1. 什么是对称密码体制，其实现加解密安全的基本手段是什么？什么是公钥密码体制，其实现安全性的根本依据是什么？（6分）

2. 根据攻击者能够获得的信息以及攻击能力，常见的攻击方式可以分为唯密文攻击等5种。请分别列出其他攻击方式，说明RSA的面临那种攻击？为什么？（8分）

3. 考虑如下同余方程组：（12分）

$$\begin{cases} x \equiv 7 \pmod{13} \\ x \equiv 5 \pmod{17} \\ x \equiv 3 \pmod{11} \end{cases} \tag{1}$$

(1) 方程组1在区间[0，2431]范围内有唯一解吗？请说明理由？

(2) 方程组1在区间[0，5000]的解是？

4.完成下列计算：（12分）

(1) 求多项式x^3+x+1在$\mathbb{Q}[x]/x^2+x+1$逆元。

(2) 求有限域GF(2^4)中x^2+1的逆，选不可约多项式x^4+x+1。

5. 考虑RSA公钥加密算法，给定明文$m=15$，私钥$k_{pr}=323$，$n=2263$：（14分）

(1) 求私钥k_{pr}加密所得密文(给出计算过程)。

(2) 利用pollard $p-1$分解n，求公钥k_{pub}。

6. 考虑Elgamal签名方案，给定公钥$k_{pub}=(p,\alpha,\beta)=(29,2,7)$，私钥$k_{pr}=d=12$，其中满足关系$\beta \equiv \alpha^d \pmod{p}$：（14分）

(1) 现给定消息$m=26$和临时密钥随机值$k_E=11$，请给出签名结果$Sig_{k_{pr}}(m,k_E)=(r,s)$。

(2) 现给出$m'=23$的签名为$(r',s')=(19,27)$，请判断该签名是否有效，说明理由。

7. 给定有限域GF(13)上的椭圆曲线$E: y^2=x^3+2x^2+5x+3$，令$p=(9,4)$（14分）

(1) E是否包含$x=4$的点？请说明理由。

(2) p是否在E上？如果在，求解$p+p$；如果不在，请说明理由。

8. 考虑Shamir秘密共享方案，在有限域GF(13)上，已知门限为3，给定share集合：$\{f(1)=1, f(2)=3, f(3)=0, f(4)=5, f(5)=5\}$，求秘密$f(0)$。（10分）

9. 给定$m_1=17, m_2=35$，请按照RSA的构造方法，令$n=m_1\times m_2$，构造一个类似RSA的加密方案？（10分）