представляє інтерес ризикова модель загроз веб безпеки, оскільки одним із розумінь ризику є поєднання ймовірності та наслідків настання несприятливих подій.

Список використаних джерел:

1. Модель загроз у розподілених мережах [Електронний ресурс]. – Режим доступу: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/7538/09-Matov.pdf?sequence=1
2. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.
3. Офіційний сайт Web Application Security Consortium. [Електронний ресурс]. – Режим доступу: http://www.webappsec.org/
4. Створення моделі загроз інформації та механізму її ефективного захисту [Електроний ресурс] – Режим доступу: http://ena.lp.edu.ua:8080/bitstream/ntb/11750/1/11_stvorennya%20modeli.pdf
5. Анализ угроз информационной безопасности [Електронний ресурс]. – Режим доступу: https://www.anti-malware.ru/analytics/Threats_Analysis
6. Методология построения модели угроз безопасности территориально распределённых объектов Интернет-журнал «Технологии техносферной безопасности» (http://ipb.mos.ru/ttb) Выпуск No 2 (48), 2013 г
7 WEB applications security statistics report [Електронний ресурс]. – Режим доступу:https://info.whitehatsec.com/rs/675-YBI-674/images/WH-2016-Stats-Report

Якименко І.З.
кандидат технічних наук, доцент;
Мачуляк М.В.
студент,
Тернопільський національний економічний університет

МЕТОД ГЕНЕРУВАННЯ ПРОСТИХ ЧИСЕЛ НА ОСНОВІ ВИКОРИСТАННЯ СИСТЕМИ ЗАЛИШКОВИХ ФУНКЦІЙ

Сучасні комп’ютерні мережі та системи інтенсивно вдосконалюються на основі нових теоретичних положень опрацювання інформаційних потоків та програмно-апаратних засобів реалізації алгоритмів формування, перетворення, ідентифікація та покращення аутентифікації користувачів інформаційних систем [1]. При цьому, на сучасному етапі розвитку комп’ютерних систем виникає ряд проблем та науково-технічних задач пов’язаних з підвищенням інформаційної стійкості комп’ютерних систем, підвищення швидкодії алгоритмів шифрування/дешифрування а також створення відповідних програмно-апаратних та спецпроцесорних засобів опрацювання інформаційних потоків.

Досвід використання відомих алгоритмів шифрування та розвиток теорії алгоритмів , які широко застосовуються в практиці на основі важко оборотних функцій хешування, факторизації, модулярних та інших операцій вже

наблизилися до границь своїх потенційних можливостей і в загальному не можуть бути основою розвитку та вдосконалення засобів захисту інформаційних потоків в сучасних та проектованих комп'ютерних системах.

Однією з важливих задач в асиметричних системах захисту інформаційних потоків є генерування модуля криптоперетворення. Тому метою даної роботи є розробка ефективного методу генерування багаторозрядних простих чисел, на основі використання системи залишкових класів.

Система числення залишкових класів.

Фундаментальною теоретичною основою СЗК є алгебра і теорія чисел [2; 4; 5], зокрема китайська теорема про залишки [2]. Відомо, що будь-яке ціле додатнє число N у десятковій системі числення представляється в СЗК у вигляді набору $(b_1, b_2, \dots, b_n)_{p1, p2, \dots, pn}$ найменших додатніх залишків від ділення цього числа на фіксовані цілі додатні попарно взаємно прості числа p_1, p_2, ... , p_n (b_i=N mod p_i), які називаються модулями (n – кількість модулів) [4]. При цьому повинна виконуватись умова $0 \le N < P-1$, де $P=\prod_{i=1}^{n} p_i$.

Зворотнє перетворення із базису Крестенсона у десяткову систему числення грунтується на використанні китайської теореми про остачі і є досить складним та громіздким [4]: $N=\left(\sum_{i=1}^{n} b_i B_i\right) mod P$, де $B_i=M_i m_i$, $M_i=\frac{P}{p_i}$, m_i шукається з виразу $(M_i m_i) mod\, p_i = 1$, при цьому повинна виконуватись умова $\left(\sum_{i=1}^{n} B_i\right) mod P = 1$.

