1、已知背包密码系统中的私钥分别为超递增序列 A=(3、4、9、17、35)，模数 p=73 和乘数 t=19，试对 good job 进行加密(利用字母对应的 ASCII 码值的二进制进行加密)。

2、若通信双方使用 RSA 单向陷门函数加解密信息，已知接收方公钥(e,n)=(5,35)，截获密文为 C=10，求明文 M。

3、RSA 算法中，选择 p=7,q=17,e=13,计算其公钥与私钥，并采用快速模乘（重复平方乘）方法，计算明文 m=19 对应的密文。

4、发送方 A 使用 ElGamal 算法进行加解密信息，已知接收方 B 的公钥($p=71, g=7, y_B=3$)。

1) 若发送方 A 在加密过程中选择的随机整数 k=3，求明文 M=10 所对应的密文。

2) 若攻击者 C 截获了 A 发送的密文是 C=(59,29)，试恢复消息 M。

5、利用椭圆曲线实现 ElGamal 密码体制，设椭圆曲线是 $E_{11}(1,6)$，生成元 G=(2,7)，接收方 A 的私钥 $n_A=7$。

1) 求 A 的公钥 PA。

2) 若发送方 B 欲给 A 发送消息 $P_m=(10,9)$，选择随机数 k=3，求密文 C_m。

3) 简述接收方 A 从密文 C_m 恢复消息 P_m 的过程。

6、 简述 CRT-RSA 的密钥生成、加密及解密运算的过程。

7、已知循环群G，生成元为g，简述A、B利用Diffie-Hellman 密钥交换协议生成公共密钥的过程。