УДК 581.3

Informatics and Mathematical Methods in Simulation
Vol. 8 (2018), No. 4, pp. 324-333

АЛГОРИТМИ ПОШУКУ ЗАЛИШКІВ ДОВГИХ ЧИСЕЛ ДЛЯ ЗАДАЧ АСИМЕТРИЧНОЇ КРИПТОГРАФІЇ

Л.М. Тимошенко[1], Ю.М. Івасьєв[2], О.Я. Лотоцький[3], В.М. Гаврилей[1]

[1]Одеський національний політехнічний університет,
просп. Шевченка, 1, Одеса, 65044, Україна; e-mail: lmt0902@gmail.com
[2]Тернопільський національний економічний університет, вул. Львівська, 11, Тернопіль, 46020, Україна;
e-mail: stepan.ivasiev@gmail.com
[3]Національний авіаційний університет,
просп. Космонавта Комарова,1, Київ, 03058, Україна, e-mail: zyzik2323@gmail.com

На сучасному етапі забезпечення інформаційної безпеки держави важливим є засекречування мереж зв'язку військового призначення, одним із ключових напрямів якого є застосування криптографічних методів захисту інформації, зокрема, асиметричної криптографії. Одним із шляхів удосконалення алгоритмів асиметричної криптографії є знаходження залишків довгих чисел. Відомі алгоритми пошуку залишків довгих чисел мають ряд суттєвих недоліків при їх реалізації. В роботі проводиться аналіз заявлених двох нових методів пошуку залишків довгих чисел, їх недоліків та обчислювальних складностей. Описано запропонований авторами метод, наведено його алгоритм та блок-схема. Досліджуються обчислювальні складності трьох розглянутих методів пошуку залишків. Чисельний експеримент оцінки складностей показує, що при виконанні модульних операцій, які використовуються в асиметричних криптоалгоритмах, при переведенні чисел з десяткової системи в систему числення залишкових класів слід використовувати запропонований метод, який характеризується меншою складністю. Для подальшого розгляду залишаються два. Виграш в ефективності запропонованого алгоритму відносно відомого визначається як співвідношення обчислювальних складностей і дорівнює 2. Розроблений на мові програмування високого рівня C++ додаток дозволяє дослідити часові характеристики виконання двох методів. В роботі наведено фрагмент тестування додатку для подвійних чисел Мерсенна та графічне зображення залежності часу знаходження залишків великих чисел від простого числа, для якого знаходиться залишок. Розроблений алгоритм пошуку залишків великих чисел дозволив підвищити швидкодію порівняно з відомим за рахунок використання властивостей залишків та числового базису Радемахера. Це зменшило обчислювальну складність та підвищило виграш у ефективності роботи алгоритму у порівнянні з відомим у два рази, що доводить доцільність його використання при опрацюванні довгих чисел в асиметричних криптографічних системах захисту інформації для підвищення швидкодії процесів шифрування та криптоаналізу.

Ключові слова: асиметрична криптографія, довга арифметика, система залишкових класів, обчислювальна складність, залишки довгих чисел.

Вступ

На жаль, сьогодні триває гібридна війна та військова агресія проти України, тому забезпечення захисту інформації є надважливим завданням інформаційної безпеки держави на даному етапі її розвитку. Перемога у сучасній війні залежить, зокрема, і від засекречування мереж зв'язку військового призначення у системі військового управління [1,2] в процесі переходу системи зв'язку Збройних сил України з аналогових на цифрові телекомунікаційні засоби.

На сучасному етапі розвитку інформаційно-технічних засобів передачі та зберігання інформації одним із шляхів захисту інформації є застосування криптографічних методів, заснованих на принципі Керкгоффза, згідно з яким стійкість криптографічного алгоритму ґрунтується на секретності ключа, а не на таємності

алгоритму шифрування [3,4]. В мережах зв'язку, як правило, використовують альтернативу шифрування з симетричними ключами – криптографічні системи, що поєднують використання пари ключів – відкритого і закритого. Один з них публікують у відкритих джерелах і використовують для шифрування даних, інший ключ тримають в секреті і застосовують для декодування повідомлення. Основна перевага асиметричних шифрів – відсутність необхідності передачі секретного ключа. Вони використовують так звані незворотні чи односторонні функції з властивістю: при заданому значенні x досить легко обчислити значення $f(x)$, проте, якщо $y = f(x)$, то немає простого шляху для обчислення значення x. Зокрема, алгоритм Діффі-Хеллмана побудовано на обчисленні дискретного логарифма у скінченному полі простих чисел, а алгоритм *RSA* – на задачі факторизації. Такі алгоритми використовують арифметику довгих чисел, причому з метою запобігання відомих атак розміри чисел повинні перевищувати 10^{309} [5-7].

