УДК 681.322.067

В.В. Гніліцький, к.т.н., доц.
Житомирський інженерно-технологічний інститут
В.П. Полторак, к.т.н., доц.
Ю.В. Сидорчук, студ.
Національний технічний університет України "КПІ"

КРИПТОГРАФІЯ – ПОТЕНЦІЙНА МОЖЛИВІСТЬ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В СИСТЕМАХ УПРАВЛІННЯ. АСИМЕТРИЧНІ КРИПТОСИСТЕМИ НА ПРИКЛАДІ RSA.

Викладено один з найбільш поширених асиметричних криптографічних алгоритмів шифрування інформації – RSA.

Характерною рисою сучасних інформаційно-обчислювальних систем (ІОС) є інтенсивний обмін даними. Для його забезпечення застосовують різні види технічних засобів зв'язку. Але дуже часто між двома законними користувачами ІОС відбувається обмін не просто даними, а конфіденційною інформацією. Така інформація підпадає під різноманітні загрози (перехоплення, прочитання, модифікація) з боку зацікавлених в цьому незаконних користувачів. Факти реалізації подібних загроз називають несанкціонованим доступом (НСД). Оскільки такі ситуації часто бувають не просто небажаними, а недопустимими через значні втрати, пов'язані з дією зловмисників, необхідно вживати спеціальних заходів для захисту інформації від НСД. Одним з потужних засобів, здатних відвернути різні форми нападу на конфіденційні дані, є стійка криптографія.

Прикладом стійкої криптографічної системи з відкритим ключем є система RSA. Алгоритм шифрування RSA – один з найбільш відомих криптографічних алгоритмів шифрування з відкритим ключем – був розроблений (а пізніше запатентований) Роном Райвестом (Ron Rivest), Ейді Шаміром (Adi Shamir) і Леном Адлеманом (Len Adleman) – трьома вченими з Массачусетського технологічного інституту – у 1977 р. [1]. Перші літери прізвищ розробників і склали назву цього алгоритму.

Важковирішувана математична задача, яка лежить в основі алгоритму RSA, пов'язана з розкладенням великих цілих чисел на множники. В наш час не існує ефективного розв'язку цієї задачі при використанні дуже великих чисел (250–300 десяткових розрядів), що дозволяє говорити про досить високу криптостійкість цього алгоритму [1, 3].

Криптографічний алгоритм RSA використовує лише один тип обчислень – піднесення до степеня, яке проводиться за модулем великого складеного числа n. Число n є добутком двох простих чисел p і q великої розрядності. Для досягнення однозначності шифрування/дешифрування повідомлення за алгоритмом RSA відкритий текст розбивають на блоки, кожен з яких може бути представлений у вигляді числа $W(i)$, яке знаходиться в діапазоні (0, n). В результаті отримують послідовність чисел $W(i)$, кожне з яких шифрується окремо. Назвемо $W(i)$

 © В.В. Гніліцький, В.П. Полторак, Ю.В. Сидорчук, 2000

числовим образом блока відкритого тексту. Будемо далі числовий образ $W(i)$ позначати як W, а криптограму блока – як C.

Враховуючи введені позначення, процес шифрування RSA можна представити таким виразом [1]:

$$C = W^e \bmod n, \tag{1}$$

де e – ключ шифрування, процедура отримання якого буде описана нижче.

Дешифрування кожного блока C шифр-тексту полягає в зніманні внесеного спотворення (1) через піднесення криптограми C до степеня, рівного ключу дешифрування d, тобто

$$W = C^d \bmod n. \tag{2}$$

Покажемо, що в результаті таких перетворень C дійсно буде відновлене початкове повідомлення W.

Справді, відомо, що для чисел, взаємно простих з числом n (у даному випадку такими числами будуть числа, не кратні p або q), справедливе таке співвідношення (теорема Ейлера) [2]:

$$W^{\varphi(n)} \equiv 1(mod\ n), \tag{3}$$

де $\varphi(n)$ – значення функції Ейлера для числа n, яке є кількістю додатних цілих k, не більших за n і таких, що НОД (k, n) = 1.

