УДК 512.624.95:378.147.091.3

О проблеме дискретного логарифма в криптосистеме Эль Гамаля. Трёхразрядный gigant step

Крупенкова Т.Г., Липницкий В.А.
Белорусский национальный технический университет,
Военная академия Республики Беларусь

Криптографическая стойкость системы базируется на проблеме дискретного логарифма: решении уравнения $g^x = \overline{h}$ в кольце Z / pZ с простым p на сегодняшний день осуществляется единственным способом – последовательным перебором степеней $\overline{g}$ до получения требуемого класса вычетов $\overline{h}$. Проблема и состоит в нахождении иного, не переборного метода определения степени x в данном уравнении.

Д. Шенкс предложил новый метод дискретного логарифмирования – под названием – алгоритм «шаг ребёнка – шаг гиганта». Он заключается в поиске пары целых чисел $Q, r,$ удовлетворяющих условиям $0 \le r < d,$ $0 \le Q < d$ и соотношению $h \cdot (g^{-d})^Q \equiv g^r (\mathrm{mod}\, P)$, где d – наименьшее натуральное число, такое, что $\sqrt{\gamma} \le d$, а γ – показатель элемента g по модулю P, $x = d \cdot Q + r$.

Авторы предлагают трёхразрядный вариант «шага гиганта». Пусть d – наименьшее натуральное число, такое, что $\sqrt[3]{\gamma} \le d$, тогда $x = a \cdot d^2 + b \cdot d + c$ для некоторых целых a, b и c таких, что $0 \le a < d,$ $0 \le b < d,$ и $0 \le c < d$. Эти неизвестные удовлетворяют сравнению

$$h \cdot (g^{-d^2})^a \equiv g^{db+c} (\mathrm{mod}\, P).$$

Первый этап – “baby-step” – состоит в составлении таблицы степеней $h \cdot (g^{-d^2})^i (\mathrm{mod}\, P)$, $0 \le i < d.$ Второй этап – “giant-step” – состоит в последовательном вычислении величин $g^{d \cdot j + k} (\mathrm{mod}\, P),$ $0 \le j < d,$ $0 \le k < d,$ и в сравнении их с данными таблицы. Если на каком-то шаге найдутся a_0, b_0, c_0 удовлетворяющие сравнению $h(g^{-d^2})^{a_0} \equiv g^{db_0 + c_0} (\mathrm{mod}\, P)$, то тогда однозначно опрелеляем искомое $x = a_0 \cdot d^2 + b_0 \cdot d + c_0$.

Для вычисления дискретного логарифма новый алгоритм значительно сокращает количество вычислений в поле Z / PZ.