（附卷纸　0　页）

得分：_____　3.（10分）设背包密码系统的超递增序列为（1，3，5，10），乘数 t=9,模数 k=20，请按背包公钥密码体制求公开密钥，并说明发送明文 M=1101 的加解密过程。

得分：_____ 4. （10 分）在 Shamir 秘密分享方案中，设 t=3，n=5，p=13，ID 号分别为 1, 2, 3, 4, 5 的 5 个人所分得的秘密值分别为 1, 5, 4, 11, 0，请从中任选 3 个，请利用拉格朗日插值公式构造插值多项式并求出共享秘密 K。

（附卷纸　0　页）

得分：_____　　5. （10 分）已知椭圆曲线 E：$y^2=x^3+x+1(\mathrm{mod}\ 5)$，求

（1） 满足该曲线方程的所有点（无穷远点除外）；　（5 分）

（2） 在椭圆曲线上任取一点 $P=(0,1)$，分别求出-P 点、2P 点、3P 点的坐标　（5 分）

得分：_____ 五、分析题（共 20 分）

得分：_____ 1. （10 分）请描述有限域上的离散对数问题，并基于该困难问题设计一种密钥交换协议，并分析该协议是否安全？若不安全，请给出具体攻击方法。

得分：
能否共

得分：_____　　2. （10 分）在 RSA 公钥加密体制中，n 为体制中使用的模数，在实际应用中能否共用模数 n？为什么？请说明理由。

1. $x_3 \equiv \lambda^2 - x_1 - x_2 \pmod p$

2. $y_3 \equiv \lambda(x_1 - x_3) - y1 \pmod p$

3. λ有两种情况：（1）P=Q，（2）P≠Q

4. P=Q情况下：$\lambda = (3x_1^2 + a)/(2 * y_1)$

5. P≠Q的情况下：$\lambda = (y_2 - y_1)/(x_2 - x_1)$

$$\lambda = \begin{cases} \dfrac{3x_1^2 + a}{2y_1}, & P = Q \\ \dfrac{y_2 - y_1}{x_2 - x_1}, & P \neq Q \end{cases}$$

$$x_3 \equiv \lambda^2 - x_1 - x_2 \pmod p$$

$$y_3 \equiv \lambda(x_1 - x_3) - y_1 \pmod p$$