Піднесемо обидві частини виразу (3) до степеня j, де j – довільне додатне ціле число:

$$W^{j\varphi(n)} \equiv 1(mod\ n).$$

При цьому, всі дії з порівняннями виконуємо відповідно до відомих з теорії чисел властивостей конгруенцій [2].

Домножимо обидві частини отриманої конгруенції на W:

$$W^{j\varphi(n)+1} \equiv W\ (mod\ n). \tag{4}$$

Накладемо вимогу виконання умови:

$$j\varphi(n)+1 = ed, \tag{5}$$

що рівносильно виконанню конгруенції:

$$ed \equiv 1\ (mod\ \varphi(n)). \tag{6}$$

Тоді, представивши ліву частину порівняння (4) з врахуванням умови (5), отримаємо:

$$W^{ed} \equiv W\ (mod\ n). \tag{7}$$

Врахуємо, що

$$C^d = (W^e)^d = W^{ed},$$

звідки випливає

$$C^d \equiv W\ (mod\ n),$$

що доводить справедливість виразу (2).

З іншого боку, співвідношення (2) справедливе також для чисел, які не є взаємно простими з числом n.

Оскільки $n > W$ є добутком p і q, такими числами будуть числа, кратні p або q. Нехай W кратне p (аналогічні міркування проводяться і для W, кратного q). Тоді для нього справедлива теорема Ейлера:

$$W^{q-1} \equiv 1\ (mod\ q).$$

Піднесемо обидві частини цього порівняння до степеня (p – 1):

© В.В. Гніліцький, В.П. Полторак, Ю.В. Сидорчук, 2000

$$W^{(q-1)*(p-1)} \equiv 1 \ (mod\ q). \quad (8)$$

Оскільки добуток $(q-1)*(p-1)$ представляє собою функцію Ейлера $\varphi(n)$, то порівняння (8) співпадає з порівнянням (3) з точністю до модуля. Проводячи аналогічні міркування, доводимо справедливість виразу:

$$W^{ed} \equiv W \ (mod\ q). \quad (9)$$

Таке ж порівняння справедливе і по модулю p, що є дільником W, оскільки числа, які стоять в лівій і правій частинах виразу (9) і кратні модулю, будуть рівнозалишковими за цим модулем (залишок дорівнює 0).

Оскільки порівняння $W^{ed} \equiv W$ справедливе для декількох модулів (а саме p і q), то згідно з однією з властивостей порівнянь в теорії чисел [2], це ж порівняння справедливе і для модуля, що дорівнює найменшому спільному кратному K цих модулів. Оскільки p і q – прості числа, то $K = p * q = n$. Таким чином, виконується співвідношення (7), з якого, як було показано вище, випливає справедливість (2), що й потрібно було довести.

Опишемо тепер основні етапи генерування ключів, які включають такі кроки [3]:

1) визначення числа n, за модулем якого проводяться обчислення при шифруванні/дешифруванні;

2) визначення ключа шифрування e і ключа дешифрування d.

Наведемо опис виконання цих етапів.

1. Визначення числа n, за модулем якого проводяться обчислення при шифруванні/дешифруванні.

Вибирають два дуже великих простих числа p і q. Число n є добутком цих чисел, тобто

$$n = p * q.$$

Криптостійкість алгоритму базується на складності оберненого перетворення, тобто визначення дільників цілого числа n (як це пов'язано з отриманням секретного ключа, необхідного для відновлення зашифрованого повідомлення, буде показано нижче). Задача розкладу числа великої розрядності на прості множники є обчислювально важковирішуваною задачею.

2. Визначення ключа шифрування e і ключа дешифрування d.

Знаходять добуток $(p-1)*(q-1)$, який є функцією Ейлера $\varphi(n)$ для числа n [2].

