

формації ДЗЗ, але є висококваліфікованими спеціалістами іншого профілю. Результатом є підвищення інформаційної віддачі корисної інформації з даних ДЗЗ.

#### Список використаних джерел

1. Прэтт У. Цифровая обработка изображений : в 2 кн. Кн. 1 / У. Прэтт. – М. : Мир, 1982. – 310 с.
2. Гонсалес Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М. : Техносфера, 2006. – 1072 с.
3. Основы геоинформатики : в 2 кн. Кн. 1 / Е. Г. Капралов, А. В. Кошкарев, В. С. Тикунов и др. ; под ред. В. С. Тикунова. – М. : Академия, 2004. – 352 с.
4. Шовенгерт Р. А. Дистанционное зондирование. Модели и методы обработки изображений / Р. А. Шовенгерт ; пер. с англ. А. В. Кирюшина. – М. : Техносфера, 2010. – 591 с.

УДК 004.056.5:004.057.42

**В.В. Соломаха**, ст. викладач

**М.В. Верьовко**, аспірант

Чернігівський національний технологічний університет, м. Чернігів, Україна

#### ДОСЛІДЖЕННЯ АЛГОРИТМІВ АСИМЕТРИЧНИХ КРИПТОСИСТЕМ

**В.В. Соломаха**, ст. преподаватель

**М.В. Вереvко**, аспирант

Черниговский национальный технологический университет, г. Чернигов, Украина

#### ИССЛЕДОВАНИЕ АЛГОРИТМОВ АСИММЕТРИЧНЫХ КРИПТОСИСТЕМ

**Valerii Solomakha**, senior teacher

**Mariia Verovko**, PhD student

Chernihiv National University of Technology, Chernihiv, Ukraine

#### THE STUDY OF ALGORITHMS FOR ASYMMETRIC CRYPTOSYSTEMS

*Стаття містить результати практичних досліджень сучасного алгоритму асиметричної криптосистеми RSA по швидкодії під час роботи з різним об'ємом інформації і з ключами різної довжини.*

**Ключові слова:** алгоритм шифрування, секретний та відкритий ключ, модуль, криптосистема, швидкодія.

*Статья содержит результаты практических исследований современных алгоритмов асимметричной криптосистемы RSA по быстродействию при работе с различным объемом информации и ключами разной длины.*

**Ключевые слова:** алгоритм шифрования, секретный и открытый ключ, модуль, криптосистема, быстродействие.

*The article contains the results of comparative studies of modern algorithms of asymmetric cryptosystem RSA on a fast-acting during work with the different volume of information and keys of different length.*

**Key words:** algorithm of encipherment, the secret and opened key modul, ckryptosystem, fast-acting.

**Постановка задачі.** Метою дослідження було порівняння роботи сучасного алгоритму асиметричної криптосистеми RSA під час шифрування (розшифрування) різних об'ємів інформації і при різних розмірах ключа.

**Аналіз останніх досліджень і публікацій** Вагомий внесок у дослідження криптографічних алгоритмів в останній час зробили як зарубіжні науковці (А. Ленстра і М. Манассі, Ж. Брассар), так і вітчизняні (В. Мельников, Б. Ключевський, П. Ісаєв, Д. Зегжда та ін.). Більшість наукових робіт з питань криптографічних систем з відкритим ключем присвячена принципам знаходження відкритих та закритих ключів, їх використанню під час шифрування та розшифрування, в яких практично не порівнюють їх характеристики. Так, не виявлено порівнянь швидкості роботи різних асиметричних криптосистем під час шифрування різних об'ємів інформації та ключами різної довжини.

**Мета статті.** Існує безліч (не менше двох десятків) алгоритмів асиметричних шифрів, істотними параметрами яких є:

- стійкість;
- довжина ключа;

- довжина оброблюваного блока;
- складність апаратної/програмної реалізації.

