4、用推广的Euclid算法求的逆元。

解1：119=1×67+52

67=1×52+15

52=3×15+7

15=2×7+1

故 1=15-2×7

=15-2×（52-3×15）

=-2×52+7×15

=-2×52+7×(67-52)

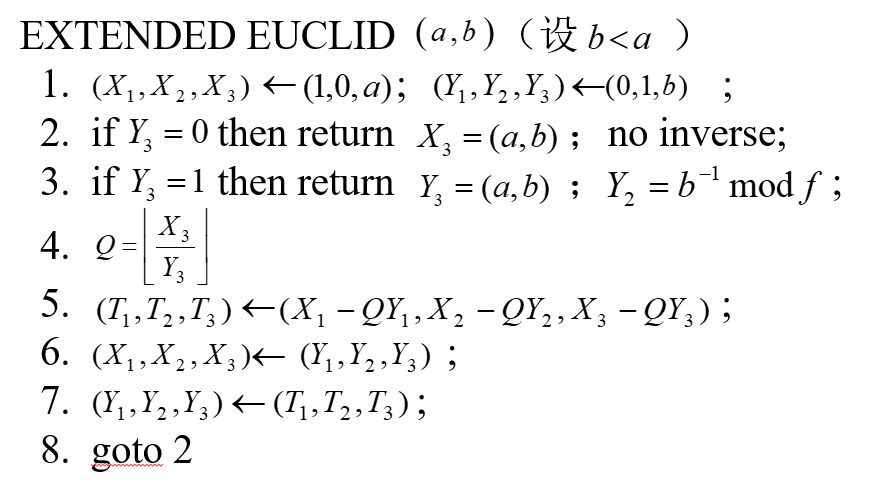
=7×67-9×52

=7×67-9×(119-67)

=-9×119+16×67

所以

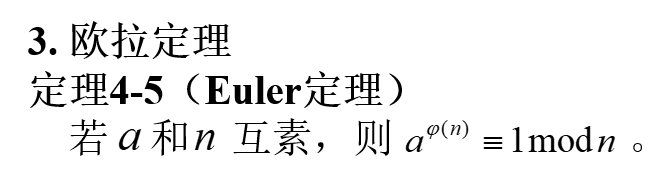
解2：利用辗转相除法求解原理：



求解过程：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | X1 | X2 | X3 | Y1 | Y2 | Y3 |
| —— | 1 | 0 | 119 | 0 | 1 | 67 |
| 1 | 0 | 1 | 67 | 1 | -1 | 52 |
| 1 | 1 | -1 | 52 | -1 | 2 | 15 |
| 3 | -1 | 2 | 15 | 4 | -7 | 7 |
| 2 | 4 | -7 | 7 | -9 | 16 | 1 |

解3：利用欧拉定理求解：



根据欧拉定理：

故有：

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

解：此题应该理解为接收方是合法的接收者，故应该考虑接收方知道模n的两个素因子，由于

n＝35＝5×7，故模n的两个素因子为5，7.



由e＝5，则，

所以

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

解： 计算公钥，B＝（t×A）mod k

则 

则 

同理，可得









故

对明文good night进行编码，编码方式为对26个英文字母，按其在字母表中的序号进行编码，空格编码为00000，每个字母需要5个比特长度的二进制信息表示，则明文编码为：

