信息安全数学基础7—平方乘算法

杨礼珍

同济大学计算机科学与技术系, 2017

Outline

作业

阅读《密码学原理与实践》5.3.1节关于平方－乘算法的部分（P138-139）

如何快速实现指数运算？

Example

计算：3^9

方法一： 直接计算，需要8次乘法运算。

方法二： 注意到：

$$
\begin{aligned}
3^9 &= 3(3^4)^2 \\
&= 3((3^2)^2)^2 && \text{第1次乘法} \\
&= 3(9^2)^2 && \text{第2次乘法} \\
&= 3 \cdot 81^2 && \text{第3次乘法} \\
&= 3 \cdot 6561 && \text{第4次乘法} \\
&= 19683
\end{aligned}
$$

算法原理：

假定指数c的二进制表示为$c = (c_{l-1}, \ldots, c_1, c_0)$，那么

$$\begin{aligned} c &= c_{l-1}2^{l-1} + c_{l-2}2^{l-2} + \ldots + 2c_1 + c_0 \\ &= (2c_{l-1} + c_{l-2})2^{l-2} + c_{l-3}2^{l-3} + \ldots + 2c_1 + c_0 \\ &= (2(2c_{l-1}+c_{l-2})+c_{l-3})2^{l-3} + c_{l-4}2^{l-4} + \ldots + 2c_1 + c_0 \\ &= 2(\ldots 2(2(2c_{l-1} + c_{l-2})+c_{l-3}) + \ldots) + c_1) + c_0 \end{aligned}$$

因此有：

$$\begin{aligned} x^c &= x^{2(\ldots 2(2(2c_{l-1}+c_{l-2})+c_{l-3})+\ldots)+c_1)+c_0} \\ &= (\ldots(((x^{c_{l-1}})^2 x^{c_{l-2}})^2 x^{c_{l-3}})\ldots)^2 x^{c_0} \\ &= (\ldots(((1^2 \cdot x^{c_{l-1}})^2 x^{c_{l-2}})^2 x^{c_{l-3}})\ldots)^2 x^{c_0} \end{aligned}$$

平方-乘算法

根据：$x^c = (\ldots(((1^2 \cdot x^{c_{l-1}})^2 x^{c_{l-2}})^2 x^{c_{l-3}})\ldots)^2 x^{c_0}$

平方-乘算法(x, c, n)

计算：$z = x^c \bmod n$。
假定c的二进制表示为$c = \sum_{i=0}^{l-1} c_i 2^i, c_i \in \{0, 1\}$。
$z \leftarrow 1$(初始化)
for $i \leftarrow l - 1$ downto 0

$$\text{do} \begin{cases} z \leftarrow z^2 \bmod n & (\ldots)^2 \\ \text{if } c_i = 1 & \\ \text{then } z \leftarrow (z \times x) \bmod n & (\ldots \cdot x^{c_i}) \end{cases}$$

return (z)

计算复杂度分析：如果n的二进制表示有k位

- 乘法运算的复杂度为$O(k^2)$
- 乘法运算次数为$O(l) = O(\log_2(c))$

计算复杂度为$O((\log c) \times k^2)$。

Example

例5.5（续）$n = 11413$，公开的解密指数为$b = 3533$，Alice利用平方-乘算法计算$9726^{3533} \bmod 11413$来加密明文9726：

i	b_i	z
11	1	$1^2 \times 9726 = 9726$
10	1	$9726^2 \times 9726 = 2659$
9	0	$2659^2 = 5634$
8	1	$5634^2 \times 9726 = 9167$
7	1	$9167^2 \times 9726 = 4958$
6	1	$4958^2 \times 9726 = 7783$
5	0	$7783^2 = 6298$
4	0	$6298^2 = 4629$
3	1	$4629^2 \times 9726 = 10185$
2	1	$10185^2 \times 9726 = 105$
1	0	$105^2 = 11025$
0	1	$11025^2 \times 9726 = 5761$