УДК 681.142.35

ПЕРЕВАГИ АСИМЕТРИЧНОЇ КРИПТОГРАФІЇ

Андрій Ботюк, Микола Карпінський, Ярослав Кінах
Тернопільська академія народного господарства

Анотація: **Висвітлено концепцію асиметричної криптографії з позиції захисту споживача. Розглянута асиметрична система шифрування RSA. Наведено алгоритм решета числового поля, що дозволяє оцінити рівень надійності системи шифрування RSA.**
Summary: **This article deals with the RSA encryption algorithm. Its safety is analyzed using the number field sieve method. The algorithm work results allow to define a define a secret key in a simple way.**
*Ключові слова: А***симетрична криптографія, алгоритм RSA**

Асиметрична криптографія або системи з відкритим ключем дозволяють зашифрувати повідомлення для конкретного адресата без попереднього обміну ключами, тобто зашифрувати лист, телефонну розмову тощо з незнайомою людиною таким чином, що перехопити ключ до шифру принципово неможливо. 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, коли відомий таємний ключ. Дану систему можна використовувати як самостійний засіб захисту, так і при розподілі ключів, а також як засіб аутентифікації, тобто, асиметрична криптографія дозволяє підтвердити, що повідомлення передане власником конкретного ключа і ніким іншим.

Надійність захисту інформації забезпечується не таємністю алгоритмів, а передусім математичними фактами (алгоритмічною нерозв'язністю визначених математичних задач).

Наприклад, лист, зашифрований за декілька хвилин на дешевому персональному комп'ютері, для "зламу" зажадає багатьох днів, а то і років, роботи самих потужних суперкомп'ютерів, якими володіють державні силові структури.

Заслуговує на увагу асиметрична криптографічна система RSA. Сьогодні алгоритм RSA активно реалізується як в окремих криптографічних продуктах, наприклад, в програмі PGP, так і в якості вмонтованих засобів у популярне прикладне програмне забезпечення, наприклад, в браузерах Інтернет від Microsoft і Netscape. Слід зазначити, що розглянутий в роботі алгоритм шифрування RSA є доступним для будь-кого. Розглянемо його практичну реалізацію.

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). Як p і q можна використовувати ймовірно прості числа, тобто числа для яких імовірність того, що вони прості, наближається до 1. Але у випадку, коли використане складене число, а не просте, криптостійкість RSA зменшується. Існують непогані алгоритми, котрі дозволяють генерувати ймовірно прості числа з ймовірністю 2^{-100}. Легко бачити, що функція E є важкооборотною при вищенаведених умовах.

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:

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

Важливий аспект реалізації RSA - обчислювальний. Адже доводиться використовувати апарат "довгої" арифметики. Якщо використовується ключ довжиною k біт, то для створення відкритого ключа необхідно $O\left(\mathrm{k}^2\right)$ операцій, закритого ключа $O\left(\mathrm{k}^3\right)$ операцій, а для генерації нових ключів потрібно $O\left(\mathrm{k}^4\right)$ операцій.

Криптографічний пакет BSAFE 3.0 (RSA D. S.) на комп'ютері Pentium-90 здійснює шифрування зі швидкістю 21,6 Кбіт/с для 512-бітного ключа і зі швидкістю 7,4 Кбіт/с для 1024 бітного. Найшвидша апаратна реалізація алгоритму RSA забезпечує швидкість в 60 разів більшу.

Під час практичної роботи з криптотекстами виникає задача дешифрування, коли таємний ключ *d* є невідомим. Поставлену задачу можна успішно розв'язати, вказавши спосіб визначення таємного ключа за відкритим. Оскільки таємний і відкритий ключі пов'язані відомим співвідношенням, то обчисливши значення функції $\phi(n)$, можна взнати таємний ключ за відкритим. Відомо, що

$$\phi(n) = (p - 1)(q - 1) \tag{4}$$

і поставлена задача зводиться до обчислення *p* і *q*, де *pq* = *n*. Тоді постає задача факторизації. Природно виникає питання, чи не можна розв'язати задачу визначення таємного ключа, обходячись без факторизації. За твердженням 2.3 [1], цю задачу можна переформулювати як задачу знаходження такого *d*, що *ed*-1 ділиться на $\psi(n)$, де значення функції $\psi(n)$ чисельно дорівнює найменшому спільному кратному чисел *p*-1 і *q*-1 для *n*=*pq*. Але для такого *d* число *m*=*ed*-1 можна використати для розкладу *n* на множники за допомогою імовірнісної процедури IV.5.2 [1]. Отже, визначення таємного ключа для RSA є таким же важким, як факторизація модуля *n*. Тобто знаходження таємного ключа для RSA є еквівалентним до факторизації чисел, що є добутком двох простих, відносно поліноміальної імовірнісної звідності [1].

