КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Разбор заданий: материал 13

Математические основы криптографии: факторизация целых чисел ρ-алгоритмом Полларда

Данный материал демонстрирует разбор задания, посвященного факторизации целых чисел с использованием ρ-алгоритма Полларда.

Задача целочисленной факторизации состоит в том, чтобы для данного натурального числа n найти его разложение на простые множители, то есть получить представление данного числа в виде $n = p_1^{l_1} p_2^{l_2} \dots p_k^{l_3}$, где p_i — попарно различные простые числа, $l_i > 1$ — натуральные числа для $i = 1, \dots, k$.

На задаче целочисленной факторизации основывается стойкость таких известных криптосистем с открытым ключом, как криптосистема RSA и криптосистема Рабина.

Наивный подход к факторизации целого числа n основан на переборе возможных делителей данного числа, удовлетворяющих равенству $1 < p < \lfloor \sqrt{n} \rfloor$. Очевидно, что данный подход является крайне трудоемким для достаточно больших n. Существуют алгоритмы, отличающиеся гораздо большей эффективность, однако даже их наличие не делает задачу факторизации легкой. Тем не менее знание таких алгоритмов необходимо для понимания того, каким образом следует выбирать параметры криптосистем с открытым ключом.

ρ-алгоритм Полларда является алгоритмом специального назначения для нахождения малых множителей составного числа.

Вход: составное число n, не являющееся степенью простого числа.

Выход: нетривиальный множитель d числа n.

Шаг 1. Присвоить $a \leftarrow 2$, $b \leftarrow 2$.

Шаг 2. Для $i = 1, 2, \dots$ выполнить следующее:

Шаг 2.1. Вычислить:

$$a \leftarrow (a^2 + 1) \bmod n,$$
$$b \leftarrow (b^2 + 1) \bmod n,$$
$$b \leftarrow (b^2 + 1) \bmod n.$$

Шаг 2.2. Вычислить $d = \text{НОД}(a - b, n)$ с помощью алгоритма Евклида.

Шаг 2.3. Если $1 < d < n$, то возврат (d);

Шаг 2.4. Если $d = n$, то возврат («неудача»).

Пример.

Выполнить целочисленную факторизацию числа 5531563 посредством ρ-алгоритма Полларда.

Решение.

Поскольку данный алгоритм носит итерационный характер, то все расчеты удобно свести в таблицу.

Первая строка данной таблицы содержит начальные значения a и b. Все последующие строки — обновленные значения a и b, полученные на шаге 2.1, и значение d, вычисленное на шаге 2.2.

i	a	b	d
—	2	2	—
1	5	26	1
2	26	458330	1
3	677	4072967	1
4	458330	1083392	1
5	5283976	4699821	43

На пятой итерации ρ-алгоритм Полларда нашел делитель числа 5531563, равный 43. Чтобы продолжить факторизацию числа n, необходимо вычислить число $n' = {}^{n}/_{d}$ и подать его на вход ρ-алгоритма Полларда.

$n' = {}^{5531563}/_{43} = 128641.$

i	a	b	d
—	2	2	—
1	5	26	1
2	26	72407	1
3	677	85096	1
4	72407	54264	1
5	9695	68745	1
6	85096	71797	1
7	127327	100856	1
8	54264	1271	197

Следующий нетривиальный делитель удалось найти на восьмой итерации. Очевидно, что это существенно быстрее полного перебора потенциальных делителей.

Вычислив $n' = {}^{128641}/_{197} = 653$, получим простое число. Следовательно, задача факторизации решена, и данное составное число имеет следующее разложение на простые множители:

$5531563 = 43 \cdot 197 \cdot 653.$