Метою дослідження було порівняння швидкодії алгоритму RSA під час шифрування (розшифрування) різних об'ємів інформації ключами різної довжини. Для цього використовувалася комп'ютерна система вивчення методів і засобів апаратно-програмного захисту інформації CRYPTO, яка написана мовою JAVA та дозволяє досліджувати криптографічні алгоритми і протоколи, формальні політики безпеки [5].

**Виклад основного матеріалу.** Застосування асиметричних алгоритмів шифрування (шифрування з відкритим ключем) вирішує основну проблему симетричних алгоритмів шифрування поширення симетричного ключа між учасниками системи. У 1976 р. публікується стаття «Новые направления в криптографии» Уїтфілда Діффі та Мартіна Хеллмана, під впливом роботи Ральфа Меркла – починається нова ера криптології з відкритими ключами.

У цьому випадку шифрування робиться відкритим ключем, а розшифрування – закритим ключем (рис.). Відкритий і закритий ключ пов'язані між собою, але не можуть бути отримані один з іншого.

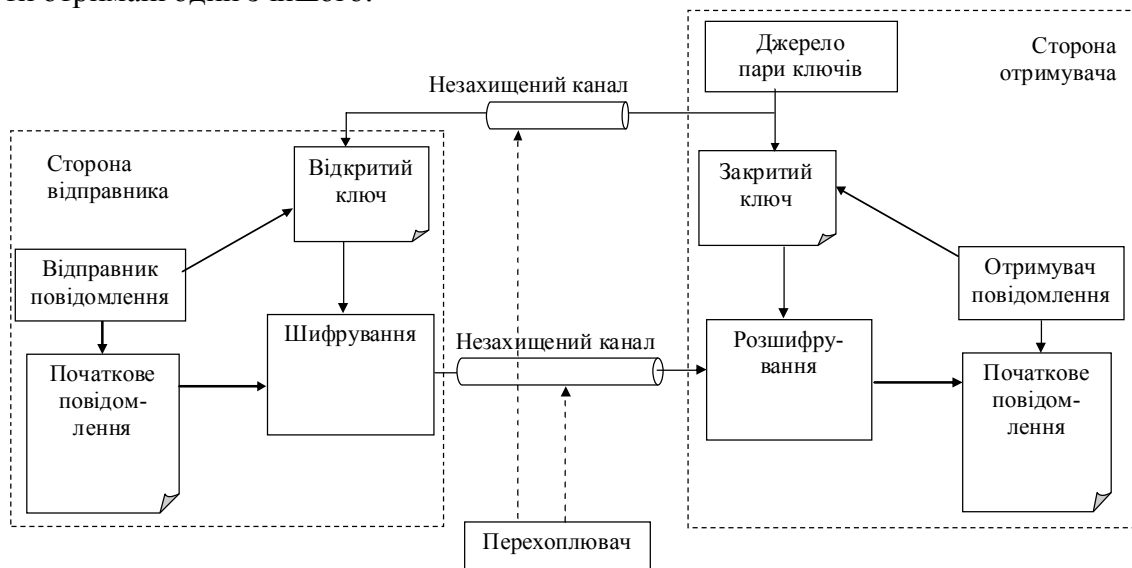


Рис. Схема асиметричного шифрування

Серед сучасних алгоритмів шифрування з симетричним ключем відомі і широко використовуються RSA (Rivest, Shamir, Aldeman) Ель Гамала, Поліга-Хеллмана, Рабіна та інші [6].

Асиметричні алгоритми шифрування ґрунтуються на застосуванні однонапрямлених функцій. Функція  $f: X \rightarrow Y$  є однонапрямлена, якщо для всіх  $x \in X$  можна легко вчислити функцію  $y = f(x)$ , де  $y \in Y$ . Але для більшості  $y \in Y$  досить складно отримати значення  $x \in X$ , таке, що  $f(x) = y$  (хоча воно існує).

