КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Разбор заданий: материал 14

Математические основы криптографии: факторизация целых чисел p – 1-алгоритмом Полларда

Данный материал демонстрирует разбор задания, посвященного факторизации целых чисел с использованием p – 1-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.

p – 1-алгоритм Полларда, как и ρ-алгоритм Полларда, является алгоритмом специального назначения. Он служит для нахождения всех простых множителей p составного числа n, таких, что $p - 1$ является B-гладким числом по отношению к некоторой относительно малой границе B.

Здесь число $p - 1$ называется B-гладким, если все его простые множители $\leq B$.

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

Выход: нетривиальный множитель d числа n.

Шаг 1. Выбрать границу гладкости B.

Шаг 2. Выбрать случайное целое число a, такое, что $2 \leq a \leq n - 1$, и вычислить $d = \text{НОД}(a, n)$. Если $d \geq 2$, то возврат (d).

Шаг 3. Для всех простых чисел $q \leq B$ выполнить следующее:

Шаг 3.1. Вычислить $l = \left\lfloor \frac{\ln n}{\ln q} \right\rfloor$.

Шаг 3.2. Вычислить $a \leftarrow a^{q^l} \bmod n$.

Шаг 4. Вычислить $d = \text{НОД}(a - 1, n)$.

Шаг 5. Если $d = 1$ или $d = n$, то алгоритм заканчивается неудачей. В противном случае возврат (d).

Пример.

Выполнить целочисленную факторизацию числа 19048567 посредством p – 1-алгоритма Полларда.

Решение.

Последовательно выполним шаги данного алгоритма.

Шаг 1. Пусть граница гладкости $B = 19$.

Шаг 2. Пусть случайное целое число $a = 3$, тогда $d = \text{НОД}(3, 19048567) = 1$.

Шаг 3. Последовательно обойдем все простые числа, не превышающие 19, и сведем расчеты, проделываемые на шагах 3.1 и 3.2 в одну таблицу.

q	l	a
2	24	2293244
3	25	13555889
5	10	16937223
7	8	15214586
11	6	9685355
13	6	13271154
17	5	11406961
19	5	554506

Шаг 4. Вычислим $d = \text{НОД}(554506 - 1, 19048567) = 5281$.

Шаг 5. Возврат (5281).

В результате получим $19048567 = 5281 \cdot 3607$.