КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Разбор заданий: материал 10

Математические основы криптографии: решение систем сравнений

Данный материал демонстрирует разбор задания, посвященного решению систем сравнений с помощью китайской теоремы об остатках.

Решение системы сравнений вида

$$\begin{cases} x = a_1 \pmod{n_1}, \\ x = a_2 \pmod{n_2}, \\ \qquad \dots \\ x = a_k \pmod{n_k}, \end{cases}$$

представляет собой восстановление натурального числа по его остаткам для различных модулей $n_1, n_2, \dots, n_k$.

Алгоритм решения этой задачи определяется китайской теоремой об остатках.

Пусть $n_1, n_2, \dots, n_k$ — попарно взаимно простые натуральные числа, $N = \prod_{i=1}^{k} n_i$, $N_i = {}^{N}/_{n_i}$ и целые числа u_i, v_i удовлетворяют равенствам $u_i N_i + v_i n_i = 1 \ \forall\, i = 1, 2, \dots, k$. Тогда единственным решением по модулю N системы сравнений

$$\begin{cases} x = a_1 \pmod{n_1}, \\ x = a_2 \pmod{n_2}, \\ \qquad \dots \\ x = a_k \pmod{n_k}, \end{cases}$$

является следующее число:

$$a = \left(\sum_{i=1}^{k} a_i u_i N_i\right) \bmod N.$$

Пример.

Решить систему сравнений $\begin{cases} x \equiv 2 \pmod{15}, \\ x \equiv 5 \pmod{13}, \\ x \equiv 3 \pmod{7}. \end{cases}$

Решение.

Приведенная теорема полностью определяет порядок вычислений всех величин, необходимых для восстановления натурального числа по его остаткам для произвольного количества попарно взаимно простых модулей.

Сначала необходимо вычислить значения вспомогательных переменных N, N_1, N_2, N_3:

$N = 15 \cdot 13 \cdot 7 = 1365$,

$N_1 = \frac{1365}{15} = 91$, $N_2 = \frac{1365}{13} = 105$, $N_3 = \frac{1365}{7} = 195$.

Последующие вычисления основываются на расширенном алгоритме Евклида, который в данном случае нужно применить трижды.

Соответствующие расчеты сведены в нижеприведенную таблицу.

Данная таблица демонстрирует расчеты с использованием усеченного варианта расширенного алгоритма Евклида, поскольку в каждом случае отсутствует необходимость вычислять оба коэффициента целочисленной линейной комбинации пары чисел, равной их наибольшему общему делителю.

q	r	x	y	N_1	n_1	x_2	x_1
—	—	—	—	91	15	1	0
6	1	1	-6	15	1	0	1
15	0	-15	91	1	0	1	-15
q	r	x	y	N_2	n_2	x_2	x_1
—	—	—	—	105	13	1	0
8	1	1	-8	13	1	0	1
13	0	-13	105	1	0	1	-13
q	r	x	y	N_3	n_3	x_2	x_1
—	—	—	—	195	7	1	0
27	6	1	-27	7	6	0	1
1	1	-1	28	6	1	1	-1
6	0	7	-195	1	0	-1	7

Из таблицы следует, что $u_1 = 1, u_2 = 1, u_3 = -1$.

Теперь можем вычислить искомое значение:

$a = 2 \cdot 1 \cdot 91 + 5 \cdot 1 \cdot 105 + 3 \cdot (-1) \cdot 195 = 122$.

Проверка показывает, что данное значение удовлетворяет всем сравнениям в исходной системе:

$$\begin{cases} 122 \pmod{15} = 2, \\ 122 \pmod{13} = 5, \\ 122 \pmod{7} = 3. \end{cases}$$