Одним із шляхів удосконалення алгоритмів асиметричної криптографії (зокрема, алгоритмів *RSA*, Рабіна, Ель-Гамаля, з використанням еліптичних кривих, електронного цифрового підпису, дослідження порядку еліптичної кривої за допомогою алгоритму Шуфа тощо) є застосування системи залишкових класів [8, 9], і звідси – знаходження залишків довгих чисел [10]. У зв'язку з цим актуальною задачею, яка розглядається в даній роботі, є дослідження існуючих алгоритмів пошуку залишків довгих чисел та розробка нових ефективних алгоритмів.

Розповсюдженим методом пошуку залишків довгих чисел можна вважати такий алгоритм. Для знаходження залишку необхідно виконати ділення, виділити цілу частину від ділення, знайти добуток цілої частини на модуль, та знайти різницю числа і знайденого добутку. Також можна від великого числа віднімати модуль, доки різниця не стане меншою від'ємника. Оскільки числа, над якими виконуються операції, на кожному кроці зменшуються, то такий процес закінчиться через певну кількість кроків [11,12]. Дані алгоритми можна програмно реалізувати, але їх часова складність велика, оскільки операція ділення досить трудомістка. Іншим недоліком алгоритмів пошуку залишків великих чисел є послідовний порядок виконання операцій, тобто неможливість розпаралелення.

Мета роботи

Метою роботи є підвищення ефективності алгоритму пошуку залишків довгих чисел для зростання швидкодії виконання операцій над довгими числами, що використовуються в асиметричних криптосистемах захисту інформації. Ефективність алгоритмів пошуку залишків великих чисел в даній роботі оцінюється їх обчислювальною складністю.

Об'єкт дослідження – процеси програмного опрацювання довгих чисел в криптографічних системах захисту інформації. Предмет дослідження – алгоритми та методи опрацювання довгих чисел, що використовуються в процесах шифрування та криптоаналізу.

Основна частина

Для знаходження залишку великого двійкового числа Y по великому цілочисельному модулю P, який представлено у доповняльному коді для виконання операції віднімання, авторами у [13] запропоновано метод, який ґрунтується на рекурсивному співвідношенні:

$$b_i = [P]_{мд} + 2b_{i-1} + a_i,\ i = n-1,...,0, \quad (1)$$

де n – розрядність числа Y, для якого визначають залишок b_i; a_i – біти двійкового числа $Y = \sum_{i=0}^{n-1} a_i 2^i$, починаючи зі старшого розряду a_{n-1}; $[P]_{мд}$ – $(k+1)$-розрядна мантиса доповняльного коду модуля P; b_i – поточне кодове значення залишку $(b_{i-1} = 0)$.

Функціональним обмеженням даного методу є наявність операцій додавання доповняльних кодів двійкового числа для визначення залишку по модулю P, що знижує швидкодію, тобто потребує n додавань n - розрядних чисел. Обчислювальна складність даного методу складе $O(n^2)$.

У [14] запропоновано метод пошуку залишку b_i двійкового числа $Y = \sum_{i=0}^{n-1} y_i 2^i$, який починається з його старшого розряду y_{n-1}, по модулю P, де y_i – значення i-го біта числа, в основу якого покладено рекурентне співвідношення:

$$b_i = (a_i + 2b_{i-1}) \bmod P_j, \quad (2)$$

де b_{i-1} – значення залишку $(i-1)$-го біта двійкового числа.

Двійковий код порозрядно зчитують, починаючи зі старших розрядів, підсумовують його з подвоєним кодом попереднього залишку, починаючи з його нульового значення та формують новий код залишку по модулю з постійної пам'яті, який після n повторень таких операцій зчитується як кінцевий код залишку, починаючи зі старшого розряду. Шуканий кінцевий залишок b_0 отримують згідно виразу $b_0 = resY (\bmod P)$, де *res* - символ операції визначення найменшого невід'ємного залишку. У випадку, якщо двійкове число буде займати 512 біт, а модуль, за яким обчислюють залишок, буде від 2 до 128 біт, то швидкодія в порівнянні з попереднім способом, зросте від 2-х до 48-ми разів.

Функціональним обмеженням даного алгоритму є постійне звертання до пам'яті, яке призводить до значних затрат часу, окрім лінійного зростання часової складності виконання операції міжбазисного перетворення Радемахера та десяткової системи числення пропорційно розрядності двійкових чисел, що обмежує можливості його використання при опрацюванні довгих чисел. Загальна часова складність запропонованого у роботі [14] методу складає $O1 = O(2n \cdot \log_2 n)$.