Основний критерій однонапрямлених функцій: відсутність ефективних алгоритмів зворотного перетворення  $Y \rightarrow X$ . Такими функціями є [3]:

- факторизація;
- дискретне логарифмування.

Факторизація (розкладання на множники) великих чисел. Знаходження дільників  $P$  і  $Q$  великого цілого числа  $N = P \cdot Q$  є практично нерозв'язаною задачею при чималих значеннях  $N$ . За сучасними оцінками теорії чисел при цілому  $N \approx 2^{64}$  і  $P \approx Q$  для розкладання числа  $N$  буде потрібно близько  $10^{23}$  операцій, тобто задача практично нерозв'язна для сучасних ЕОМ.

Дискретне логарифмування: за відомими цілими  $A$ ,  $N$ ,  $y$  знайти ціле число  $x$ , таке, що  $A^x \bmod N = y$ . Якщо  $y = A^x$ , то природно  $x = \log_a(y)$ . Алгоритм обчислення дискретного логарифма за прийнятний час доки не знайдений. За сучасними оцінками теорії чисел при цілих числах  $A \approx 2^{664}$  і  $N \approx 2^{664}$  для вирішення завдання дискретного логарифмування потрібно близько  $10^{26}$  операцій, тобто в  $10^3$  раз більше обчислювальна складність, ніж завдання факторизації.

Криптосистема RSA створена у 1978 році [1]. Отримала назву від прізвищ розробників – Райвест, Шамир, Адлеман (США). Це перший повноцінний алгоритм з відкритим ключем, може працювати як у режимі шифрування даних, так і в режимі електронного цифрового підпису.

У криптосистемі RSA відкритий ключ  $K_B = e$ , секретний ключ  $k_B = d$ , повідомлення  $M$  та криптограма  $C$  належать множині цілих чисел

$$Z_N = \{0, 1, 2, \dots, N-1\}, \text{ де } N \text{ — модуль, } N = P \cdot Q.$$

Тут  $P$  і  $Q$  – випадкові великі прості числа. Для забезпечення максимальної безпеки вибирають  $P$  і  $Q$  рівної довжини і зберігають у таємниці.

Відкритий ключ  $K_B$  вибирають випадковим способом так, щоб виконувалися умови:

$$1. 1 < K_B \leq \varphi(N),$$

$$2. \text{НОД}(K_B, \varphi(N)) = 1, \varphi(N) = (P-1)(Q-1), \text{ де } \varphi(N) \text{ — функція Ейлера.}$$

Далі, використовуючи розширений алгоритм Евкліда, обчислюють секретний ключ  $k_B$ , такий, що  $k_B \cdot K_B \equiv 1 \pmod{\varphi(N)}$  або  $k_B = K_B^{-1} \pmod{(P-1)(Q-1)}$ . Це можна здійснити, якщо одержувач  $B$  знає пару простих чисел  $(P, Q)$  і може легко знайти  $\varphi(N)$ , при цьому  $k_B$  і  $N$  мають бути взаємно простими.

Відкритий ключ  $K_B$  використовують для шифрування даних, а секретний ключ  $k_B$  – для розшифрування. Перетворення шифрування визначає криптограму  $C$  через пару (відкритий ключ  $K_B$ , повідомлення  $M$ ) відповідно до такої формули

$$C = E_{K_B}(M) = E_B(M) = M^{K_B} \pmod{N}.$$

Припустимо: користувач  $A$  хоче передати користувачу  $B$  повідомлення, яке зашифроване, криптосистемою RSA. Таким чином, користувач  $A$  є відправником повідомлення, а користувач  $B$  – отримувачем. Криптосистему RSA повинен сформував отримувач повідомлення, тобто користувач  $B$ . Послідовність дій користувачів  $B$  та  $A$  такі.

