6. Коркішко Т.А., Мельник А. О., Мельник В.А. Захист інформації в комп'ютерних і телекомунікаційних мережах: Алгоритми та процесори симетричного блокового шифрування. Львів: БАК, 2003. – 168 с.
7. Karpinskyy M., Korkishko L. Architecture of cryptographic devices resistant to side-channel attacks // Proc. of the International Conf. on Computer Science and Information Technologies. CSIT-2006. – Lviv: Lviv Polytechnic National University,2006. – P. 167-170.
8. Golic J., Tymen Ch. Multiplicative masking and power analysis of for AES // Lecture Notes in Computer Science: Proc. of International workshop Cryptographic Hardware and Embedded Systems. CHES 2002. – Berlin: Springer, 2002. – Vol. 2523. – P. 198-212.

УДК 681.3

МЕТОД ФАКТОРИЗАЦІЇ ЧИСЕЛ ВЕЛИКОЇ РОЗРЯДНОСТІ НА ОСНОВІ ТЧБ РАДЕМАХЕРА-КРЕСТЕНСОНА

Якименко І.З.[1)], **Івасьєв С.В,**[2)], **Назаров В.І.** [3)]
Тернопільський національний економічний університет
[1)] *к.т.н., доцент;* [2)] *аспірант;* [2)] *магістрант*

I. Постановка проблеми

Факторизацією натурального числа називається його розкладання в добуток простих множників. Це завдання має велику обчислювальну складність. Один з найпопулярніших методів криптографії з відкритим ключем, метод RSA, заснований на трудомісткості завдання факторизації довгих цілих чисел [1].

II. Мета роботи

Метою роботи є модифікація методу факторизації Ферма для оцінки криптостійкості RSA-подібних асиметричних шифрів в криптографічних системах захисту інформації, зменшення складності та підвищення швидкодії алгоритмів.

III. Удосконалений алгоритм Ферма

В даному методі Ферма доцільно скористатися теоретико-числовим базисом Крестенсона [2], який дозволяє зменшити обчислювальну складність за рахунок зменшення розрядностей чисел, над якими проводяться операції.

Тобто в рівнянні:

$$x^2 = y^2 - n \tag{1}$$

робимо наступне перетворення:

$$x^2 mod\ p = y^2 - n\ mod\ p, \tag{2}$$

в результаті отримали $x^2 \equiv (y^2 - n) mod\ p$

Для рішення даного порівняння доцільно скористатися символами Якобі, які дозволяють однозначно вказувати, чи обчислюється корінь за модулем.

Нехай p – просте, a – ціле число. Символ Лежандра $\left(\frac{a}{p}\right)$ визначається так:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, \text{ якщо } p \text{ ділиться на } a \\ 1, \text{ якщо } a \in Q_p \\ -1, \text{ якщо } a \in \bar{Q}_p \end{cases}.$$

Число a, яке не ділиться на непарне просте p, є квадратичним лишком за модулем p тоді і тільки тоді, коли $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, і квадратичним нелишком тоді і тільки тоді коли $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

За теоремою Ферма [1, 2] ap-1 ≡ 1 (mod p) при НСД(a, p) = 1 та НСД(2, p) = 1. Або:

$$\left(a^{\frac{p-1}{2}} + 1\right) * \left(a^{\frac{p-1}{2}} - 1\right) \equiv 0 \bmod p.$$

Звідси вираз в одній із дужок ділиться на p. Обидві дужки не можуть ділитися на p, оскільки тоді на p ділилася б і їх різниця, яка дорівнює 2, а за умовою теореми p – непарне просте число. Якщо a є квадратичним лишком, то a = x2 (mod p) для деякого такого x, що НСД(x, p) = 1. Маємо:

$a^{\frac{p-1}{2}} \equiv \left(x^2\right)^{\frac{p-1}{2}} \equiv$ xp-1 $\equiv$1 mod p, тобто $a^{\frac{p-1}{2}} \equiv 1 \bmod p$ або $a^{\frac{p-1}{2}}$ - 1 ділиться на p. Якщо a є квадратичним нелишком, то $a^{\frac{p-1}{2}}$ - 1 не ділиться на p, звідки $a^{\frac{p-1}{2}}$ + 1 повинно ділитися на p, або $a^{\frac{p-1}{2}} \equiv -1 \bmod p$.

Висновок

Співвідношення обчислювальних складностей розробленого алгоритму відносно класичного визначає виграш в ефективності:

$$E(n) = \frac{n\left(\log_2 n\right)^2}{n\left(\log_2 n\right)} = \log 2n.$$

Отже, виграш в ефективності удосконаленого методу при зростанні розрядності чисел зростає в log2n разів.

Застосування на практиці різних методів розкладання чисел показало, що час виконання алгоритму безпосередньо залежить від його типу та обчислювальної складності.

Список використаних джерел

1. Акушский И.Я. Машинная арифметика в остаточных классах. // Акушский И.Я., Юдицкий Д.И – М: Сов.радио, 1968. – 440 с.
2. Николайчук Я.М. Теорія джерел інформації. – Тернопіль: ТзОВ„Терно–граф”, 2010. – 536 с.

УДК 683.1

ЗАХИСТ ІНФОРМАЦІЇ В МЕРЕЖАХ ЗАГАЛЬНОГО КОРИСТУВАННЯ

Якименко І.З.[1)], Сіверський М.І.[2)]

Тернопільський національний економічний університет

[1)] к.т.н., доцент; [2)] магістрант

І. Постановка проблеми

Швидкий ріст структур інформаційних зв'язків спричинив багаторазовий ріст швидкості інформаційних потоків в комп’ютерних мережах. Величезний потенціал розвитку цих технологій породив загрозу інформаційній безпеці - складну науково-практичну проблему із соціальними наслідками. У цій ситуації найважливішим завданням є організація швидкого, надійного та захищеного зв'язку в мережах загального користування (МЗК).

Захист інформаційних потоків на сьогоднішній день стає усе більш складною проблемою, яка зумовлена певними обставинами, а саме: масове розповсюдження засобів електронної обчислювальної техніки; ускладнення шифрувальних технологій; необхідність захисту не тільки державних і військових секретів, але й промислової, комерційної та фінансової таємниць; можливості несанкціонованих дій з інформацією, що розширюються [1]. Однак наразі приділяється мало уваги факту екстенсивного росту мереж загального користування, а також тому, що більша частина інформації передається саме за їхньою допомогою.

ІІ. Мета роботи.

Проведення аналізу моделей захисту інформації в мережах загального користування на основі класифікації показників безпеки.

ІІІ. Захист інформації в мережах загального користування

Відомо, що основними каналами передачі інформації в МЗК є лінії зв'язку (телефонні). Захист ліній зв'язку являє собою дуже серйозну проблему, тому що ці лини найчастіше бувають безконтрольними і з них можуть несанкціоновано отримуватися інформація [2].

Розробка технічних методів і засобів захисту інформації заснована на використанні методів математичного моделювання [3].

До основних задач моделювання систем захисту інформаційних потоків в комп’ютерних мережах, які найчастіше зустрічають в літературних джерелах, можна поділити на [4]: оцінка якості