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} mod 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(mod 221)=185，160^4(mod 221)=191，160^8(mod 221)=16，160^{16}(mod 221)=35，
160^{32}(mod 221)=120，160^{64}(mod 221)=35，160^{72}(mod 221)=118，160^{76}(mod 221)=217，
160^{77}(mod 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}(mod 221)=35＝160^{64}(mod 221)，

此即 $160^{64}-160^{16}=0 \pmod{221}$

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

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

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

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×(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”

16.已知 n＝pq，p，q 都是素数，x，y∈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}(mod 47)]+1*47*[47^{-1}(mod 59)] (mod n)

＝1*59*4+1*47*54 (mod 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=(3×2²＋1)/(2×7) mod11＝13×4 mod11＝8

x_3＝8²－2－2 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＝2²－5－2 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=(3×5²＋1)/2×2 mod11＝10×3 mod11＝8

x_3＝8²－5－5 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＝5²－10－8 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 $\lambda = (5-9)/(3-10) \bmod 11 = -1$

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

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）$= (10，9)$