Слід зазначити, що пошук коефіцієнтів $m_i = M_i^{-1} mod\, p_i$ становить значну обчислювальну складність, оскільки для знаходження оберненого елемента потрібно використовувати алгоритм Евкліда із виконанням не більше 5k операцій ділення з остачею, де k – кількість цифр в десятковому записі меншого з чисел.

Досить перспективними модифікаціями СЗК, які на даний час глибоко досліджуються, є розроблена досконала цілочисельна ($m_i = 1$), напівдосконала ($m_i = \pm 1$), нормалізована та розмежована форми СЗК [4; 5].

Алгоритм ідентифікації простого числа з використанням СЗК

Для генерування простого числа можна скористатися розробленим алгоритмом, який дозволяє ефективно шукати прості числа.

Алгоритм – пошук найбільшого простого числа.

1. Маємо останнє просте число $p_i - \max$.

2. Визначаємо двійкове представлення цього числа n – розрядів.

3. Через розмежовану систему числення залишкових класів та властивість періодичності рекурентним шляхом отримуємо залишок числа p_i по заданому модулю, наступним чином:

$$\begin{cases} c_{i+1} = c_i \cdot 2(\text{mod } p), c_1 = 1, a_1 = 1 \\ b_{i+1} = (c_{i+1} \cdot a_i + b_i) \text{ mod } p, b_1 = 1, i = 1, a_i = 0,1 \end{cases}. \quad (1)$$

Програмним шляхом організовуємо генератор залишків по модулю p_j. В результаті знаходимо зображення цього числа в СЗК до числа простих чисел, які не перевищують $\sqrt{p_i}$ – половина розряду p_i.

4. Додаємо до залишків число 2 по всіх модулях, ця операція припиняється, коли по одному з модулів отримаємо 0. Тоді пропускаємо числа, кратні модулю, по якому залишок дорівнює 0. Операцію повторюємо до тих пір, поки не буде знайдено найбільше просте число.

Основною перевагою даного алгоритму є те, що операції виконуються тільки над залишками, а не з великими простими числами. Отже, для генерування p можна скористатися алгоритмом, який дозволяє спростити процедуру знаходження простого числа. Структура програмного забезпечення даного алгоритму базується на запропонованих теоретичних викладках і зображена на рисунку 1. Основними перевагами даного алгоритму ідентифікації простого числа n є використання системи залишкових класів по всіх простих модулях до $\sqrt{n}+1$. Якщо один з залишків рівний нулю, то до залишків додаємо 2 по всіх модулях. Ця операція припиняється коли по одному з модулів отримаємо 0. Тоді пропускаємо числа кратні модулю, по якому залишок 0, і знаходимо послідовність простих чисел. Це дозволяє значно зменшити складність алгоритму пошуку простих чисел за рахунок введення циклу D.