Згідно з твердженням 4.4 [1], 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

$$y \neq \pm y' (\mathrm{mod}\, n). \tag{5}$$

Таким чином, поставлена задача зводиться до розв'язання конгруенції $y^2 = (y')^2 (\mathrm{mod}\, n)$.

Двома самими помітними проривами, що дозволяють розв'язати останню конгруенцію стали алгоритм "квадратичного решета", винайдений Джоном Поллардом на початку 1980-х років, і алгоритм "решета числового поля", запропонований цілою групою математиків на початку 1990-х років. Для чисел із довжиною менше 350 біт краще працює перший алгоритм, для чисел із більшою довжиною - другий алгоритм.

Розглянемо метод решета числового поля детальніше.

Подамо число *n* у формі

$$n = r^e - s, \tag{6}$$

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

$$r^{kd} \equiv sr^{kd-e} (\mathrm{mod}\, n). \tag{7}$$

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

$$m^d \equiv c (\mathrm{mod}\, n). \tag{8}$$

Сформуємо многочлен

$$f(x) = x^d - c \in Z[x], \tag{9}$$

де α – корінь многочлена.

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

$$\varphi(a + \alpha b) = (a + mb \bmod n). \tag{10}$$

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

$$y^2 = (y')^2 (\mathrm{mod}\, n). \tag{11}$$

Під час пошуку можна обмежити нас 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 $N(a + \alpha b) = a^d - c(-b)^d \in Z$, де a і b - взаємопрості числа.

Для того щоб знайти конкретні значення чисел a і b поступають таким чином: зафіксуємо b і перевіряємо $a+mb$ на гладкість за допомогою решета поля. Для простого p стартова точка для решета є $-mb$ mod p кінцева точка b+1. Якщо $f(c_p) \equiv 0 \bmod p$, то значення a обчислюємо за формулою $a \equiv -c_p b \bmod p$. Згідно алгоритму p ділить $N(a + \alpha b) = a^d - c(-b)^d \in Z$, якщо $a \equiv -c_p b \bmod p$. Отже ми знайшли пару чисел a і b, котрі будуть використані для факторизації числа n.

Результат роботи алгоритму дозволяє визначити таємний ключ системи шифрування RSA за відкритим ключем. 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.

Література: 1. Вербіцький О.В. Вступ до криптології. – Львів: ВНТЛ, 1998. – 247 с., 2. Lenstra A.K., Lenstra H.W., Manasse Jr, M.S., Pollard J.M. The number field sieve. Online access through WWW: http://www.rsasecurity.com/rsalabs/faq/., 3. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення. – Введ. 01.01.98. – К.: Держстандарт України, 1997. – 11 с.

УДК 638.322

ИСПОЛЬЗОВАНИЕ АППАРАТА БУЛЕВЫХ ФУНКЦИЙ ДЛЯ ОЦЕНКИ ЭФФЕКТИВНОСТИ КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ ЗАЩИТЫ ИНФОРМАЦИИ

Константин Самофалов, Эль-Хами Иад, Святослав Кожемякин
Национальный Технический Университет Украины "КПИ"

Анотація: **Ціллю досліджень є розробка підходу до визначення рівня захищеності широкого класу криптографічних алгоритмів, що базується на використанні апарату булевих функцій. Показано, що криптографічні властивості широкого класу алгоритмів мають за основу математичну задачу віднаходження коренів системи булевих нелінійних рівнянь, що не має аналітичного вирішення. Доведена тотожність проблеми порушення захисту та проблеми розв'язання систем нелінійних булевих рівнянь. Запропоновано оцінювати стійкість алгоритмів за допомогою досліджень специфічних властивостей еквівалентних булевих функцій.**

Summary: **The aim of the study is to develop an approach to analysis of the security level of cryptographic algorithm on the basis of Boolean function tool application. It has been shown that security of the broad class of cryptographic algorithms, is based on the difficulty to solve an analytically intractable problem of finding the roots of a nonlinear Boolean equation system. The break methods for cryptographic algorithms of this class are identical with strategy of search diminishing at finding the roots of such a system. Criteria for evaluation of equivalent Boolean equation system solution difficulty are worked out as well as means of their practical identification are presented.**

Ключові слова: **булеві функції, повна та умовна ентропія булевих функцій, критерій лавинного ефекту, алгоритми захисту інформації**.

I Введение

Одним из наиболее важных компонент современных систем защиты информации являются криптографические алгоритмы. Определение обьективного уровня устойчивости криптографических алгоритмов к вскрытиям аналитическими и комбинированными методами представляет собой практически важную