Загальний недолік розглянутих в [13, 14] схем пошуку залишків є отримання не завжди найменших залишків та надлишковість порівнянь.

В основу запропонованого методу покладено наступні ідеї. Якщо від числа Y відняти число, кратне модулю P, то його залишок по цьому модулю не зміниться. Та друга – у двійковій арифметиці множення на $2_{(10)}=10_{(2)}$ – це дописування нуля зправа до числа.

Для знаходження залишку L великого числа Y по великому цілочисельному модулю P подамо числа Y та P у вигляді:

$$Y = \sum_{i=0}^{n-1} y_i 2^i,\ де\ y_i = 0,1,\ P = \sum_{i=0}^{k-1} p_i 2^i,\ де\ p_i = 0,1.$$

Тут n – кількість цифр (знаків) числа, i – порядковий номер цифри.

Необхідно знайти $Y \bmod P = L$.

Виділяємо $(n-k-2)$ молодших розрядів числа Y і доповнюємо модуль нулями. Одержимо число S у двійковому поданні:

$$S = (p_{k-1}, p_{k-2}, ..., p_{0,} 0, ..., 0). \quad (3)$$

Якщо $(k-1)$ старших розрядів $Y \geq P$, знаходимо $Y \bmod S$, шляхом віднімання: $Y - S = M$. Подаємо число $M = \sum_{i=1}^{n-k-2} M_i 2^i$, , звідси

$$M = (M_{n-k-2}, M_{n-k-3}, ..., M_1, M_0). \quad (4)$$

Якщо $M \geq P$, то формуємо наступне число шляхом дописування в молодший розряд $P(n-2k-3)$ нулів – $L = (p_{k-1}, p_{k-2}, ..., p_{0,} 0, ..., 0)$.

Якщо $M \geq L$, то обчислюємо значення $M \bmod L = M - L$, де

$$U = (U_{n-2k-3}, U_{n-2k-4}, ..., U_1, U_0).$$

Якщо $U \geq P$, то дописуємо в молодший розряд $P(n-3k-4)$ нулів – $F = (p_{k-1}, p_{k-2}, ..., p_1, p_0, 0, ..., 0)$.

Якщо $U \geq F$, то обчислюємо значення $U \bmod F = U - F = H$.

Описану процедуру продовжуємо доти, доки двійкове число $H = (H_{n-3k-4}, H_{n-3k-5}, ..., H_1, H_0)$ не буде менше за P.

Для знаходження залишку числа обчислюємо:

$$Y \bmod P = U \bmod F = H.$$

Алгоритм знаходження залишку великого числа за певним модулем представимо такими кроками.

Вхід: Y, P.

Крок 1. Двійкове подання числа P: $P(p_n ... p_0)$.

Крок 2. Зменшення розрядності n подання числа P на кількість одиниць від p_n до p_i (поки $p_i = 0$), запис у двійкове число $K(k_m ... k_0)$.

Крок 3. Зміна $Y = Y - n - 1$.

Крок 4. Додавання числа K у двійковому поданні до числа P з урахуванням позиції бітів.

Крок 5. Зменшення бітової розрядності m числа K на кількість одиниць від k_m до k_i, і запис у число K.

Крок 6. Зміна $Y = Y - m - j$.

Крок 7. Перехід на крок 5, доки $Y \geq P$.

Вихід: $K = resY \bmod P$.

На рисунку 1 подано блок-схему алгоритму пошуку залишків великих чисел.

Основними перевагами даного алгоритму в порівнянні з описаними в роботах [13,14] є зменшення надлишкового використання пам'яті та кількості порівнянь, і зменшення кількості операцій додавання пропорційно розрядності чисел. Часова складність даного алгоритму становить $O2 = O(n \cdot \log_2 n)$.

На рисунку 2 представлено графічні залежності обчислювальних складностей методів, описаних в [13, 14], та запропонованого вище методу.

Ефективність алгоритмів пошуку залишків великих чисел в даній роботі оцінюється їх обчислювальною складністю. Виходячи з графіка, далі покажемо порівняння ефективностей методу з [14] та вищеописаного методу.

