также активном мониторинге сетей на присутствие «подозрительных» гармоник в их спектрах.

Литература

1. Kuhn M.G., Anderson R.J. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations, in David Aucsmith (Ed.): Information Hiding, Second International Workshop, IH'98, Portland, Oregon, USA, April 15-17, 1998, Proceedings, LNCS 1525, Springer-Verlag, pp 124-142.

2. «Информационная безопасность офиса». Научно-практический сборник Выпуск первый «Технические средства защиты информации».– К.: ООО «ТИД «ДС», 2003.– 216 с.

ДИСКРЕТНОЕ ЛОГАРИФМИРОВАНИЕ НА МУЛЬТИПЛИКАТИВНОЙ ГРУППЕ ДЛЯ ДВУХСОСТАВНОГО МОДУЛЯ RSA

В.Н.Сюрин, И.Л.Гаврилова, Д.В.Шилко
Беларусь, г. Гродно

Хорошо известно, что дискретное логарифмирование на мультипликативной группе относится к числу NP-полных проблем, которые решаются путем перебора. По-нашему мнению, можно получить некоторые аналитические результаты в этой области, если учитывать специфику решаемой задачи.

Рассмотрим данные особенности на мультипликативной группе G_2 для двухсоставного модуля криптосистемы RSA $N = pq$, где p и q - большие простые числа.

Очевидно, что на группе G_2 в данном случае [1]

$$2^N = 2^{(p-1)(q-1)} \times 2^{p+q-1}, \bmod N = 2^{p+q-1}, \bmod N. \qquad (1)$$

Вычисление (1) снижает порядок исследуемого пространства элементов группы, а также при вычислении логарифма правой его части дает возможность определения p и q путем решения системы уравнений

$$\begin{aligned} p \times q &= N; \\ p + q &= a, \end{aligned} \qquad (2)$$

где $a = \log_2 2^{p+q-1} + 1$, то есть произвести вскрытие криптосистемы RSA.

Логарифм правой части (1) может быть вычислен путем последовательного умножения на элемент, обратный элементу 2^1 и сравнения на каждом шаге с системой заранее вычисленных остатков $2^i, \bmod N$. Для удобства ограничим эту систему значениями $2^0, 2^1, \ldots, 2^i < N$, тогда сравнение с каждым остатком на

каждом шаге домножения на 2^{-i} можно заменить на ассемблерную операцию CE -счет единиц, что существенно снизит объем вычислений. Если операция CE в конце концов даст 1, то далее определяется номер единичного разряда, процесс домножения заканчивается и логарифм определяется как

$$a = i \times n_c + {}^{1}{}_{\delta} + 1, \tag{3}$$

где n_c - число циклов домножения;

$^{1}{}_{\delta}$ - номер единичного разряда в последнем домножении.

В случае если подобным образом вычисляется параметр $x = (p-1)(q-1)$, при правильном выборе параметров RSA вычислительная сложность определяется как

$$O(n) \sim N/n, \tag{4}$$

где $n = \log_1 N$;

$\sim r$ - означает одного порядка с r.

Рассмотренный алгоритм дает сложность

$$O(n) \sim (p+q)/n. \tag{5}$$

Сравнение (4) и (5) наглядно показывает выигрыш в вычислительной сложности для (5), который к тому же быстро возрастает с ростом N. Эффективным считается алгоритм вскрытия RSA с вычислительной сложностью [2]

$$O(n) = n^5. \tag{6}$$

Совместное решение (5) и (6) показывает, что рассмотренный алгоритм эффективен до $n = 64$.

Таким образом, данная процедура логарифмирования с последующим вскрытием RSA занимает промежуточное значение между описанными в [1] и [3].

Литература

1. Сюрин В.Н., Гаврилова И.Л. Конструктивная процедура вскрытия криптосистемы RSA. - Инженерный Вестник, 2005, №1(20). - С. 60 - 62.

2. Dan Boneh. Twenty Year of Attacks on the RSA Cryptosistem. - Notices of the AMS, 1999, vol.46, #2. - P. 203 - 213.

3. Сюрин В.Н., Гаврилова И.Л., Шилко Д.В. Безусловный алгоритм вскрытия криптосистемы RSA. – Современные средства связи: Материалы XI Международной научно-технической конф., 25-29 сентября 2006 года, Нарочь, РБ, - Минск, 2006. – С.98.