УДК 681.142.35

М.П. КАРПІНСЬКИЙ, д-р техн. наук, Я.І. КІНАХ

ВИКОРИСТАННЯ МЕТОДІВ ФАКТОРИЗАЦІЇ ДЛЯ ОЦІНКИ НАДІЙНОСТІ СИСТЕМИ ШИФРУВАННЯ RSA

Бурхливий розвиток комп'ютеризації всіх сфер життя надає нові можливості для національних економік. Поширення інформаційних технологій має і свій негативний аспект: це відкриває шлях до антисоціальної і злочинної поведінок. Крім того, що комп'ютерні злочини наносять значні економічні збитки, суспільство стає все залежнішим від роботи комп'ютеризованих систем у різноманітних сферах життя — від керування рухом літаків і поїздів до медичного обслуговування та національної безпеки. Будь-який збій у функціонуванні таких систем може привести до реальної загрози життю людей. Стрімке зростання глобальних комп'ютерних мереж, а також можливість під'єднання до них через звичайні телефонні лінії посилюють можливості їх використання для несанкціонованого доступу.

У порівнянні з високорозвиненими країнами інформаційна безпека України поки що залежить від комп'ютерних мереж значно менше. На сьогодні в нашій державі основна маса несанкціонованих доступів спостерігається у фінансово-кредитній сфері. Але у недалекому майбутньому такі несанкціоновані доступи можуть викликати глобальні катастрофи. Введення сучасної системи управління повітряним рухом, поширення телекомунікаційної мережі, впровадження системи електронних платежів, використання комп'ютерів у діяльності правоохоронних органів та керуванні військами значно збільшили інтерес до несанкціонованого доступу серед користувачів і програмістів [1].

Система шифрування інформації RSA на сьогодні стала де-факто світовим стандартом, що реалізується в якості самостійних програмних продуктів і у складі продуктів прикладного програмного забезпечення. Систему RSA використовують у світових банківських мережах, зокрема для роботи з кредитними картками. Вона зустрічається в таких стандартах: SSL, S-HHTP, S-MIME, S/WAN, STT і PCT.

Система RSA належить до асиметричних криптографічних систем. Їх суть полягає в тому, що кожний користувач генерує два ключі, які пов'язані деяким співвідношенням. Один ключ функціонує відкрито, інший є таємним. Текст шифрується відкритим ключем адресата. Процес дешифрування можна здійснити тоді і тільки тоді, якщо відомий таємний ключ. Дану систему можна використовувати як самостійний засіб захисту, так і при розподілі ключів, а також як засіб аутентифікації.

Перед шифруванням текст кодують у зручну для роботи систему числення. Закодований текст розбивають на блоки $B_i \in Z_n$ і перетворюють блоки згідно з правилом:

$$E(B_i) = B_i^e \pmod n, \tag{1}$$

де e – відкритий ключ, такий що $e < \phi(n)$, $(e, \phi(n)) = 1$ - найбільший спільний дільник, $\phi(n)$ – функція Ейлера, n – модуль перетворення, що є добутком двох, бажано «сильних», простих чисел p і q достатньо великої розрядності (p і q не розголошуються).

В результаті отримаємо криптотекст, що також формується з блоків $P_i = E(B_i)$. Очевидно, що $P_i \in Z_n$. Процес дешифрування відбувається за правилом:

$$D(P_i) = P_i^d \pmod n. \tag{2}$$

Тут d – таємний ключ, що пов'язаний з відкритим ключем таким співвідношенням:

$$ed \equiv 1 (\mathrm{mod}\, \phi(n)). \tag{3}$$

Під час практичної роботи з криптотекстами виникає задача дешифрування, коли таємний ключ d є невідомим. Оскільки таємний і відкритий ключі пов'язані відомим співвідношенням, то обчисливши

значення функції $\phi(n)$, можна взнати таємний ключ за відкритим. Відомо, що $\phi(n) = (p - 1)(q - 1)$ і поставлена задача зводиться до обчислення p і q, де $pq = n$. Тоді постає задача факторизації.