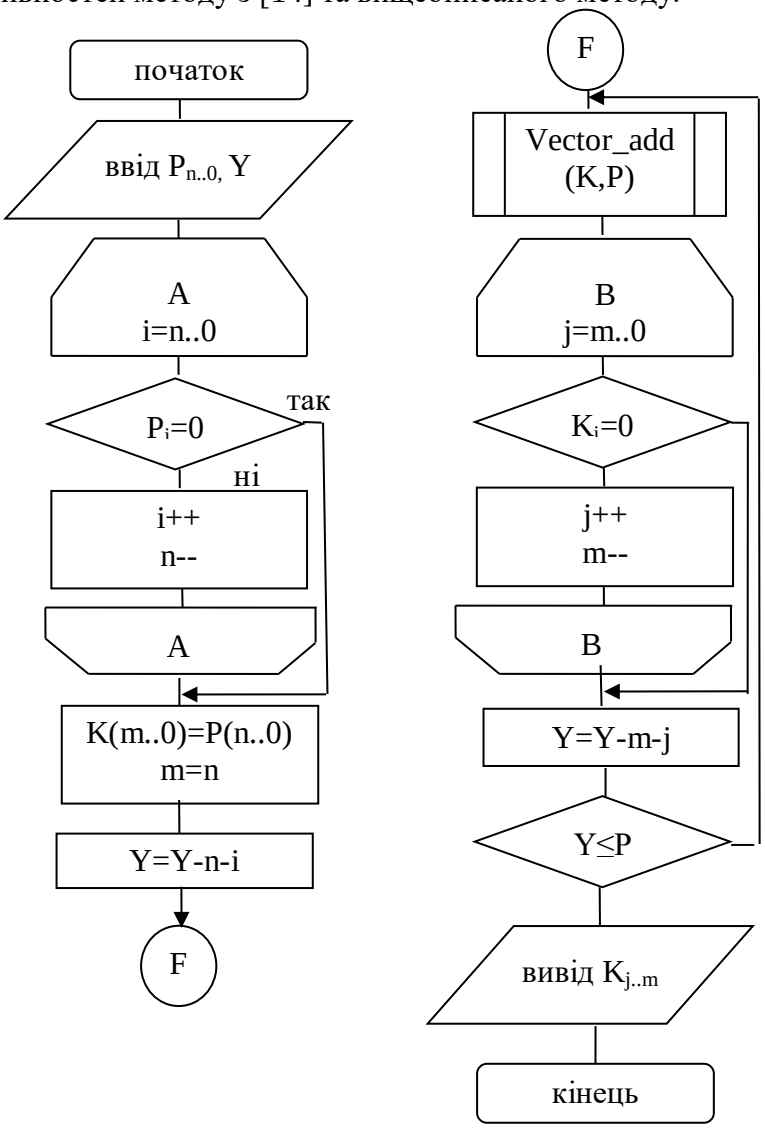

Рис. 1. Блок-схема алгоритму пошуку залишків довгих чисел

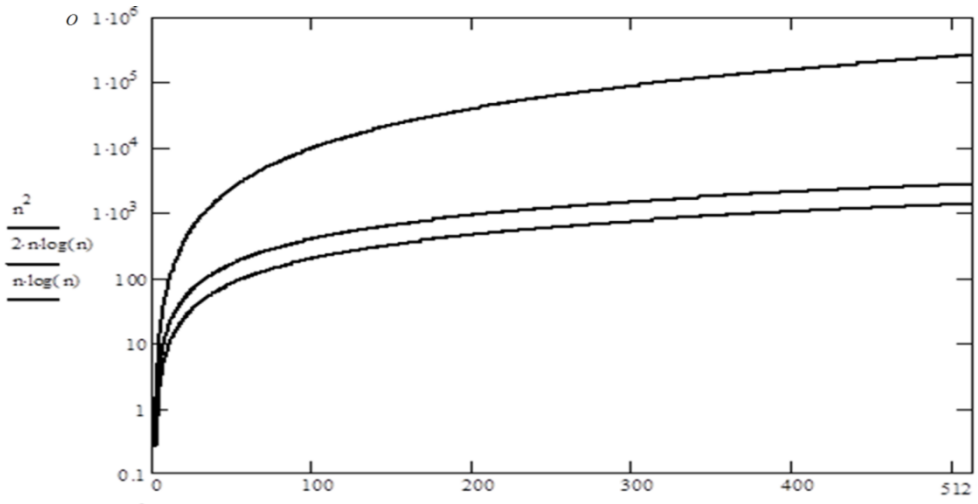

Рис. 2. Графічні залежності обчислювальних складностей відомих та запропонованого методу

Виграш в ефективності запропонованого в роботі алгоритму відносно відомого визначимо як співвідношення обчислювальних складностей:

$$E(n) = O1 / O2 = 2.$$

Отже, виграш в ефективності запропонованого методу при зростанні розрядності чисел зростає в 2 рази.

Чисельний експеримент оцінки складностей відомих і розробленого методу пошуку залишків великих чисел показує, що при виконанні модульних операцій, які використовуються в симетричних та асиметричних криптоалгоритмах, при переведенні чисел з десяткової системи числення в систему числення залишкових класів слід використовувати запропонований метод, який характеризується меншою складністю.

