1. （公钥密码算法实现）实现2048位RSA。

要求：需要包括素性检测，加解密（允许调用库）

1. （公钥密码算法计算）设E是Z11上的椭圆曲线。
   1. 计算E上的所有点。
   2. 证明 是本原元。
   3. 设为基点，使用椭圆曲线上的ElGamal算法，完成对明文 (为椭圆曲线上的点)的加解密（随机选择k=3）。
2. （数字签名算法）假设Alice使用ELGamal签名方案， 以及 。给定消息 的签名 以及 的签名 ，计算k和a的值。

附：ElGamal签名算法

