《密码学》课程习题

执笔 张焕国

第五章习题

1、 证明 RSA 密码加解密算法的可逆性。

2、 证明 RSA 密码加解密算法的可交换性。

3、 说明对于 RSA 密码从公开加密钥不能求出保密的解密钥。

4、 令 p=3,q=11,d=7,m=5,手算密文 C 。

5、 设 RSA 密码的 e=31,n=35,C=10,手算明文 M 。

6、 分析反复平方乘算法的计算复杂度。

7、 分析 Montgomery 算法计算模幂速度快的原因。

8、 在利用函数 **Mon**（A，B，R，n）计算 y=ab mod n 的完整过程中，需要按式(5-18)进行预处理。若将式(5-18)的预处理改为 A＝aR , B=b，即只对 A 进行预处理，有什么优点？又有什么缺点？

9、 在 RSA 中使用 e=3 作为加密指数有何优缺点？使用 d=3 作解密指数的好吗？为什么？

10、 证明 ELGamal 密码的可逆性。

11、 为什么 ELGamal 密码要求参数 K 是一次性的？

12、 设 p=5，m=3,构造一个 ELGamal 密码，并用它对 m 加密。

13、 证明例 5-8 中 P_{12}= (1000，0001)的阶为 11。

14、 取为 p=29,求出椭圆曲线 $y^2=x^3+4x+20$ 的全部解点。

15、 以教材例 5-5 为例，分别以 G=(2,7)和 G=(5,2)构造椭圆曲线密码，

并设 m=3，分别进行加密和解密。

16、 以教材例 5-8 为例，以 G= P_5= (0010，1111)构造椭圆曲线密码，并设 m= (1010) ，分别进行加密和解密。