Оскільки при вирішенні окремих задач число операцій додавання може перевищити 2^{32}, то збільшення ефективності в два рази є суттєвим і значно розширює функціональні можливості опрацювання великих чисел.

Отже, розроблений метод з використанням операцій в числовому базисі Радемахера доцільно використовувати при опрацюванні інформаційних потоків, включаючи арифметичні операції та перевірку чисел на простоту, факторизацію та інші операції.

З метою забезпечення високої точності опрацювання інформації у базисах полів Галуа, необхідно вибирати великі значення простих модулів P, що задовольняють діофантовому рівнянню $2^q \equiv 1(2^q - 1)$, що приводить до арифметики по модулю $P = 2^k - 1$ і $P = 2^k + 1$. Такими числами є відомі числа Мерсенна $P = 2^q - 1$, де q – просте число, і Ферма $F_n = 2^{2^n} + 1$, де n – ціле число.

Для реалізації алгоритмів обрано мову програмування С++, середовище програмування С++ Buider 6.0. Додаток дозволяє дослідити часові характеристики виконання двох методів. Після запуску на екрані буде відображатись форма, що зображена на рисунку 3.

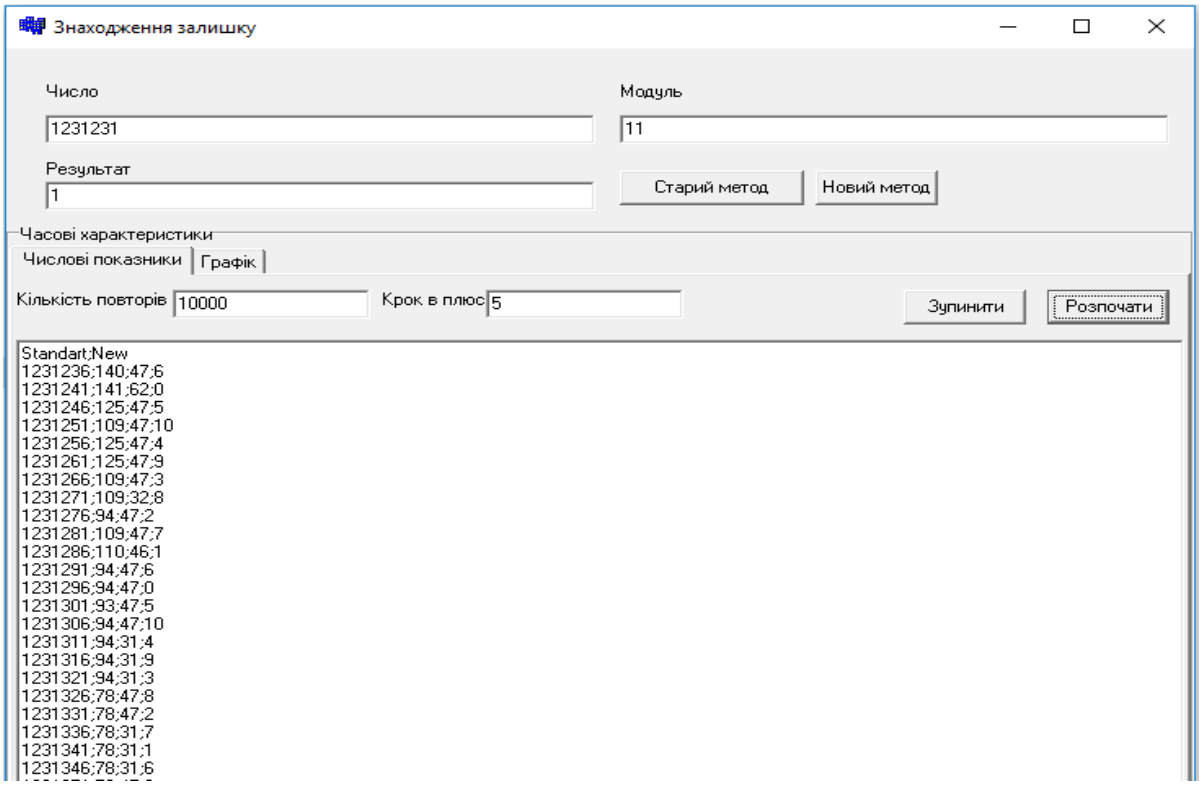

Рис. 3. Головна форма додатку

Додаток дозволяє порівняти швидкість виконання операцій знаходження залишку впорядкованої числової послідовності з випадково згенерованими модулями двома методами. Для аналізу та візуального порівняння одержаних часових характеристик роботи програми є можливість графічного відображення процесу. Верхню межу чисел можна вказати у відповідному полі головної форми.

