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：

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

根据费马小定律：xp-1≡1(mod p)，

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

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

即：Med-M同时p和q整除,因p、q为不同素数，

因此：Med-M被n=pq整除，即 mod n = M成立。