解：P_m＝（P_m+kP_A）－$n_A(kG)$＝（10，2）－7（8，3）＝（10，2）－（3，5）＝（10，2）＋（3，6）＝(10，9)

第五章作业参考答案

1．6.1.3 节的数据认证算法是由 CBC 模式的 DES 定义的，其中初始向量取为 0，试说明使用 CFB 模式也可获得相同的结果。

解：设需认证的数据分为 64 比特长的分组，$D_1,D_2,\ldots,D_N$，其中 D_N 不够 64 比特则右边补 0，

由题设，数据认证算法相当于在 CBC 模式中初始向量取为 0，并按如下关系进行：

$O_1=E_K(D_1\oplus 0)$； $O_2=E_K(D_2\oplus O_1)$；… $O_N=E_K(D_N\oplus O_{N-1})$；

数据认证码取为 O_N 或 O_N 的最左 M 个比特

对于同样的认证数据序列，$D_1,D_2,\ldots,D_N$，使用 DES 的 CFB 模式，且取 $j=64$，IV=D_1，并从 D_2 开始加密得

$C_1=E_K(D_1)\oplus D_2=O_1\oplus D_2$，$C_2=E_K(C_1)\oplus D_3=E_K(O_1\oplus D_2)\oplus D_3=O_2\oplus D_3$，

由此可推出，对最后一个分组 D_N 加密后的密文 $C_{N-1}=O_{N-1}\oplus D_N$，则此时将 CFB 模式再进行一步，在该步中只计算 DES 的输出，则该输出值为 $E_K(C_{N-1})=E_K(O_{N-1}\oplus D_N)=O_N$。

所以可获得相同的结果。

2．有很多杂凑函数是由 CBC 模式的分组加密技术构造的，其中的密钥取为消息分组。例如将消息 M 分成分组 $M_1,M_2,\ldots,M_N$，H_0=初值，迭代关系为 $H_i=E_{Mi}(H_{i-1})\oplus H_{i-1}(i=1,2,\ldots,N)$，杂凑值取为 H_N，其中 E 是分组加密算法。

(1)设 E 为 DES，第 3 章习题 1 已证明如果对明文分组和加密密钥都逐比特取补，那么得到的密文也是原密文的逐比特取补，即如果 $Y=\mathrm{DES}_K(X)$则 $Y'=\mathrm{DES}_{K'}(X')$。利用这一结论证明在上述杂凑函数中可对消息进行修改但却保持杂凑值不变。

证：由 DES 的取反特性，如果令 M_i 和 H_{i-1} 取反，则有

$E_{M'i}(H'_{i-1})\oplus H'_{i-1}=[E_{Mi}(H_{i-1})]'\oplus H'_{i-1}=E_{Mi}(H_{i-1})\oplus H_{i-1}=H_i$

因此对任意的初始值 H_0，如果将 H_0 取反且将第一个消息分组 M_1 也取反则杂凑值不变

(2)若迭代关系改为 $H_i=E_{Hi-1}(M_i)\oplus M_i$，证明仍可对其进行上述攻击。

证：与(1)同，略。

3．考虑公钥加密算法构造杂凑函数，设算法是 RSA，将消息分组后用公开钥加密第一个分组，加密结果与第二个分组异或后，再对其加密，一直进行下去。设一消息被分成两个分组 B_1 和 B_2，其杂凑值为 $\mathrm{H}(B_1,B_2)=\mathrm{RSA}(\mathrm{RSA}(B_1)\oplus B_2)$。证明对任一分组 C_1 可选 C_2，使得 $\mathrm{H}(B_1,B_2)=\mathrm{H}(C_1,C_2)$，证明这种攻击方法，可攻击上述用公钥加密算法构造的杂凑函数。

证：攻击值如果获得两个消息分组 B_1 和 B_2，及其杂凑值 $\mathrm{H}(B_1,B_2)$，则攻击者可任选分组 C_1 并令 $C_2=\mathrm{RSA}(B_1)\oplus B_2\oplus\mathrm{RSA}(C_1)$

于是有 $\mathrm{H}(C_1,C_2)=\mathrm{RSA}(\mathrm{RSA}(C_1)\oplus(\mathrm{RSA}(B_1)\oplus B_2\oplus\mathrm{RSA}(C_1)))=\mathrm{RSA}(\mathrm{RSA}(B_1)\oplus B_2)=\mathrm{H}(B_1,B_2)$则攻击成功。

6．设 $a_1a_2a_3a_4$ 是 32 比特长的字中的 4 个字节，每一 a_i 可看作由二进制表示的 0 到 255 之间的整数，在 big－endian 结构中该字表示整数 $a_12^{24}+a_22^{16}+a_32^8+a_4$，在 little-endian 结构中该字表示整数 $a_42^{24}+a_32^{16}+a_22^8+a_1$。

(1)用 MD5 使用 little－endian 结构，因消息的摘要值不应依赖于算法所用的结构，因此在 MD5 中为了对以 big－endian 结构存储的两个字 $X=x_1x_2x_3x_4$ 和 $Y=y_1y_2y_3y_4$，进行模 2^{32} 加运算，必须对这两个字进行调整，试说明如何调整？

解：首先对 X 中的 4 个字节做如下处理：

将 x_1 和 x_4 交换，x_2 和 x_3 交换，对 Y 进行相同的处理

然后计算 $Z=X+Y \bmod 2^{32}$

最后再将 z_1 和 z_4 交换，z_2 和 z_3 交换。

第六章重点课后题参考答案

1．在 DSS 数字签名标准中，取 p=83=2×41+1，q＝41，h＝2，于是 g≡2^2≡4 mod 83，若取 x＝57，则 $y≡g^x≡4^{57}$＝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 $r＝(g^k \bmod p) \bmod q＝(4^{23} \bmod 83) \bmod 41=51 \bmod 41=10$

k^{-1}mod q=23^{-1} mod 41=25

$s=k^{-1}(M+xr) \bmod q$=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＝$(g^{u1}y^{u2} \bmod p) \bmod q$=($4^9$×$77^6$ mod 83) mod 41＝10

所以有 v＝*r*′，即验证通过。

2．在 DSA 签字算法中，参数 k 泄漏会产生什么后果？

解：如果攻击者获得了一个有效的签名(*r*,*s*)，并且知道了签名中采用的参数 k，那么由于在签名方程 $s=k^{-1}(M+xr) \bmod q$ 中只有一个未知数，即签名者的秘密钥 x，因而攻击者可以求得秘密钥 x＝$r^{-1}(sk－M) \bmod q$，即参数 k 的泄漏导致签名秘密钥的泄漏。