Для проведення експериментів при дослідженні часових характеристик реалізована ітераційна затримка, оскільки процесорний час між потоками розподіляється нерівномірно. Контрольні дані відображаються на кожному кроці алгоритму знаходження залишку. Фрагмент тестування додатку для подвійних чисел Мерсенна показано в таблиці 1.

Таблиця 1.

Результати тестування для чисел Мерсенна

Число	Модуль	CLOCKS методу 1	CLOCKS методу 2
2^{32}-1	3811	62	31
2^{64}-1	3811	78	68
2^{128}-1	3811	78	63
2^{256}-1	3811	234	230
2^{512}-1	3811	1264	1092
2^{1024}-1	3811	4072	3120
2^{2048}-1	3811	14383	8674

У таблиці наведено CLOCKS двох методів – це кількість часових тактів з початку запуску програми.

Для тестування програмного продукту передбачено пошук залишку за вказаним модулем з певним кроком, який задається користувачем. На рис. 4 наведено графічне зображення залежності часу знаходження залишків великих чисел від номера по порядку наступного простого числа, для якого знаходиться залишок. Початкове число 1231231, за модулем 11, та кроком 5. Експеримент виконано для 1000 початкових чисел. Верхня ламана – для відомого алгоритму, нижня для запропонованого.

З рисунка видно, що час знаходження залишку за новим алгоритмом суттєво менший від відомого. Таким чином одержали експериментальне підтвердження теоретичним викладкам.

Висновки

У роботі проаналізовано відомі швидкодіючі алгоритми опрацювання великих чисел та запропоновано свої рішення для підвищення швидкодії; виконано порівняльний аналіз ефективності запропонованого і відомого методів; розроблено програмні засоби реалізації попередньо розглянутих алгоритмів та досліджено їх роботу.

Розроблений у результаті роботи алгоритм пошуку залишків великих чисел дозволив отримати підвищення швидкодії порівняно з відомим за рахунок використання властивостей залишків та числового базису Радемахера. Це значно зменшило обчислювальну складність та підвищило виграш у ефективності роботи алгоритму у порівнянні з відомим у два рази, що підтверджено експериментальними дослідженнями.

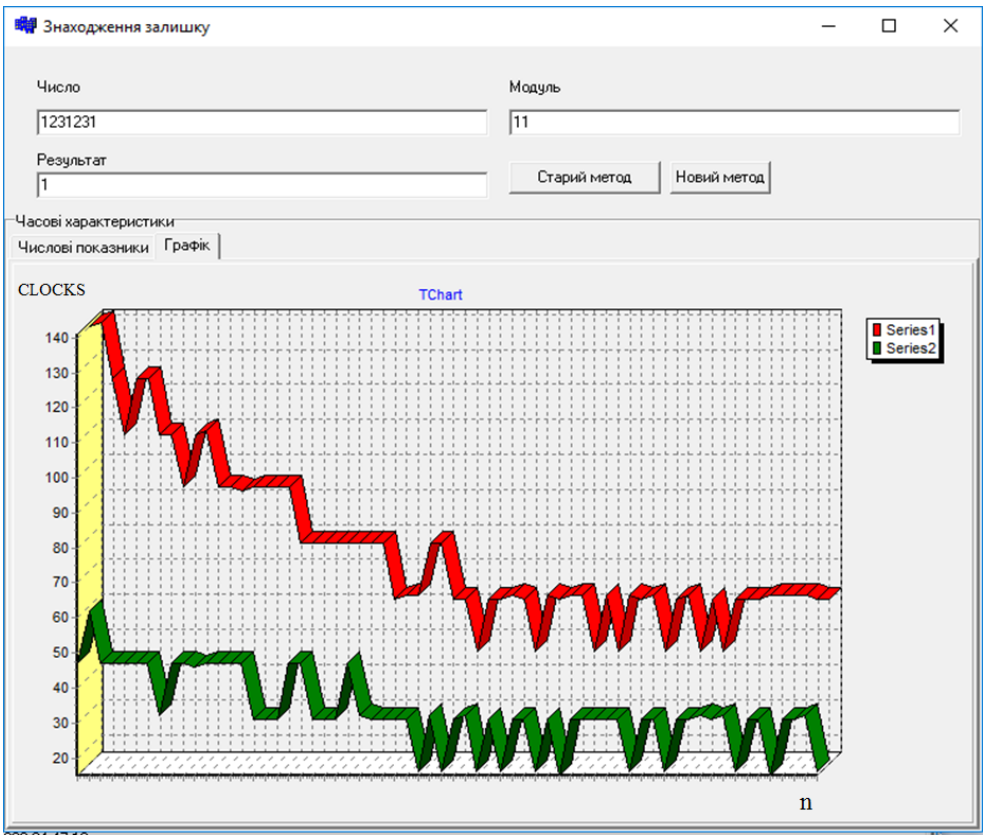

Рис. 4. Відображення залежності часу пошуку залишку числа від номеру

Отже, існує доцільність його використання при опрацюванні довгих чисел в асиметричних криптографічних системах захисту інформації для підвищення швидкодії процесів шифрування та криптоаналізу.

