公钥密码作业答案

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?

   解: 从理论的角度来说，公钥密码学可以用来替代对称密码学。但是，从现实应用来说，对称密码运行速度远远快于公钥密码算法 (约 1000 倍)。所以，对称密码常常被用于大规模数据加密。

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其对应的私钥 d。

   解: (a) $p = 41, q = 17$，则 $n = p \cdot q = 697, \varphi(n) = 40 \cdot 16 = 640 = 2^7 \cdot 5$。在RSA密码系统中公钥$e$需要与$\varphi(n)$互素，所有只有$e_2 = 49$可以被用作公钥。

   (b) $ed \bmod \varphi(n) = 1$，故 $d = e^{-1} \bmod \varphi(n) = 49^{-1} \bmod 640$

   根据欧几里得算法有

   $640 = 13 \cdot 49+3$

   $49 = 16 \cdot 3+1$

   从而$1 = 49-16 \cdot 3 = 49-16(640-13 \cdot 49) = 209 \cdot 49-16 \cdot 640$

   故私钥 $d = 49^{-1} \bmod 640 \equiv 209$。

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。

   解: (a) 由初始参数可得 $n = p \cdot q = 31 \cdot 37 = 1147, \varphi(n) = 30 \cdot 36 = 1080$,

   故私钥 $d = e^{-1} = 17^{-1} = 953 \bmod 1080$。

   $d_p = 953 \equiv 23 \bmod 30$

   $d_q = 953 \equiv 17 \bmod 36$

   $x_p = c^{d_p} = 2^{23} \equiv 8 \bmod 31$

   $x_q = c^{d_q} = 2^{17} \equiv 18 \bmod 37$

   $q^{-1} = 37^{-1} \equiv 6^{-1} \equiv 26 \bmod 31$

   $p^{-1} = 31^{-1} \equiv 6 \bmod 37$

   所以明文 $m = (qq^{-1})x_p+(pp^{-1})x_q = (37 \cdot 26) \cdot 8+(31 \cdot 6) \cdot 18 = 8440 = 721 \bmod 1147$。

   (2) $m = c^d \bmod n = 2^{953} = 721 \bmod 1147$

4. 按照《密码编码学与网络安全》——原理与实践 (第七版) 第 39 页表 2.7 的方式确定 Z_{13}^*中每个元素的阶。

解: 《密码编码学与网络安全》—原理与实践 (第七版) 第 39 页表 2.7 的方式构造模 13 的整数幂表如下, Z_{13}^*中每个元素的阶在最后一列。

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	阶
1												1
2	4	8	3	6	12	11	9	5	10	7	1	12
3	9	1										3
4	3	12	9	10	1							6
5	12	8	1									4
6	10	8	9	2	12	7	3	5	4	11	1	12
7	10	5	9	11	12	6	3	8	4	2	1	12
8	12	5	1									4
9	3	1										3
10	9	12	3	4	1							6
11	4	5	3	7	12	2	9	8	10	6	1	12
12	1											2

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。

解: 根据 $p = 97, g = 5, A$ 和 B 分别选取随机数 $a = 36$ 和 $b = 58$。

A 计算 $y_a = 5^{36} \bmod 97 = 50$, 并将 y_a 发送给 B。

B 计算 $yb = 5^{58} \bmod 97 = 44$, 并将 y_b 发送给 A。

然后, A 计算 $k = y_b{}^a = 44^{36} \bmod 97 =75$。

B 计算 $k = y_a{}^b = 50^{58} \bmod 97 = 75$。

故 A 和 B 之间建立的共享密钥 $k = 75$。

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。

解: (a) 由于选择整数 $k = 2$, 发送方A利用B的公钥$y_B = 3$计算:

$c_1 = g^k \bmod p = 7^2 \bmod 71 = 49$, $c_2 = m \cdot y_B{}^k \bmod p = 30 \times 3^2 \bmod 71 =57$。

消息$m = 30$的密文为 $c = (c_1, c_2) = (49, 57)$。

(c) 根据$c_1 = g^k \bmod \mathrm{p} = 7^k \bmod 71 = 59$可知$k = 3$，所以

$c_2 = my_B{}^k \bmod p = 30 \times 3^3 \bmod 71 = 29$。

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?

解: (a) 将0-6依次代入方程计算$x^3 + 3x + 2 \bmod 7$，然后判断所得的结果是否是mod 7的平方剩余，若是，则所得的点(x, y)在E上，通过这种方式可以求得E上的所有点为$\{(0, 3), (0, 4), (2, 3), (2, 4), (4, 1), (4, 6), (5, 3), (5, 4)\}$。

(2) 该椭圆曲线上的点组成的群的阶为

$\#\mathrm{G} = \#\{O, (0, 3), (0, 4), (2, 3), (2, 4), (4, 1), (4, 6), (5, 3), (5, 4)\} = 9$。

(3) 根据椭圆曲线上点的乘法规则我们可以计算$0P = O$, $1P = (0, 3)$, $2P = (2, 3)$, $3P = (5, 4)$, $4P = (4, 6)$, $5P = (4, 1)$, $6P = (5, 3)$, $7P = (2, 4)$, $8P = (0, 4)$, $9P = O = 0P$。

由上可知P的阶$\mathrm{ord}(P) = 9 = \#G$，所以$P = (0, 3)$是该椭圆曲线上的点组成的群的生成元。