Згідно з твердженням 4.4 [2], обчисливши два квадратні корені y та y' з деякого числа x за модулем n, можна твердити: найбільший спільний дільник $(y + y', n)$ є одним з дільників p або q числа n, за умови, що

$$y \neq \pm y' (\mathrm{mod}\, n). \tag{4}$$

Таким чином, поставлена задача зводиться до розв'язання конгруенції $y^2 = (y')^2 (\mathrm{mod}\, n)$. Серед ефективних методів розв'язку останньої конгруенції заслуговують на увагу метод квадратичного решета і метод решета числового поля. Останній метод вважається найперспективнішим на сьогоднішній день. Розглянемо його детальніше.

Подамо число n у формі

$$n = r^e - s, \tag{5}$$

де $r > 0$, $s \neq 0$. При цьому r і $|s|$ є достатньо малими.

Виберемо мінімальні $d \in Z_{>0}$ і $k \in Z_{>0}$, такі, що $kd \geq e$. Звідси випливає, що

$$r^{kd} \equiv s r^{kd-e} (\mathrm{mod}\, n). \tag{6}$$

Нехай $m = r^k$, $c = s r^{kd-e}$. Тоді

$$m^d \equiv c (\mathrm{mod}\, n). \tag{7}$$

Сформуємо многочлен

$$f(x) = x^d - c \in Z[x], \tag{8}$$

де α – корінь многочлена.

Побудуємо гомоморфізм φ такий, що відображає $Z[\alpha]$ в Z / nZ. Метод решета поля дозволяє відшукати пару цілих алгебраїчних чисел a і b, які зустрічаються в співвідношенні

$$\varphi(a + \alpha b) = (a + mb \bmod n). \tag{9}$$

Отримані числа a і b використовують для знаходження розв'язку конгруенції

$$y^2 = (y')^2 (\mathrm{mod}\, n). \tag{10}$$

Під час пошуку можна обмежитися головними ідеалами Z[α] простої норми, бо вони єдині містять алгебраїчні цілі числа форми $a + \alpha b$, де a і b - взаємопрості числа.

Множину головних ідеалів Z[α] простої норми визначають пари чисел p і c_p, де p - просте число і $c_p \in \{0, 1, \ldots, p - 1\}$. Число c_p повинно задовольняти умову $f(c_p) \equiv 0 \bmod p$. Під час пошуку пар можна використовувати головні ідеали норми p, породжені p і $\alpha - c_p$, або еквівалентні головні ідеали Z[α], що перетворюються гомоморфізмом в Z / pZ, і α відображається в c_p. Зокрема, число $a + \alpha b$ знаходиться в головному ідеалі, що відповідає парі чисел p і c_p, якщо тільки $a + c_p b \equiv 0 \bmod p$. Головний ідеал $a + \alpha b$ характеризується нормою $N(a + \alpha b) = a^d - c(-b)^d \in Z$.

Зафіксуємо межу розкладу $B \in R_{>0}$. Значення B визначаємо експериментально. Нехай a і b цілі числа і $b > 1$. Припустимо, що:

$$|N(a + \alpha b)| = \prod_{p \leq B} p^{v_p} \tag{11}$$

$$|a+mb| = \prod_{p \le B} p^{w_p}, \tag{12}$$

де v_p, $w_p \in Z$.

Для продовження процесу факторизації представимо числа $a + \alpha b$ у вигляді:

$$a + \alpha b = (\prod_{u \in U} u^{t_u})(\prod_{g \in G} g^{v_g}), \tag{13}$$

де v_g, $t_u \in Z$. U - множина деяких груп. G - множина головних ідеалів Z[α] простих норм. Звідси випливає:

$$((\prod_{u \in U} \varphi(u)^{t_u})(\prod_{g \in G} \varphi(g)^{v_g}) = \prod p^{w_s} \bmod n. \tag{14}$$