Список літератури

1. Розум, І.Ю. Застосування прикладної криптографії в системі військового управління в інтересах засекречування мереж зв'язку військового призначення // І.Ю. Розум // Збірник наукових праць НАДПСУ. Сер. : Військові та технічні науки. – 2013. – № 2. – С. 170-179.
2. Горбенко, А.Ю. Аналіз досвіду створення та бойового застосування систем оперативного управління / А.Ю. Горбенко, О.В. Головченко, М.Ю. Голобородько // Збірник наукових праць центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського. – 2017. – № 2. – С. 98-102.
3. Корченко, О.Г. Прикладна криптологія : системи шифрування : підручник / О.Г. Корченко, В.П. Сіденко, Ю.О. Дрейс. – К.: ДУТ, 2014. – 448 с.
4. Задірака В.К. Комп'ютерна криптологія: Підручник / В.К. Задірака, О.С. Олексюк. – Київ, 2002. – 504 с.
5. Kasyanchuk, M. Fundamental Backgrounds of the Discrete Logarithms Theory in the Rademacher-Krestensons Basis / M. Kasyanchuk, S. Ivasiev, I. Pazdriy, R. Trembach, I. Yakymenko // Proceedings of the XI-th International conference "Modern Problems of Radio Engineering, Telecommunications and Computer Science" (TCSET-2012). – Lviv-Slavsk. – 93 p.
6. Kozaczko, D. Vector Module Exponential in the Remaining Classes System / D. Kozaczko, I. Yakymenko, M. Kasianchuk, S. Ivasiev // Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2015). – Warsaw, Poland. – Vol. 1. – 2015. – Pp.161-163.
7. Тимошенко, Л.М. Удосконалення алгоритму факторизації для криптографічних систем захисту інформації / Л.М. Тимошенко, К.В. Вербик, С.В. Івасьєв // Сучасна спеціальна техніка. – 2014. – № 3(38). – С. 56-59.
8. Iakymenko, I. Construction of distributed thermal or piezoelectric sensor based on residue systems / I. Iakymenko, M. Kasianchuk, Ia. Kinakh, M. Karpinski // Przeglad Elektrotechniczny. – 2017. – No. 1. – Pp. 290-294.

9. Omondi, A. Residue number systems: theory and implementation / A. Omondi , B. Premkumar. – London: Imperial College Press, 2007. – 296 p.
10. Kasianchuk, M. Algorithms of findings of perfect shape modules of remaining classes system / M. Kasianchuk, I. Yakymenko, I. Pazdriy, O. Zastavnyy // Proceedings of the XIII-th International Conference "The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2015) ". – 2015. – Pp. 168-171.
11. Задірака, В.К. Комп'ютерна арифметика багаторозрядних чисел: Наукове видання / В.К. Задірака, О.С. Олексюк. – Київ, 2003. – 264 с.
12. Шумейко, О.О. Інформаційна безпека: Навч. посібник / О.О. Шумейко. – Дніпропетровськ: ДДТУ, 2012. – 144 с.
13. Патент на корисну модель № 68872. МПК G 06 F7/00. Пристрій визначення залишку багаторозрядного числа / Николайчук, Я.М., Якименко І.З., Воронич А.Р., Волинський О.І.; заявл. 10.04.2012.
14. Патент на корисну модель № 74576. Спосіб визначення залишку двійкового числа / Николайчук, Я.М., Волинський О.І.; заявл. 12.11.2012.

