УДК 621.327

# 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 блоковым. В нём сообщение **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

$$\mathbf{C_i = M_i^{E_K} (mod\ N)}, \tag{1}$$

где $\mathbf{E_K}$ – ключ прямого преобразования, а **N** – модуль шифрования, причем

$$\mathbf{N = P * Q}, \tag{2}$$

где **P**, **Q** – большие простые числа.

Дешифрование производится по правилу

$$\mathbf{M_i = C_i^{Д_K} (mod\ N)}, \tag{3}$$

где $\mathbf{Д_K}$ – ключ обратного преобразования.

Подставив (1) в (3), получим

$$\mathbf{M_i^1 = M_i^{E_K Д_K} (mod\ N)}. \tag{4}$$

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

Предлагается для факторизации такого модуля использовать свойства чисел, представленных в модулярной системе счислений по основаниям **P** и **Q**.

Известно [2], что любое число **X** в диапазоне от **0** до **N** можно представить в модулярной системе счислений по модулям с основаниями **P** и **Q**:

$$\mathbf{X_P = X(mod\ P)}; \tag{5}$$

$$\mathbf{X_Q = X(mod\ Q)}, \tag{6}$$

причём для перевода чисел **X** из модулярной системы счисления в позиционную систему счисления необходимо знание базисных чисел $\mathbf{B_1}$ и $\mathbf{B_2}$:

$$\mathbf{B_1 = \left[ Q^{P-2} (mod\ P) \right] \cdot Q}; \quad (7)$$

$$\mathbf{B_2 = \left[ P^{Q-2} (mod\ Q) \right] \cdot P}. \quad (8)$$

Тогда обратное преобразование будет иметь вид

$$\mathbf{X_P \cdot B_1 + X_Q \cdot B_2 = X (mod\ N)}. \quad (9)$$

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

$$\mathbf{B_1 = 0\ (mod\ Q)}; \quad (10)$$

$$\mathbf{B_2 = 0\ (mod\ P)}; \quad (11)$$

$$\mathbf{B_1 + B_2 = N + 1}; \quad (12)$$

$$\mathbf{B_1 + B_2 = 0\ (mod\ N) = k \cdot N}. \quad (13)$$

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.:

$$\mathbf{\frac{N+1}{2} - Z = B_1}; \quad (16)$$

$$\mathbf{\frac{N+1}{2} + Z = B_2}. \quad (17)$$

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

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

Для нахождения базисных чисел предлагается рассмотреть систему уравнений (12) – (13), анализ которой показывает, что в системе из двух уравнений существуют три неизвестных параметра $\mathbf{B_1, B_2, k}$.

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)

$$\mathbf{B_{min} = min\ (B_1, B_2) > max\ (P, Q)}, \quad (19)$$

получим следующее соотношение для оценки изменения диапазона **k**:

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

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

$$\mathbf{B_1/B_2 \sim k} \qquad (21)$$

при $\mathbf{B_1 > B_2}$.

Анализ данного способа взлома RSA алгоритма позволяет сделать предварительный вывод, что при $\mathbf{Z \le t\sqrt{N}}$, либо $\mathbf{Z \ge \frac{N+1}{2} - \sqrt{N(t+1)}}$, где $\mathbf{t \le 10^5..10^6}$, 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 $\left[\mathbf{max(P,Q)},\ \left(\mathbf{N+1}\right)/\mathbf{2}\right]$ может привести к успешному решению задачи факторизации с минимальными вычислительными затратами.

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

$$\mathbf{Z^2 \equiv A(mod\ N)}, \qquad (22)$$

где $\mathbf{A = (N+1)^2/4}$.

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 конвеерной 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.*