При наявності достатньої кількості пар чисел *a, b* формуємо вирази (15) і (16), обчислюємо значення функції *x(a, b)* за допомогою методу Гауса, додавши вектори за модулем 2 в рівності (14). Одержуємо:

$$\prod_{a,b} (a + \alpha b)^{x(a,b)} = \left((\prod_{d \in U} u^{\overline{v_u}}) \cdot (\prod_{g \in G} g^{\overline{v_g}}) \right)^2, \tag{15}$$

$$\prod_{a,b} (a + mb)^{x(a,b)} = \left(\prod_{p \le B} p^{\overline{w_p}} \right)^2. \tag{16}$$

Прирівнявши праві частини виразів (15) і (16), отримаємо:

$$\left((\prod_{u \in U} \varphi(u)^{\overline{t_u}})(\prod_{g \in G} \varphi(g)^{\overline{v_g}}) \right)^2 = \left((\prod_{p \le B} p^{\overline{w_p}})^2 \bmod n \right). \tag{17}$$

Тут $\overline{t_u}, \overline{v_g}, \overline{w_p} \in Z$. З рівності (17) знаходимо цілі числа y і y', що задовільняють конгруенцію $y^2 = (y')^2 (\bmod n)$.

Одержані результати розв'язку дозволяють достеменно визначити таємний ключ системи RSA.

Час роботи алгоритму що реалізує метод решета числового поля оцінюється виразом $\exp\left((c + o(1))(\ln n)^{1/3}(\ln \ln n)^{2/3}\right)$, c=1,526. Під час факторизації методом решета числового поля числа довжиною в сто десяткових цифр необхідно проаналізувати принаймні 900 ідеалів простої норми. Матриця (14) має розмір порядку 10^5 на 10^5. Для її обробки необхідно виконати кількість арифметичних операцій порядку 10^{13}. Для порівняння наведемо вираз, що дозволяє оцінити час роботи алгоритму квадратичного решета: $\exp\left((1 + o(1))(\ln n)^{1/2}(\ln \ln n)^{1/2}\right)$ [3]. Рисунок 1 дозволяє наочно спостерігати перевагу методу решета числового поля над методом квадратичного решета, бо графічна ілюстрація виразу, що дозволяє оцінити складність методу квадратичного решета - 2, мажорує відповідний вираз для решета числового поля - 1 для будь-якого допустимого n.

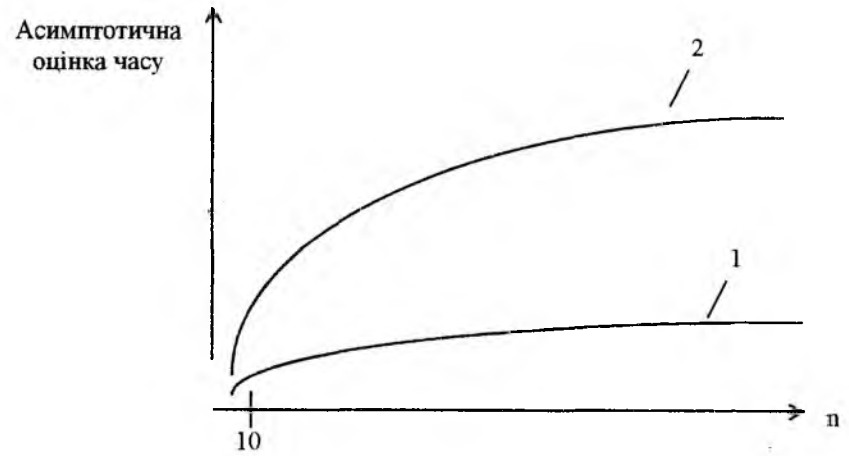

Рис. 1

Список літератури: **1.** *Криміналістика* / П.Д.Біленчук, О.П.Дубовий, М.В.Салтевський П.Ю.Тимошенко / За редакцією П.Д. Біленчука. – К.: АТІКА, 1998. – 416 с. **2.** *Вербіцький О.В.* Вступ д криптології. – Львів: ВНТЛ, 1998. – 247 с. **3.** *Lenstra A.K., Lenstra H.W., Manasse M.S., Pollard J.M.* Th number field sieve. Online access through WWW: http://www.rsasecurity.com/rsalabs/faq/.

Харьковский государственный технический университет радиоэлектроники

Поступила в редколлегию 10.02.2000