АЛГОРИТМЫ ПОИСКА ОСТАТКА ДЛИННЫХ ЧИСЕЛ ДЛЯ ЗАДАЧ АСИММЕТРИЧНОЙ КРИПТОГРАФИИ

Л.М. Тимошенко[1], Ю.М. Івасьев[2], О.Я. Лотоцкий[3], В.М. Гаврилей[1]

[1]Одесский национальный политехнический университет,
просп. Шевченко, 1, Одесса, 65044, Украина; e-mail: lmt0902@gmail.com
[2]Тернопольський национальный экономический университет,
ул. Львовская, 11, Тернополь, 46020, Украина; e-mail: stepan.ivasiev@gmail.com
[3]Национальний авиационный университет,
просп.Космонавта Комарова, 1, Киев, 03058, Украина, e-mail: zyzik2323@gmail.com

На современном этапе обеспечения информационной безопасности государства важно засекречивание сетей связи военного назначения, одним их ключевых направлений которого является применение криптографических методов защиты информации, в частности, асимметричной криптографии. Одним из путей совершенствования алгоритмов асимметричной криптографии является нахождение остатков длинных чисел. Известные алгоритмы поиска остатков длинных чисел имеют ряд существенных недостатков при их реализации. В работе проводится анализ заявленных двух новых методов поиска остатков длинных чисел, их недостатков и вычислительных сложностей. Описан предложенный авторами метод, приведены его алгоритм и блок-схема. Исследуются вычислительные сложности трех рассмотренных методов поиска остатков, численный эксперимент оценки сложностей показывает, что при выполнении модульных операций, которые используются в асимметричных криптоалгоритмах, при переводе чисел из десятичной системы в систему счисления остаточных классов следует использовать предложенный метод, который характеризуется меньшей сложностью. Для дальнейшего рассмотрения остаются два. Выигрыш в эффективности предложенного алгоритма относительно известного определяется как соотношение вычислительных сложностей и равен 2. Разработанное на языке программирования высокого уровня C++ приложение позволяет исследовать временные характеристики выполнения двух методов. В работе приведен фрагмент тестирования приложения для двойных чисел Мерсенна и графическое изображение зависимости времени нахождения остатков больших чисел от простого числа, для которого находится остаток. Разработанный алгоритм поиска остатков больших чисел позволил повысить быстродействие по сравнению с известным за счет использования свойств остатков и числового базиса Рademахера. Это уменьшило вычислительную сложность и повысило выигрыш в эффективности работы алгоритма по сравнению с известным в два раза, что доказывает целесообразность его использования при обработке длинных чисел в асимметричных криптографических системах защиты информации для повышения быстродействия процессов шифрования и криптоанализа.

Ключові слова: ассиметричная криптография, длинная арифметика, система остаточных классов, вычислительная сложность, остатки длинных чисел.

ALGORITHMS FOR SEARCHING LONG-TERM NUMBERS FOR THE TASK ASYMETRIC CRYPTOGRAPHY

L.M. Tymoshenko[1], S.V. Ivasiev[2], O.Y. Lototskyy[3], V.M. Gavriley[1]

[2] Odessa National Polytechnic University,
1 Shevchenko Ave., Odessa, 65044, Ukraine; e-mail: lmt0902@gmail.com
[1] Ternopil National Economic University,
11 Lvivska str., Ternopil, 46020, Ukraine; e-mail: e-mail: stepan.ivasiev@gmail.com
[3] National Aviation University,
1 Kosmonavtom Komarova Ave., Kiev, 03058 e-mail: zyzik2323@gmail.com

At the present stage of providing information security of the state, it is important to make secret military communication networks. One of the key areas to secret a network is the use of cryptographic methods for information protection, in particular, asymmetric cryptography. To improve asymmetric cryptography algorithms we can find the remains of long numbers. The implementation of known algorithms for finding the remains of long numbers has a number of significant drawbacks. The paper analyzes two new methods of finding long-numbered residues, their drawbacks, and computational complexities. The method proposed by the authors is described, its algorithm and block diagram are presented. The computational complexities of the three researched methods are studied. The numerical complexity evaluation experiment shows that when performing modular operations used in asymmetric cryptographic algorithms, when transferring numbers from the decimal system to the system of the numbers of residual classes, the proposed method should be used. The method has less complexity. There are two ways of further consideration. It is well-known that the algorithm effectiveness gain is equal to the ratio of computational complexity and equal 2. The application developed in the high-level programming language C ++ allows us to investigate the time characteristics of the two methods. In this paper, we give a fragment of the testing of the application for double Mersenne numbers and a graphic representation of the dependence of the time of finding the remnants of large numbers from the prime number for which the remainder is. The developed algorithm for finding the remnants of large numbers allowed to increase the speed compared to the known due to the use of the properties of residues and the numerical basis of Rademacher. This reduced the computational complexity and increased the efficiency of the algorithm compared with the known twice, which proves the expediency of its use in processing long numbers in asymmetric cryptographic information security systems to increase the speed of encryption and cryptanalysis.

Key words: asymmetric cryptography, long arithmetic, system of residual classes, computational complexity, remains of long numbers.