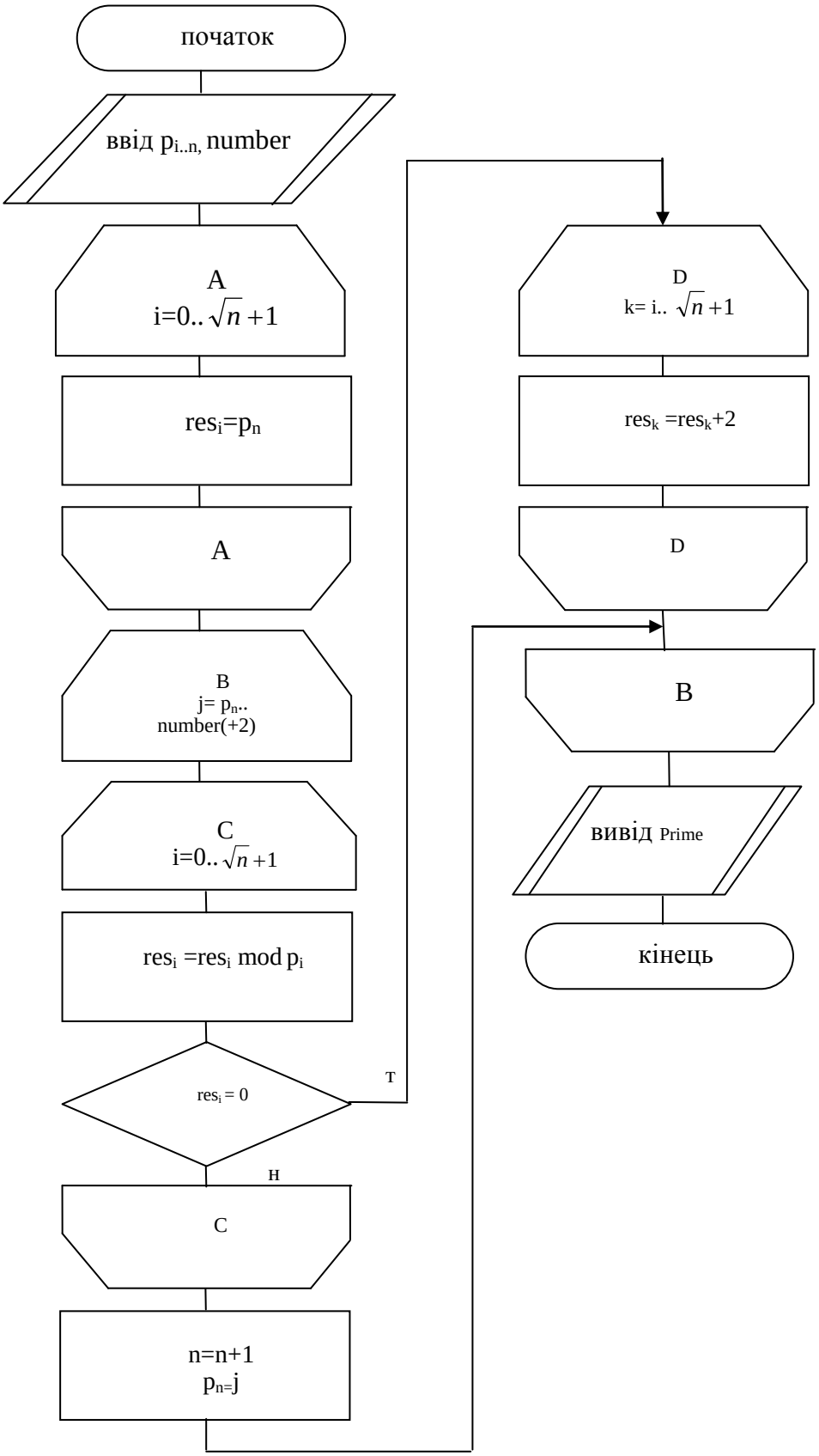

Рис. 1. Блок-схема алгоритму генерування простого числа з використанням базису Крестенсона

Особливості даної структури, яка по ефективності переважає відомі алгоритми завдяки введенню блоку швидкого перетворення з базису Рademахера в базис Крестенсона та модуля пошуку залишків в розмежованій системі числення.

Алгоритм дозволяє оперативно обчислювати прості числа в діапазоні до 2^{256} за 60 с, а в діапазоні 2^{512} за 180 с.

В роботі запропоновано метод генерування багато розрядних простих чисел на основі використання системи залишкових чисел, який завдяки введенню блоку швидкого перетворення з базису Рademахера в систему залишкових класів та модуля пошуку залишків в розмежованій системі числення дозволяє оперативно обчислювати прості числа в діапазоні до 2^{256} за 60 с, а в діапазоні 2^{512} за 180 с.

Список використаних джерел:

1. W. Stallings. «Cryptography and Network Security: Principles and Practice». 5th Prentice Hall Press Upper Saddle River, NJ, USA. – 2010. – 719 p.

2. Omondi, B. Premkumar. «Residue Number System: Theory and Implementation». Imperial College Press, 2007,Vol. 2, 296 p.

3. M.M. Kasianchuk, Ya. M. Nykolaychuk, I. Z. Yakymenko «Theoretical Foundations of the Modified Perfect form of Residue Number System». Cybernetics and Systems Analysis, 2016, p. 219-223.

4. M. N Kasianchuk, Ya. N Nykolaychuk, I.Z. Yakymenko. «Theory and Methods of Constructing of Modules System of the Perfect Modified Form of the System of Residual Classes». Journal of Automation and Information Sciences. 2016, Vol.48, №8, p. 56-63.

5. Sachenko, V. Yatskiv, R. Krepych, A. Karachka. «Data Encoding in Residue Number System». Proceeding of the International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: IDAACS‘2009, 2009, p. 679–681.