公钥密码作业

1. 公钥 (非对称) 密码能够实现加密、密钥交换, 还能用于实现对称密码无法提供的不可否认性等功能。我们为什么仍然需要在当前应用中使用对称密码算法?
2. 对一个 RSA 加密方案, 其参数设置为 $p = 41, q = 17$。
   (a) 给$e_1 = 25, e_2 = 49$。这两个数中哪一个可以作为该RSA加密算法的公钥, 为什么?
   (b) 对 (a) 中选定的公钥, 使用欧几里得算法计算器对应的私钥 d。
3. 对一个 RSA 加密方案, 其初始参数 $p = 31, q = 37$, 公钥为 $e = 17$。
   (a) 使用中国剩余定理解密密文 $c = 2$。
   (b) 通过常规的解密算法解密密文$c = 2$, 验证 (a) 步的解密结果。
4. 确定 Z_{13}^*中每个元素的阶。
5. 在 Diffie-Hellman 密钥交换协议中, 设 $p = 97, g = 5$, A 和 B 分别选取随机数 $a = 36$ 和 $b = 58$。试计算 A 和 B 之间建立的共享密钥 k。
6. 一个 ElGamal 密码系统的参数为模数 $p = 71$, 本原元 $g = 7$。
   (a) 如果接收者 B 的公钥为 $y_B = 3$, 发送者 A 随机选择整数 $k = 2$, 求明文 $m = 30$ 所对应的密文。
   (b) 如果发送者 A 选择另一个随机整数 k', 使得明文 $m = 30$ 加密后的密文为 $c = (59, c_2)$, 求c_2。
7. 设 E 是一条定义在模 7 上的椭圆曲线

$$E: y^2 = x^3 + 3x + 2 \bmod 7$$

   (a) 计算 E 上的所有点。
   (b) 该椭圆曲线上的点组成的群的阶是多少? (勿忽略无穷远点O)
   (c) 给一个元素 $P = (0, 3)$, 请确定 P 的阶。P是否是一个生成元?