信息安全引论作业 02

梁昱桐 2100013116

Peking University

1 题目1

用Fermat定理计算 $3^{201} \mod 11$ 。

1.1 解答

根据Fermat小定理，如果 p 是素数且 a 是一个不被 p 整除的整数，那么 $a^{p-1} \equiv 1 \pmod{p}$。因此：

$3^{10} \equiv 1 \pmod{11}$

所以：

$3^{201} = (3^{10})^{20} \times 3 \equiv 1^{20} \times 3 \equiv 3 \pmod{11}$

2 题目2

用Fermat定理找到一个位于0到72之间的数，使得 $a \mod 73$ 与 9^{794} 同余。

2.1 解答

根据Fermat小定理：

$9^{72} \equiv 1 \pmod{73}$

所以：

$9^{794} = 9^{72\times11+2} \equiv (9^{72})^{11} \times 9^2 \equiv 1^{11} \times 9^2 \equiv 9^2 \equiv 81 \equiv 8 \pmod{73}$

因此， $a \equiv 8 \pmod{73}$。

3 题目3

用RSA算法对下列数据实现加密和解密。

3.1 a 参数

- $p = 3$; $q = 11$; $e = 7$; $M = 5$

3.1.1 解答

1. 计算 $n = pq = 33$。
2. 计算 $\phi(n) = (p-1)(q-1) = 20$。
3. 计算私钥 d，满足 $ed \equiv 1 \pmod{\phi(n)}$，所以 $d = 3$。
4. 加密：$C = M^e \mod n = 5^7 \mod 33 = 14$。
5. 解密：$M = C^d \mod n = 14^3 \mod 33 = 5$。

3.2 b 参数

- $p = 3$; $q = 11$; $e = 7$; $M = 9$

3.2.1 解答

1. 加密：$C = M^e \mod n = 9^7 \mod 33 = 15$。
2. 解密：$M = C^d \mod n = 9^3 \mod 33 = 9$。

3.3 c 参数

- $p = 7$; $q = 11$; $e = 17$; $M = 8$

3.3.1 解答

1. 计算 $n = pq = 77$。
2. 计算 $\phi(n) = (p-1)(q-1) = 60$。
3. $d = 53$。
4. 加密：$C = M^e \mod n = 8^{17} \mod 77 = 57$。
5. 解密：$M = C^d \mod n = 57^{53} \mod 77 = 8$。

4 题目4

通过中国剩余定理（CRT）解决：六位教授分别在周一至周六开始授课，并且分别每隔2, 3, 4, 1, 6, 5天授课一次，该大学禁止周日上课。什么时候所有六位教授首次发现必须同时停一次课?

4.1 解答

假设我们考虑的天数是第 x 天（从第一个星期一开始算起），那么：

$$x = 1 + 2K_1 = 2 + 3K_2 = 3 + 4K_3 = 4 + K_4 = 5 + 6K_5 = 6 + 5K_6 = 7K_7 \tag{1}$$

其中 K_i 是整数，即：

1. $x \equiv 1 \pmod{2}$
2. $x \equiv 2 \pmod{3}$
3. $x \equiv 3 \pmod{4}$
4. $x \equiv 4 \pmod{1}$
5. $x \equiv 5 \pmod{6}$
6. $x \equiv 6 \pmod{5}$
7. $x \equiv 0 \pmod{7}$

在这些同余条件中，（4）没有限制，（1）和（2）不如（3）和（5）严格。在后两个条件中，（3）表明 x 同余于 3, 7 或 11（模 12），而（5）表明 x 同余于 5 或 11（模 12），所以（3）和（5）共同等价于 $x \equiv 11 \pmod{12}$。因此问题转化为求解：

$$x \equiv 11 \pmod{12} \tag{2}$$
$$x \equiv 6 \pmod{5} \tag{3}$$
$$x \equiv 0 \pmod{7} \tag{4}$$

或

$$\begin{aligned} x &\equiv -1 \pmod{12} \quad (5) \\ x &\equiv 1 \pmod{5} \quad (6) \\ x &\equiv 0 \pmod{7} \quad (7) \end{aligned}$$

我们计算得到：

- $m_1 = 12$，$m_2 = 5$，$m_3 = 7$，$M = 420$
- $M_1 = 35$，$M_2 = 84$，$M_3 = 60$

然后：

$$x \equiv (-1)(-1) \times 35 + (-1) \times 1 \times 21 + 2 \times 0 \times 60 \equiv -49 \equiv 371 \pmod{420} \quad (8)$$

满足条件的第一个 x 是 371。

5 题目5

设ElGamal体制的公用素数 $p = 71$，其本原根 $g = 7$。

5.1 a. 若 B 的公钥 $Y_b = 3$，A 选择的随机整数 $k = 2$，则 $M = 30$ 的密文是什么？

5.2 解答

1. 计算 $r = g^k \mod p = 7^2 \mod 71 = 49$。
2. 计算 $s = M \times Y_b^k \mod p = 30 \times 3^2 \mod 71 = 57$。
3. 密文为 $(49, 57)$。

5.3 b. 若 A 选择的 k 值使得 $M = 30$ 的密文 $C = (59, C_2)$，则整数 C_2 是多少？

5.4 解答

$7^k \equiv 59 \pmod{71}$，解得 $k = 3$。

$C_2 = M \times Y_b^k \mod p = 30 \times 3^3 \mod 71 = 29$。

6 题目6

在ElGamal算法中，为什么要使用不同的随机数 k 来加密不同的消息？

6.1 解答

如果使用相同的 k 来加密两个不同的消息 m_1, m_2，得到的密文分别为 $(a_1, b_1), (a_2, b_2)$，则 $\frac{b_1}{b_2} = \frac{m_1}{m_2}$。这意味着一旦已知 m_1，就可以很容易地计算出 m_2。因此，为了保证两次加密的安全性的独立性，每次加密都必须使用不同的随机数 k。