Тест Миллера-Рабина

Ильинский

29 января 2020 г. — 29 января 2020 г.

В чём смысл

Можно сделать такой алгоритм шифрования. Пусть p — большое простое число, g — первообразный корень по его модулю. Алиса загадывает a и передаёт g^a, а Боб b и передаёт g^b. Тогда они оба знают число g^{ab} и могут делать по его модулю разные вещи, а сторонний наблюдатель, зная g^a и g^b, не может нормально узнать g^{ab} (по крайней мере, не сейчас).

На самом деле p не обязано быть простым — просто надо, чтобы был какой-то g, что его степени дают много разных остатков, т.е. что у него большой порядок. Например, если $m = pq$, оно скорее всего подойдёт.

Определение 1. Система вычетов Z_m — множество всех остатков по модулю m.

Определение 2. Приведённая система вычетов Z_m^* — множество остатков по модулю m, взаимно простых с ним.

Теорема 1 (Эйлер). $\forall x \in Z_m^* : x^{\phi(m)} = 1$.

Определение 3. Порядок элемента x — минимальное такое k, что $x^k = 1$. Например, порядок первообразного по модулю m равен $\phi(m)$.

Теорема 2. Максимальный порядок по модулю $m = pq$ равен $[p-1; q-1]$.

Лемма 3 (Китайская теорема об остатках). Пусть есть модули $m_1, \ldots, m_n$, которые попарно взаимно просты. Тогда для любых $a_1 \in \mathbb{Z}_{m_1}, a_2 \in \mathbb{Z}_{m_2}, \ldots$ существует единственное решение $x \in Z_{m_1 m_2 \ldots m_n}$ такой системы: $\forall i : x \equiv a_i (\mathrm{mod}\ x_i)$.

Доказательство теоремы 2. Пусть g_1 — первообразный корень по модулю p, а g_2 — первообразный корень по модулю q. Рассмотрим $x : x \equiv g_1(p), x \equiv g_2(q)$. Тогда очевидно, что $ord(x) = [p-1; q-1]$. ■

Как искать большие простые числа

Определение 4. Число Кармайкла — непростое m такое, что для всех a выполнено $a^{m-1} \equiv 1 \mod m$.

Тест Ферма

Выберем m, для которого мы проверяем простоту. Будем брать разные числа a и проверять, что $a^m \equiv a$. К сожалению, тест работает не идеально: существуют числа Кармайкла. Но во-первых, чисел Кармайкла мало, во-вторых, по их модулю существуют числа с большим порядком. С другой стороны, у него довольно большая точность.

Теорема 4. Пусть m составное и не число Кармайкла. Тогда хотя бы половина остатков по модулю m не проходят тест Ферма.[1]

Доказательство. Пусть b не проходит тест, а C — множество тех чисел, которые проходят. Тогда каждое число вида bc_i не проходит тест, значит, «плохих» не меньше, чем «хороших». ■

Теорема 5. Составное m — число Кармайкла тогда и только тогда, когда оно свободно от квадратов для каждого $p \mid m$ верно $p - 1 \mid m - 1$.

Доказательство. Пусть свойство выполняется. Докажем, что $\forall a \in Z_m^*$ выполняется $a^{m-1} \equiv 1 \mod m$. Для каждого p_i оно выполняется, поскольку $p_i - 1 \mid m - 1$ и по малой теореме Ферма.

Теперь предположим, что m — число Кармайкла и что $p^2 \mod m$. Тогда пусть $m = p^k \cdot d, k \geq 2, p \nmid d$. Пусть $a \equiv 1 + p \mod p^k$ и $a \equiv 1 \mod d$. Найдём a^{m-1}:

$$a^{m-1} = (1+p)^{m-1} = 1 + (m-1)p + Mp^2 = 1 - p \mod p^2.$$

Противоречие.

Наконец, докажем, что $p-1 \mid m-1$. Это так, потому что можно взять первообразный корень по модулю каждого простого делителя m. ■

[1] На самом деле, можно доказать, что если C — множество хороших остатков, то $C \mid m - 1$.

Тест Соловея-Штрассена

Заметим, что если m — простое, то

$$a^{\frac{m-1}{2}} = \binom{a}{m},$$

т.е. символу Лежандра a по модулю m. Оказывается, для составных чисел можно обобщить символ Лежандра (получится символ Якоби). Алгоритм делает следующее. Он берёт большое нечётное число m и случайное число a и проверяет факт выше (для символа Якоби). Скорость такая же, но алгоритм игнорирует числа Кармайкла.

Тест Миллера-Рабина

Пусть $p - 1 = 2^s \cdot d$, где d нечётное. Тогда для любого a выполнено либо $a^{2^{s-1}d} = -1$, либо $a^{2^{s-2}d} = -1$, либо $\ldots$, либо $a^d = \pm 1$.

Теорема 6 (Миллер, Рабин). Если m составное, то вероятность того, что для a выполнено хотя бы одно из сравнений выше, не больше $\frac{1}{4}$.