Далі вибирають велике випадкове число e, взаємно просте з $\varphi(n)$. Це число і буде ключем шифрування. Ключ дешифрування d вибирається таким, щоб виконувалось співвідношення (6), а саме:

$$e * d = 1 \ mod\ \varphi(n).$$

Секретним (закритим) ключем в криптосистемі RSA є число d, яке повинне зберігатися користувачем в таємниці. Крім того, звичайно, необхідно зберігати в таємниці числа p і q. Відкритим ключем є пара чисел e і n, які можуть бути вільно поширені у відкритому каналі і опубліковані.

Як зазначалося раніше, теорія криптосистем з відкритим ключем базується на понятті односторонньої функції або односторонньої функції з секретом («потаємним ходом»). «Потаємним ходом» в алгоритмі RSA є сукупність чисел $\{p, q, e\}$. Очевидно, що обчисливши функцію Ейлера $\varphi(n)$, можна знайти секретний ключ, використавши вираз (6). У зв'язку з цим спроби несанкціоно-

 © В.В. Гніліцький, В.П. Полторак, Ю.В. Сидорчук, 2000

ваного доступу в цій криптосистемі пов'язані з відшуканням $\varphi(n)$. На сьогодні обчислення функції Ейлера для числа n без знання простих дільників цього числа p і q є практично невирішуваною задачею, тому криптоаналіз цього алгоритму пов'язаний з розв'язанням задачі знаходження дільниікв великого цілого числа (так званої задачі факторизації числа). Криптостійкість алгоритму грунтується на обчислювальній складності розв'язку цієї задачі.

Через перестановочність операції множення в алгоритмі RSA не має значення, який з ключів буде використано для шифрування повідомлення, а який для дешифрування. При звичайній передачі конфіденційної інформації *відправник* зашифровує дані відкритим ключем отримувача, а *отримувач* розшифровує їх своїм секретним ключем. При реалізації ж цифрового підпису *відправник* зашифровує частину повідомлення (ставить підпис) своїм секретним ключем, а отримувач має можливість ідентифікувати підпис відправника, використовуючи його ж відкритий ключ. При цьому той, хто підписав повідомлення таким чином, не зможе від нього відмовитися, оскільки секретний ключ належить йому і зберігається лише у нього. Тим самим і здійснюється ідентифікація відправника.

До переваг криптосистеми RSA можна віднести такі:

- можливість управління ключами, а також захищеного поширення ключів та їх заміни;
- можливість реалізації цифрового підпису;
- відсутність необхідності у секретному каналі зв'язку.

До недоліків RSA можна віднести:

- низьку швидкість процесів шифрування/дешифрування;
- необхідність задавання нового типу даних для ПК та інших обчислювальних пристроїв і організації спецпроцесорів для обробки таких даних з розрядністю в декілька сотень десяткових знаків.

ЛІТЕРАТУРА:

1. *Жельников В.* Криптография от папируса до компьютера. – М., ABF, 1997. – 336 с.
2. *Виноградов И.М.* Основы теории чисел. – М.: Наука, Гл. ред. физ.-мат. лит., 1981. – 176 с.
3. Защита информации в персональных ЭВМ / Спесивцев А.В., Вегнер В.А. и др. – М.: Радио и связь, 1992. – 192 с.

ГНІЛІЦЬКИЙ Віталій Васильович – кандидат технічних наук, доцент, завідувач кафедри автоматики та управління в технічних системах Житомирського інженерно-технологічного інституту.

Наукові інтереси:

– цифрова обробка сигналів;

– інформаційні системи.

© В.В. Гніліцький, В.П. Полторак, Ю.В. Сидорчук, 2000

ПОЛТОРАК Вадим Петрович – кандидат технічних наук, доцент кафедри АУТС Національного технічного університету України «Київський політехнічний інститут».

Наукові інтереси:

– передача, обробка та захист інформації.

СИДОРЧУК Юлія Вікторівна – студентка 6-го курсу Національного технічного університету України «Київський політехнічний інститут».

Наукові інтереси:

– комп'ютерна криптографія та засоби захисту інформації.

Подано 15.11.1999.

 © В.В. Гніліцький, В.П. Полторак, Ю.В. Сидорчук, 2000