

ИСПОЛЬЗОВАНИЕ СИСТЕМЫ СЧИСЛЕНИЙ В ОСТАТОЧНЫХ КЛАССАХ ДЛЯ КРИПТОАНАЛИЗА АЛГОРИТМА RSA

к.т.н. В.Н. Федорченко, к.т.н., проф. Л.С. Сорока, А.А. Смирнов
(представил д.т.н., проф. Ю.В. Стасев)

В статье рассмотрен метод факторизации двухсоставного модуля криптоалгоритма RSA, основанный на использовании представлений чисел в системе остаточных классов.

В настоящее время в качестве алгоритма криптографической защиты и аутентификации информации широко используется алгоритм RSA [1]. Алгоритм RSA является блочным. В нём сообщение \mathbf{M} , которое шифруется, разбивается на блоки \mathbf{M}_i , с длиной блока $l_j \geq l_g$ (512 бит минимум, реально 1024, 2048 бит). Операция шифрования выполняется по правилу

$$\mathbf{C}_i = \mathbf{M}_i^{\mathbf{E}_K} \pmod{\mathbf{N}}, \quad (1)$$

где \mathbf{E}_K – ключ прямого преобразования, а \mathbf{N} – модуль шифрования, причем

$$\mathbf{N} = \mathbf{P} * \mathbf{Q}, \quad (2)$$

где \mathbf{P} , \mathbf{Q} – большие простые числа.

Дешифрование производится по правилу

$$\mathbf{M}_i = \mathbf{C}_i^{\mathbf{D}_K} \pmod{\mathbf{N}}, \quad (3)$$

где \mathbf{D}_K – ключ обратного преобразования.

Подставив (1) в (3), получим

$$\mathbf{M}_i^1 = \mathbf{M}_i^{\mathbf{E}_K \mathbf{D}_K} \pmod{\mathbf{N}}. \quad (4)$$

Наиболее предпочтительным методом криптоанализа данного алгоритма является решение задачи факторизации модуля \mathbf{N} , причём размерность факторизируемого числа должна быть порядка 512 – 1024 бит [1].

Предлагается для факторизации такого модуля использовать свойства чисел, представленных в модулярной системе счисления по основаниям \mathbf{P} и \mathbf{Q} .

Известно [2], что любое число \mathbf{X} в диапазоне от $\mathbf{0}$ до \mathbf{N} можно представить в модулярной системе счисления по модулям с основаниями \mathbf{P} и \mathbf{Q} :

$$\mathbf{X}_P = \mathbf{X} \pmod{\mathbf{P}}; \quad (5)$$

$$\mathbf{X}_Q = \mathbf{X} \pmod{\mathbf{Q}}, \quad (6)$$

причём для перевода чисел \mathbf{X} из модулярной системы счисления в позиционную систему счисления необходимо знание базисных чисел \mathbf{B}_1 и \mathbf{B}_2 :

$$\mathbf{B}_1 = \left[Q^{P-2} \pmod{P} \right] \cdot Q ; \quad (7)$$

$$\mathbf{B}_2 = \left[P^{Q-2} \pmod{Q} \right] \cdot P . \quad (8)$$

Тогда обратное преобразование будет иметь вид

$$\mathbf{X}_P \cdot \mathbf{B}_1 + \mathbf{X}_Q \cdot \mathbf{B}_2 = \mathbf{X} \pmod{N} . \quad (9)$$