Користувач  $B$  вибирає два довільно великих простих числа  $P$  і  $Q$ . Користувач  $B$  обчислює значення модуля  $N = P \cdot Q$ . Користувач  $B$  обчислює функцію Ейлера

$$\varphi(N) = (P-1)(Q-1)$$

і вибирає випадковим способом значення відкритого ключа  $K_B$  з урахуванням виконаних умов:  $1 < K_B \leq \varphi(N)$ ,  $\text{НОД}(K_B, \varphi(N)) = 1$ .

Користувач  $B$  обчислює значення секретного ключа  $k_B$ , використовуючи розширений алгоритм Евкліда під час вирішення порівняння  $k_B = K_B^{-1} \pmod{\varphi(N)}$ .

Користувач  $B$  пересилає користувачеві  $A$  пару чисел  $(N, K_B)$  по незахищеному каналу.

Якщо користувач  $A$  хоче передати користувачеві  $B$  повідомлення  $M$ , він виконує такі кроки. Користувач  $A$  розбиває вихідний відкритий текст  $M$  на блоки, кожен з яких може бути представлений у вигляді числа.

Користувач  $A$  шифрує текст, представлений у вигляді послідовності чисел  $M_i$ , за формулою  $C_i = M_i^{K_B} \pmod{N}$  і відправляє криптограму  $C_1, C_2, C_3, \dots, C_i$  користувачеві  $B$ .

## TECHNICAL SCIENCES AND TECHNOLOGIES

Користувач В розшифровує прийнятну криптограму, використовуючи секретний ключ  $k_B$  за формулою  $M_i = C_i^{k_B} \pmod{N}$ .

У результаті буде отримана послідовність чисел  $M_i$ , які є вихідним повідомленням М. Щоб алгоритм RSA мав практичну цінність, необхідно мати можливість без істотних витрат генерувати великі прості числа, вміти оперативно обчислювати значення ключів  $k_B$  і  $K_B$  [2].

Порівняння симетричних та асиметричних криптосистем [3]:

Головною гідністю криптосистем з відкритим ключем є їх потенційно висока безпека: не треба передавати значення секретних ключів.

У симетричних криптосистемах існує небезпека розкриття секретного ключа під час передачі.

Недоліки асиметричних криптосистем:

- генерація нових ключів ґрунтується на генерації великих простих чисел, а перевірка простоти чисел займає багато процесорного часу;
- процедури, пов'язані з піднесенням до степеня багатозначного числа, досить громіздкі.

Тому швидкодія криптосистем з відкритим ключем у сотні і більше разів менше швидкодії симетричних криптосистем з секретним ключем.

Криптосистеми реалізуються як апаратно, так і програмно.

Для апаратної реалізації розроблені спеціальні процесори на (СВІС), що дозволяють виконувати піднесення великих чисел до колосально великого степеня за модулем N за відносно коротким часом.

Кращими з них є ті, що серійно випускаються, тобто процесори фірми CYLINK, які виконують 1024-бітове шифрування RSA.

**Результати досліджень.** Швидкодія алгоритму RSA під час шифрування та розшифрування різних об'ємів інформації довжиною від 100 до 1000 біт та при розмірах ключа від 1000 до 20 000 біт.

**Висновки і пропозиції.** 1. Середній час шифрування та розшифрування повідомлень 1 мс.

2. Чим довший ключ, тим довше відбувається дешифрування.

3. Чим довший ключ, тим швидше відбувається шифрування.

4. Апаратна реалізація асиметричної криптосистеми  $\approx$  в 1000 разів повільніше за апаратну реалізацію симетричного криптоалгоритму.

5. Програмна реалізація RSA  $\approx$  в 100 разів повільніше DES.

З розвитком комп'ютерних технологій ці оцінки можуть дещо змінюватися, але асиметрична криптосистема ніколи не досягне швидкодії симетричних криптосистем [6]. Головна гідність криптосистем з відкритим ключем є їх потенційно висока безпека: не треба передавати значення секретних ключів.

У симетричних криптосистемах існує небезпека розкриття секретного ключа під час передачі.

