Дальневосточный математический журнал. 2020. Т. 20. № 2. С. 221–223

УДК 512.624.95
MSC2010 35Q31

© Н. В. Маркова[1]

Новый метод формирования ключей в криптосистеме RSA

В.А. Быковский построил новый вариант криптосистемы RSA, в котором при тех же длинах личных ключей длина открытого ключа уменьшается асимптотически в три раза. В работе предлагается новая конструкция на эту тему, в которой длина открытого ключа уменьшается более чем в три раза.

Ключевые слова: *Теория простых чисел, криптография с открытым ключом, криптосистема RSA.*

DOI: https://doi.org/10.47910/FEMJ202021

В криптосистеме RSA из [1] (см. также [2]) в качестве личного ключа пользователя выбирается пара (p_1, p_2) больших простых чисел, а их произведение $q = p_1 p_2$ – открытый ключ. Из открытых ключей администратор сети формирует общедоступную таблицу. Её размер пропорционален числу пользователей и может достигать значительной величины. В работе [3] была предложена следующая модификация криптосистемы RSA на этапе формирования личных ключей.

Администратор выбирает пару натуральных чисел (Δ, δ) с $2 < \delta < \Delta$. Каждый пользователь формирует личный ключ (p_1, p_2) с простыми p_1 и p_2, для которых

$$\Delta < q = p_1 p_2 < \Delta + \delta.$$

При таком выборе простых чисел можно считать, что $q' = q - \Delta$ – открытый ключ, по которому однозначно определяется личный ключ (p_1, p_2). Поэтому объём таблицы открытых ключей уменьшается асимптотически не менее чем в $\log_2 \Delta / \log_2 \delta$ раз.

В работе [3] был предложен алгоритм построения личных ключей с $\delta = 30\Delta^{1/3}$, опирающийся на теорию непрерывных дробей. Мы улучшаем эту конструкцию в следующем виде.

[1] Хабаровское отделение Института прикладной математики ДВО РАН, 680000, г. Хабаровск, ул. Дзержинского, 54. Электронная почта: nata_mark@mail.ru

Алгоритм.

Фиксируем $\alpha \in (0, 1/6]$ и выбираем случайное натуральное число t, для которого

$$\frac{1}{2}\Delta^{\alpha}\log_2^3\Delta < t < \Delta^{\alpha}\log_2^3\Delta. \tag{1}$$

Положим последовательно

$$m = \left[\sqrt{\Delta}\right] + t, \qquad \Delta' = m^2 - \Delta,$$
$$n = \left[\sqrt{\Delta'}\right], \qquad a = m + n, \qquad b = m - n,$$
$$q = ab = (m+n)(m-n),$$
$$q' = q - \Delta = m^2 - n^2 - \Delta.$$

Из асимптотического закона распределения простых чисел

$$\pi(x) = \sum_{p \leqslant x} 1 = \frac{x}{\log x}\,(1 + o(x))$$

и вероятностных соображений следует, что за $O(\log^2\Delta)$ шагов алгоритма мы найдем t, для которого $(a,b) = (p_1, p_2)$ — пара простых чисел, которые мы выбираем в качестве личного ключа.

Теперь оценим величину q'. Заметим, что

$$0 < m^2 - \Delta = \left(\left[\sqrt{\Delta}\right] + t\right)^2 - \Delta =$$
$$= \left(\sqrt{\Delta} + t - \theta\right)^2 - \Delta = 2\sqrt{\Delta}(t-\theta) + (t+\theta)^2,$$

где $0 \leqslant \theta < 1$. Поэтому

$$\Delta' = m^2 - \Delta < 2\Delta^{\alpha+1/2}\log_2^3\Delta + \Delta^{2\alpha}\log_2^6\Delta < 4\Delta^{\alpha+1/2}\log_2^6\Delta.$$

И, наконец,

$$0 < q' = \Delta' - n^2 = \Delta' - \left(\left[\sqrt{\Delta'}\right]\right)^2 < \Delta' - \left(\sqrt{\Delta'} - 1\right)^2 =$$
$$= 2\sqrt{\Delta'} - 1 < 4\Delta^{\alpha/2+1/4}\log_2^3\Delta.$$

Поэтому асимптотический размер таблицы открытых ключей уменьшится не менее, чем в

$$(\alpha/2 + 1/4)^{-1} = \frac{4}{2\alpha + 1} \tag{2}$$

раза. Устремляя α к нулю, для правой части (2) получим выражение $4 + O(\alpha)$ вместо 3 из [3]. Заметим, что в нашем случае правая часть в (2) равна 3 при $\alpha = 1/6$.

Если выбирать простые p_1 и p_2 с

$$\Delta = 2^{2048} < p_1 p_2 < 2^{2049},$$

то при $\alpha = 1/32$

$$\frac{4}{2\alpha+1} = \frac{4}{1+1/16} = \frac{64}{17} = 3 + \frac{13}{17}.$$

Так как $\Delta^{1/32} = 2^{64}$, то при существующих вычислительных мощностях невозможно разложить q на простые множители путём перебора t в пределах (см. (1))

$$2^{95} < t < 2^{96}.$$

Автор благодарит Быковского В. А. за постановку задачи.

Список литературы

[1] R. L. Rivest, A. Shamir, L. Adleman, "Method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Commun. ACM*, **21**:2, (1978), 120–126 doi https://doi.org/10.1145/359340.359342.

[2] О. Н. Василенко, *Теоретико-числовые алгоритмы в криптографии*, МЦНМО, М., 2003, 328 с.

[3] В. А. Быковский., *Вычисление случайных пар простых чисел, произведение которых лежит в заданном коротком интервале*, Препринт ИПМ ДВО РАН, Дальнаука, Владивосток, Хабаровск, 1994, 7 с.

Поступила в редакцию
23 октября 2020 г.

Markova N. V. A new method for generating keys in the RSA cryptosystem. *Far Eastern Mathematical Journal.* 2020. V. 20. No 2. P. 221–223.

ABSTRACT

V.A. Bykovsky built a new version of the RSA cryptosystem, in which for the same private key lengths the length of the public key decreases asymptotically by a factor of three. The paper proposes a new construction on this theme, in which the length of the public key is reduced by more than three times.

Key words: *Number theory, cryptography, RSA cryptosystem.*