00111 01111 01111 00100 00000 01110 01001 00111 01000 10100

背包序列长度为5，故对明文的分组长度也为5，故对明文的加密为：

其中

所以：



同理：













所以密文为：（64，67，67，25，0，59，11，64，3，82）

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

解：利用上题中的推广的Euclid算法，可求

t－1mod67＝4

分别用t－1乘以密文25、2，72、92，可得

4×25mod67＝33

4×2 mod67＝8

4×72mod67＝20

4×92mod67＝33

设每一分组的明文都为（x1，x2，x3，x4，x5），

则对于第一个分组：

因为：33=33，故x5＝1；

33-33=0, 故有x4＝0；

x3＝0；

x2＝0；

x1＝0；

所以第一个分组的明文为（0，0，0，0，1）

采用同样的方法，对于第二、三、四个分组可分别得明文为：

第二分组明文：（0，0，1，0，0）

第三分组明文：（1，0，0，1，0）

第四分组明文：（0，0，0，0，1）

17、在Rabin密码体制中设p＝53，q＝59

（1）确定1在模n下的4个平方根？

（2）求明文消息2347所对应的密文？

（3）对上述密文，确定可能的4个明文？

此题中，，所以不满足Rabin密码对参数的要求，在素数较大的情况下，可能无法求出方程的解，在素数较小的情况下，可以穷举出答案。因此，本题考虑两种情况进行解答，第一种，使用书上题中的p＝53进行解答，第二章，考虑修改p值，使其满足Rabin密码的条件，比如可以修改为p＝43。先考虑第一种情况：

解：（1）设方程的解为x，则得方程：



该方程可分解为如下的方程组：

 两个解分别为1，52

 两个解分别为1，58

由此可得4个方程组：

利用中国剩余定理求解这四个方程组：



利用扩展欧几里德算法，可算出

同理，，可算出

因此，利用中国剩余定理，第一方程的解为；

第二组方程：

第三组方程：

第四组方程：

所以1在模n下的4个平方根为：1，1066，2066，3126

（2）因为：，故无需对明文进行分组，因此加密为



故密文为：1762

（3）设1762模n的平方根为x，得方程：



该方程可分解为如下的方程组：

 两个解分别为15，38

 两个解分别为13，46

由此可得4个方程组：

利用（1）中求得的，，利用中国剩余定理，分别求4个方程组，则

第一个方程组：

第二个方程组：

第三个方程组：

第四个方程组：

在考虑第二种情况：即p＝43的情况：

（1）设方程的解为x，则得方程：



该方程可分解为如下的方程组：

利用中国剩余定理求解：



利用扩展欧几里德算法，可算出

同理，，可算出



所以，可以得到x的四个解分别为：

x＝1 或x＝2536 或1592或945。

（2）因为：，故无需对明文进行分组，因此加密为



故密文为：582

（3）设方程的解为x，则得方程：



该方程可分解为如下的方程组：

利用中国剩余定理求解：



利用扩展欧几里德算法，可算出

同理，，可算出



所以，可以得到x的四个解分别为：

x＝2347 或x＝190 或1960或577。

20、 利用椭圆曲线实现ElGamal密码体制，设椭圆曲线是，生成元是G（2,7），接收方A的秘密钥。

（1）、求A的公开钥；

（2）、发送方B欲发送消息=（10,9），选择随机数k=3，求密文；

（3）显示接收方A从密文恢复消息的过程。

（1）解：根据题意，可得椭圆曲线为：，

则接收方A的公钥;

求2G：

所以2G=（5,2）

求4G=2G+2G：

所以4G=（10,2）

求3G=G+2G：

所以 3G=（8,3）；

求7G=3G+4G：

所以7G=（7,2）即接收方A的公开钥=（7,2）；

（2）发送方B欲发送消息=（10,9），选择随机数k=3，求密文；

根据椭圆曲线加密方案，加密方加密的密文为：

则加密最终的结果为两个椭圆曲线上的点，即点kG和点

先看点kG，因为选择的随机数k=3，即需要求3G，而在（1）个问题，实际上已经求得了3G的值，即3G=（8,3）；所以，只需求点即可

求=（10,9）+3=（10,9）++2

所以，需要先求2：

所以2=（2,7）

求3=：

所以3=（3,5）

求：=（10,9）+（3,5）

=（10,9）+（3,5）=(10,2),

所以，加密德密文：

（3）显示接收方A从密文恢复消息的过程。

解：接收方A从密文恢复消息的过程是：

在上式中，对于接收来说，已知的数据有：=（10,2），=（8,3），秘密钥，所以要求的为：

=（10,2）-7（8,3）

因此，这里的关键是要求出7（8,3）这个点，这个求法和第一步求的步骤完全一样，我这里略过这个过程，最后求得的7（8,3）=（3,5）；-7（8,3）=（3,6）。

然后再求（10,2）-7（8,3）=（10,2）+（3,6）=（10,9）。