Исходя из соотношений (7), (8) можно показать, что базисные числа обладают следующими свойствами:

$$\mathbf{B}_1 = \mathbf{0} \pmod{Q} ; \quad (10)$$

$$\mathbf{B}_2 = \mathbf{0} \pmod{P} ; \quad (11)$$

$$\mathbf{B}_1 + \mathbf{B}_2 = N + 1 ; \quad (12)$$

$$\mathbf{B}_1 + \mathbf{B}_2 = \mathbf{0} \pmod{N} = k \cdot N . \quad (13)$$

Таким образом, исходя из соотношений (10) и (11), нахождение одного из базисных чисел позволяет, применяя алгоритм Эвклида вычисления НОД, найти какое-либо из составляющих модуля N (P или Q):

$$(\mathbf{B}_1, N) = P ; \quad (14)$$

$$(\mathbf{B}_2, N) = Q . \quad (15)$$

Кроме того, анализ (12) показывает, что базисные числа равноудалены от середины отрезка $[0, N + 1]$, т. е.:

$$\frac{N+1}{2} - Z = \mathbf{B}_1 ; \quad (16)$$

$$\frac{N+1}{2} + Z = \mathbf{B}_2 . \quad (17)$$

Это позволяет систему уравнений (12) - (13) привести к виду

$$\frac{(N+1)^2}{4N} - \frac{Z^2}{N} = k . \quad (18)$$

Для нахождения базисных чисел предлагается рассмотреть систему уравнений (12) – (13), анализ которой показывает, что в системе из двух уравнений существуют три неизвестных параметра $\mathbf{B}_1, \mathbf{B}_2, k$.

Первым способом для нахождения базисных чисел (решения системы уравнений), является проведение ряда итераций для различных k . Диапазон изменения k будет определять вычислительную сложность данного способа.

Используя (18) и учитывая, что исходя из (7) – (8)

$$\mathbf{B}_{\min} = \min (\mathbf{B}_1, \mathbf{B}_2) > \max (P, Q), \quad (19)$$

получим следующее соотношение для оценки изменения диапазона k :

$$\sqrt{N} - 1 < k < \frac{(N+1)^2}{N} . \quad (20)$$

Учитывая, что при реальных значениях N диапазон изменения k до-

статочно велик, для более конкретного определения значения k можно в систему уравнений (12) – (13) добавить соотношение

$$B_1/B_2 \sim k \quad (21)$$

при $B_1 > B_2$.

Анализ данного способа взлома RSA алгоритма позволяет сделать предварительный вывод, что при $Z \leq t\sqrt{N}$, либо $Z \geq \frac{N+1}{2} - \sqrt{N(t+1)}$,

где $t \leq 10^5 \cdot 10^6$, взлом алгоритма может быть успешным и без использования соотношения (21) (путём перебора k). Таким образом, выбор модуля RSA алгоритма, при котором соответствующие базисные числа "располагаются" близко к концам отрезка $[\max(P, Q), (N+1)/2]$ может привести к успешному решению задачи факторизации с минимальными вычислительными затратами.

Второй способ факторизации N основан на преобразовании выражения (18) к виду:

$$Z^2 \equiv A \pmod{N}, \quad (22)$$

где $A = (N+1)^2/4$.

Следовательно, приходим к классическому квадратичному уравнению, имеющему решение [3].

Зная Z , из соотношения (22) можно определить базисные числа (16), (17) и, используя алгоритм Эвклида, найти составляющие модуля, т.е. решить задачу факторизации.

ЛИТЕРАТУРА

1. Чмора А. Современная прикладная криптография. – М.: Гелиос АРВ, 2001. – 244 с.
2. Коляда А.А., Пак И.Т. Модулярные структуры конвейерной обработки информации. – Мн.: Университетское, 1992. – 256 с.
3. X9.63-1998, *Public Key Cryptography For The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography*.

Поступила 18.06.2002

ФЕДОРЧЕНКО Владимир Николаевич, кандидат технических наук, старший преподаватель кафедры ХВУ. Окончил ХВВКИУ в 1989 году. Область научных интересов – защита информации в автоматизированных системах управления и сетях.

СОРОКА Леонид Степанович, канд. техн. наук, профессор. Окончил ХВВКУ в 1974 году. Область научных интересов – методы и средства обработки информации.

СМИРНОВ Алексей Анатольевич, адъюнкт ХВУ. В 1999 году окончил ХВУ. Область научных интересов – защита информации в автоматизированных системах управления и сетях.