Але в асиметричних криптосистемах є і недоліки:

- генерація нових ключів ґрунтується на генерації великих простих чисел, а перевірка простоти чисел займає багато процесорного часу;
- процедури, пов'язані з піднесенням до степеня багатозначного числа, досить громіздкі.

Поширені довжини ключів симетричних і асиметричних криптосистем, для яких труднощі атаки повного перебору приблизно дорівнюють труднощам факторизації відповідних модулів асиметричних криптосистем (табл.).

Довжини ключів [7]

| Довжина ключа симетричної криптосистеми, біт | Довжина ключа асиметричної криптосистеми, біт |
|--|---|
| 56   | 384   |
| 64   | 512   |
| 80   | 768   |
| 112  | 1792  |
| 128  | 2304  |

Тому швидкодія криптосистем з відкритим ключем звичайно в сотні і більше разів менше швидкодії симетричних криптосистем з секретним ключем.

Ось чому застосовується комбінований (гібридний) метод шифрування: поєднання високої секретності асиметричних криптосистем з високою швидкістю роботи симетричних криптосистем: криптосистема з відкритим ключем застосовується для шифрування, передачі і подальшого розшифрування тільки секретного ключа симетричної криптосистеми, яка застосовується для шифрування і передачі початкового відкритого тексту. Це схема електронного цифрового конверта.

#### Список використаних джерел

1. Диффи У. Защищенность и имитостойкость: Введение в криптографию / У. Диффи, М. Э. Хэллман // ТИИЭР. – 1979. – Т. 67, № 3. – С. 71–109.
2. Зегжда Д. П. Основы безопасности информационных систем / Д. П. Зегжда, А. М. Ивашко. – М.: Горячая линия – Телеком, 2000. – 496 с.
3. Мельников В. В. Защита информации в компьютерных системах / В. В. Мельников. – М.: Финансы и статистика, 1997. – 368 с.
4. Программирование алгоритмов защиты информации / А. В. Домашев, В. О. Попов, Д. И. Правиков, И. В. Прокофьев, А. Ю. Щербаков. – М.: Нолидж, 2000. – 288 с.
5. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. – М.: Радио и связь, 1999. – 328 с.
6. Столингс В. Криптография и защита сетей / В. Столингс. – М.: Вильямс, 2001. – 672 с.
7. Яценко В. В. Введение в криптографию / В. В. Яценко. – СПб.: Питер, 2001. – 288 с.

УДК 519.8

**Ю.М. Гебура**, аспірант

Ужгородський національний університет, м. Ужгород, Україна

#### ПРИНЦИПИ МАТЕМАТИЧНОГО МОДЕЛЮВАННЯ ДЕРЕВОПОДІБНИХ РОЗПІЗНАВАЛЬНИХ СИСТЕМ

**Ю.М. Гебура**, аспірант

Ужгородский национальный университет, г. Ужгород, Украина

#### ПРИНЦИПЫ МАТЕМАТИЧЕСКОГО МОДЕЛИРОВАНИЯ ДРЕВОВИДНЫХ РАСПОЗНАВАТЕЛЬНЫХ СИСТЕМ

**Yurii Hebura**, PhD student

Uzhhorod National University, Uzhhorod, Ukraine

#### PRINCIPLES OF MATHEMATICAL MODELLING OF TREELIKE RECOGNITION SYSTEMS

*Розглянуто принципи математичного моделювання деяких деревоподібних розпізнавальних систем, де система різницевих рівнянь, із вбудованими в них графіками подій, може бути вирішена аналітично для траєкторії системи. Деревоподібні розпізнавальні системи є дискретними подіями ієрархічних систем. Представлені імітаційні моделі є основними принципами математичного моделювання деревоподібних розпізнавальних систем, які мають явні переваги у порівнянні з керованими моделями моделювання.*

**Ключові слова:** математичне моделювання, деревоподібні розпізнавальні системи, ієрархічні системи, граф, імітаційна модель.