УДК 512.624.95:378.147.091.3

Алгоритмические аспекты криптосистемы Рабина

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

Данная криптосистема является результатом переосмысления криптосистемы RSA. Рабин М. заинтересовался вопросом выбора ключа e в криптосистеме RSA. Там e всегда взаимно просто с $\varphi(n)$ и, в частности, всегда нечётно. А что произойдёт, если взять чётным? Да, а если возьмём наипростейший случай $e=2$? В результате подробного рассмотрения неожиданно и появилась рассматриваемая здесь криптосистема Рабина.

Пусть p и q – два различных простых числа. Пусть $N = pq$. Зафиксируем число B, $0 \le B < N$. Пара $\{N, B\}$ есть пара открытых ключей криптосистемы Рабина. Сообщение C рассматривается как элемент кольца Z/NZ и шифруется формулой: $m = c(c+B)(\mathrm{mod}\, N)$. Расшифровка здесь представляет гораздо более сложную процедуру даже для законного получателя криптотекста. Фактически, сообщение C есть один из корней квадратного уравнения $x^2 + Bx - m = 0$ в кольце Z/NZ. В этом кольце 2, очевидно, является обратимым элементом. Поэтому для решения данного квадратного уравнения вполне пригодны стандартные формулы: $x = (\sqrt{\frac{B^2}{4} + m} - \frac{B}{2})(\mathrm{mod}\, N)$. Разумеется, деление на 2 здесь реализуется умножением на $2^{-1} \in (Z/NZ)^*$. Сложность этих вычислений в том, что из каждого квадрата в данном кольце Z/NZ извлекаются 4 различных корня. И лишь один – верный. Как на него указать адресату – дополнительная проблема.

Другая проблема – как найти быстро квадратные корни из данного элемента кольца Z/NZ – в общем случае остаётся открытой. Существенно облегчает её решение знание делителей числа N. Тогда можно воспользоваться китайской теоремой об остатках и формулой Гарнера. Поэтому сложность взлома криптосистемы Рабина такая же, как и криптосистемы RSA.