

中国剩余定理:

定理 中国剩余定理

① 有解条件

设正整数 m_1, m_2, \dots, m_k 两两互素, 对任意整数 a_1, a_2, \dots, a_k , 一次同余方程组

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

在模 m 意义下有唯一解, 该解可表示为

$$x \equiv M_1 M_1^{-1} a_1 + M_2 M_2^{-1} a_2 + \dots + M_k M_k^{-1} a_k \pmod{m}$$

其中 $m = m_1 m_2 \dots m_k$, $M_j = m / m_j$, $M_j M_j^{-1} \equiv 1 \pmod{m_j}$, $j = 1, 2, \dots, k$.

Mignotte (t,n) 门限秘密共享方案:

秘密分割:

例题 基于中国剩余定理的(t,n)门限秘密共享方案

① (t,n) 门限, 选择 n 个整数 d_1, d_2, \dots, d_n , 满足

- (1) $d_1 < d_2 < \dots < d_n$; d_i 严格递增
- (2) $(d_i, d_j) = 1, i \neq j$; d_i 两两互素
- (3) $N = d_1 \times d_2 \times \dots \times d_t$ $2-1=1$

$M = d_{n-t+2} \times d_{n-t+3} \times \dots \times d_n$, 有

$N > M$

② 对于某个秘密 k , 要求 $N > k > M$, 计算

$$\begin{cases} k_1 \equiv k \pmod{d_1} \\ k_2 \equiv k \pmod{d_2} \\ \vdots \\ k_n \equiv k \pmod{d_n} \end{cases}$$

则子秘密为 (d_i, k_i) 。

秘密分割

$t=2, n=3$

(2,3) 门限, 选择 3 个整数 $d_1 = 9, d_2 = 11, d_3 = 13$

$N = 99, M = 13$, 有 $N > M$

对于秘密 $k = 74$, 要求 $99 > 74 > 13$, 计算

$$\begin{cases} k_1 \equiv 74 \equiv 2 \pmod{9} \\ k_2 \equiv 74 \equiv 8 \pmod{11} \\ k_3 \equiv 74 \equiv 9 \pmod{13} \end{cases}$$

一个秘密 k , 被分成 n 个子秘密 (d_i, k_i)

Mignotte 序列/d 序列的生成:

要保证任意 $t-1$ 个元素的最大乘积小于 k , 任意 t 个元素的最小乘积大于 k

因此我们根据 k 的二进制位数去生成 n 个大素数, 其中每个大素数的二进制位长都为 $\text{gen_bsize} = k_bsize // (t-1)$, 注意 gen_bsize 用 $//$ 向下取余

因此 M 的位长一定小于 k_bsize , N 的位长 $k_bsize // (t-1) * t$ 一定大于 k_bsize

这种方案的缺陷是秘密长度一定要足够长, 否则可能生成的素数数量不能够满足 n 所需 (gen_bsize 位长的素数是有限的), 所以我们还需要对 n, k 进行检查, 主要是保证 n 要小于能够生成的所有 gen_bsize 位长的素数的数量

例题 基于中国剩余定理的 (t, n) 门限秘密共享方案

3个子密钥 $\{(9, 2), (11, 8), (13, 9)\}$ 中任意选择2个:

$(9, 2), (11, 8)$

建立下列方程组

$$\begin{cases} x \equiv 2 \pmod{9} \\ x \equiv 8 \pmod{11} \end{cases}$$

基于中国剩余定理, 解之得 $x \equiv 74 \pmod{99}$ 。

恢复出秘密 $k = 74$

n 个子秘密 (d_i, k_i) 中任意选择 t 个:

$(k_{i_1}, d_{i_1}), (k_{i_2}, d_{i_2}), \dots, (k_{i_t}, d_{i_t})$

基于中国剩余定理计算下列一次同余方程组

$$\begin{cases} x \equiv k_{i_1} \pmod{d_{i_1}} \\ x \equiv k_{i_2} \pmod{d_{i_2}} \\ \vdots \\ x \equiv k_{i_t} \pmod{d_{i_t}} \end{cases}$$

恢复出秘密 $x \equiv k \pmod{N_1}$, $N_1 = d_{i_1} d_{i_2} \dots d_{i_t}$ 。

秘密恢复

Why: 任意大于等于 t 个 (k, d) 对可解, 任意小于 t 个 (k, d) 对不可解