加密：C = mod n

解密：M = mod n

加密：C = mod 221 = 8

13 = 1 + 4 + 8

602 = 3600 ≡ 64(mod 221)

604 ≡ 642 ≡ 118(mod 221)

608 ≡ 1182 ≡ 1(mod 221)

因此6013 = 601+4+8 ≡ 60\*118\*1 ≡ 8(mod 221)

解密：M = mod 221 = 60

133 = 1 + 4 + 128

82 = 64

84 = 642 ≡ 118(mod 221)

88 ≡ 1182 ≡ 1(mod 221)

8128 = (88)16 ≡ 1(mod 221)

因此8133 = 81+4+128 ≡ 8\*118\*1 ≡ 60(mod 221)

加密：C = mod n

解密：M = mod n

= mod n

= mod n = M

mod n = M成立的证明过程如下：

若M不能整除p，因p为质数，因此M与p互质。

此时满足费马小定律：

M与p互质时，Mp-1≡1(mod p)

由ed≡1(mod (p-1)(q-1))得：ed=(p-1)(q-1)N+1

Med=M(p-1)(q-1)N+1=M\*(M(p-1))(q-1)N≡M(mod p)

若M可以整除p，此时Med≡0≡M(mod p)

因此无论M是否整除p，均有Med≡M(mod p)

同理可得：Med≡M(mod q)

即：Med-M同时p和q整除,因p、q为不同质数，

因此：Med-M被n=pq整除，即 mod n = M成立。

RSA防范计时攻击操作过程：

1、产生0至n-1之间随机数r。

2、计算C’=C(re) mod n。

其中e为公钥中的e。

3、与之前相同，计算M’=(C’)d mod n。

4、计算M = M’r-1 mod n。

其中r-1为r的模n的乘法逆元。

证明过程：

因red ≡ r (mod n)，即：red-1 ≡ 1(mod n)

因此：M’r-1 mod n = (C’)dr-1 mod n

= (C(re))dr-1 mod n

= Cdred-1 mod n = Cd mod n = M。

即：M = M’r-1 mod n。