第7章　公钥密码

1. **一个使用RSA公钥密码体制的公开密钥系统中，设p=43，q=59，取e=13，试加密“pu”并解密（为简化，将pu代替数字1520作为一个整体运算）。**

答案：已知RSA公钥密码算法，参数p=43,q=59,n=p×q=2537,φ(2537)=(p-1)(q-1)=42×58=

2436,其中选取e=13,gcd(13,2436)=1,13×d≡1mod2436,因此计算得到d=937。

公钥：（n,e）=(2537,13)。

私钥：d=937。

明文：pu,由题目可知，明文编码后取m=1520。

加密：利用c≡m13 mod 2537,得到密文0095。

解密：利用m≡c937 mod 2537,利用计算器可以得到明文1520即”pu”。

1. **设在一个使用RSA公钥密码体制的密码应用系统中，有两个用户A与B使用了相同模数161，且公钥（加密指数）分别为5与7，若你作为一个攻击者，当同时截获用户C分别发给用户A与用户B加密同一消息*m*的密文c1=27与c2=55时，试恢复消息*m*。**

答案：由题意得：*m*5=27mod161，*m*7=55mod161，因为gcd(5,7)=1，计算得：

3×5+（-2）×7=1mod(φ(n))。

得到，(*m*5)3×(*m*7)-2=*m*mod161

也就是*m*=(27)3×(55)-2=(27)3×(55-1)2 mod161

其中，55-1mod161=41，所以*m*= (27)3×(41)2 mod161。

又因为，(27)3 mod161=41，那么，*m*= 41×(41)2 =(41)3 =13mod161。

1. **已知某个RSA公钥密码体制的公钥(e,n)=(23,247)，且泄露φ(n)=216，请你作为攻击者完成以下工作：**

**（1）不采用小整数去试除的方法，分解该RSA密码的模数*n*；**

**（2）试求出该RSA密码的私钥d；**

**（3）如果截获该RSA密码加密的一个密文c=10，试求出相应的明文*m*。**

答案：（1）通过已知条件n=249,φ(n)=216,可以得到以下方程组：

解得p=19,q=13或者p=13,q=19。

（2）由题意得，n=249, φ(n)=216,e=23,gcd(23,216)=1, (e×d-1)modφ(n)=0,得私钥d=47。

（3）由题意可得，带入c≡me mod φ(n) ,m=6。

**4．在一个RSA密码中，已知公钥为（51，253），试求出相应的私钥（即解密指数）及加密明文18所对应的密文。**

答案：由题意得，n=253,e=51,可知p=11,q=23, φ(n)=22×10=220,且满足gcd(253,36)=1

,(51×d-1)mod220≡0,因此计算得到私钥d=151。

由题意可得，带入c≡me mod φ(n) ,c=110。

**5．设通信双方使用RSA公钥密吗体制，接收方的公钥是(*e*，*n*)=(3，253)，接收的密文是*c*=110，求明文*m*。**

答案：由题意得，n=253,e=3,c=110,可知p=11,q=23, φ(n)=22×10=220, 且满足gcd(253,3)=1

(3×d-1)mod220≡0, 因此计算得到私钥d=73,加密c≡me mod φ(n) ,m=11073mod253，m=6.

**6．在ElGamal公钥密码体制中，设素数*p*=71，a=7是Zn的生成元，β=3是公开的加密密钥，（1）设随机整数*k*=2，试求明文*m*=30所对应的密文；（2）假设选取一个不同的随机整数*k*，使得明文*m*=30所对应的密文为(59,c2)，试确定c2。**

答案：（1）令m=30所对应的密文为(c1,c2)，则c1=akmodp=72mod71=49，

c2=m×βkmodp=30×32mod71=57，所以密文为c=(47,57)。

（2）c1=7kmod71=59，则k=3，所以c2=30×33mod71=29。c=(c­1,c2),c1=akmodp=72mod71=49,

c2≡mβkmodp≡30×32mod71≡270mod71≡57mod71。

**7．设通信双方使用RSA公钥密码体制，接收方的公开密钥是（5，35），接收的密文是10，求明文。**

答案：由已知公钥（e,n）=(5,35),c=10,n=35=p×q=5×7, φ(n)=4×6=24，（5d-1）mod 24≡0,d=5,

m≡cd mod φ(n) ,m=5。

**8．在RSA公钥密码体制中，有一个公开的密钥*e*和一个保密的解密密钥*d*，还有一个公开的模板*n*，假设一个用户泄露了他的解密密钥*d*，这时他需要更换新的参数，但他只选取了新的加密密钥e’和解密密钥d’，而没有更换*n*，这样做安全吗？为什么？**

答案：不安全，原因如下：

RSA：1<e<φ(n)且ed ≡1 modφ(n)，泄漏了*d*后，φ(n)容易被计算出来；在*n*不变的情况，φ(n)不变，即便是更改成公钥e’，则e’d’ ≡1 modφ(n)可求出d’。

综合以上，这样不安全。

**9．设RSA公钥密码体制中的模数为35，试证明其加密密钥和解密密钥一定相同。**

答案：因为n=35，得φ(n)=24，因为1<d,e<24，且（*e*，24）=1，（*d*，24）=1，所以*d*，*e*可以选取的对应数分别为：5,7,11,13,17,19,23和5,7,11,13,17,19,23，所以加解密的密钥一定相同。

**10．证明：在RSA公钥密码体制中，对于素数*p*和*q*的每一种选择，存在公钥1<e<φ(n)，使得对于任意的明文*x*都有xe=x mod n。**

答案：令，因为φ(n) =（p-1）（q-1）>1，所以1<w<φ(n)，p-1|e-1,

q-1|e-1，所以对于任意的*x*，都有xe=xmodn。

**11．设在RSA公钥密码体制中，已选定素数*p*、*q*及加密指数*e*，且计算出模数n=pq与解密指数*d*，为了快速，私钥不用*d*，而用4个数*p*、*q*，d1=d mod (q-1)与r=q-1modp。这时，相应于密文*c*的明文m=q﹒(r(m1-m2)mod p)+m2(其中m1=cd1 mod p，m2=cd2mod q），试给出证明。**

（基于中国剩余定理进行证明，有待完善）