УДК 004.056.55

В. Л. Поліщук[1]
Р. С. Белзецький[1]

ПРОГРАМНА РЕАЛІЗАЦІЯ АЛГОРИТМУ ГЕНЕРАЦІЇ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ ТА БІНАРНИХ ПОСЛІДОВНОСТЕЙ

[1] Вінницький національний технічний університет.

Анотація

Робота присвячена розробці програмного засобу генерації псевдовипадкових чисел (ПВЧ) та псевдовипадкових бітових послідовностей (ПВБП), на основі алгоритму BBS. З можливість додаткової пост обробки результатів, що базується на методі ініціалізації S-блоку потокового алгоритму RC-4 (KSA).

Ключові слова: псевдовипадкова бітова послідовність, генератори псевдовипадкових чисел, алгоритм BBS, S-блок.

Abstract

The work is devoted to the development of a software tool for generating pseudorandom numbers (PRNG) and pseudorandom bit sequences (PRBS) based on the BBS algorithm. With the possibility of additional post-processing of the results based on the method of initialisation of the S-block of the RC-4 streaming algorithm (KSA).

Keywords: pseudorandom bit sequence, pseudorandom number generators, BBS algorithm, S-block.

Вступ

Генератори псевдовипадкових чисел і псевдовипадкових бітових послідовностей часто зустрічається в багатьох областях захисту даних, для генерації ключів, одноразових паролів, сольових значень тощо [1, 2].

При цьому вимоги до їх технічних характеристик відрізняються в залежності від мети їхнього застосування.

До основних характеристик, що має забезпечити генератор ПВБП та ПВЧ належать:

Статистична випадковість – послідовність повинна відповідати певним критеріям випадковості, таким як рівномірний розподіл, відсутність очевидних закономірностей і кореляцій.

Відтворюваність – якщо використовується той самий початковий стан, генератор створює ту саму послідовність.

Довгий період повторення – хороший генератор має великий період перед тим, як послідовність почне повторюватися.

Однорідність і непередбачуваність – особливо важливо для криптографічних застосувань, де послідовність повинна бути складною для прогнозування.

Відомо, що при реалізації криптографічних перетворень використовують різні псевдовипадкові послідовності. Звідси випливає, що стійкість криптоперетворень безпосередньо залежить від алгоритму формування псевдовипадкових чисел та послідовностей [3].

Метою цієї роботи є розробка програмного засобу, для реалізації алгоритму генерації псевдовипадкових чисел та псевдовипадкових бітових послідовностей на основі алгоритму BBS з можливістю додаткової пост обробки на основі алгоритму ініціалізації S-блок потокового алгоритму RC-4 (KSA).

Результати досліджень

Програмний продукт є десктопним додатком, що встановлюється нативним застосунком на операційні системи Windows. Програму реалізовано мовою програмування Java з використанням платформи для розробки десктопних додатків JavaFX.

Основні характеристики та переваги Java:

Платформонезалежність – програми, написані на Java, можуть запускатися на різних операційних системах, таких як Windows, macOS, Linux та інших, без потреби в перекомпіляції.

Об'єктно-орієнтований підхід – Java підтримує ключові принципи ООП, зокрема спадкування, поліморфізм, інкапсуляцію та абстракцію, що сприяє зручності розробки та масштабованості коду.

Розширена стандартна бібліотека – мова містить велику кількість вбудованих бібліотек, які забезпечують широкий набір функцій, зокрема для роботи з мережею, введенням-виведенням та обробкою даних.

Безпека – Java має вбудовану систему безпеки, що дозволяє контролювати доступ до ресурсів та захищати програми від небезпечного виконання.

Мультипотоковість – Java надає вбудовану підтримку для паралельного виконання завдань.

В ході розробки програмного комплексу було проведено аналіз вимог, що включав вивчення потреб користувачів і формулювання функціональних та нефункціональних вимог. На основі даного аналізу розроблено загальну концепцію системи, яка визначає її мету та завдання, орієнтовані на вирішення визначених вимог.

Особлива увага приділена проектуванню архітектури системи, визначенню компонентів, їх структури та взаємозв'язків.

Застосовано UML-діаграми для візуалізації структури та функціональності системи, що сприяє кращому розумінню взаємодії її компонентів.

Рисунок 1 – UML-діаграма класів для розроблюваного програмного продукту

Остаточним етапом стало розроблення плану, який містив графік виконання робіт, розподіл обов’язків і визначення контрольних точок для успішної реалізації проекту.

Інструкція по встановленню програми на ОС Windows

Для встановлення потрібно щонайменше 340 МБ вільного місця в пам’яті.

1. Запустити візард встановлення, двічі натиснувши ліву кнопку миші по виконавчому файлі «generator-setup.exe».

2. Вибрати мову, що буде використовуватись в процесі встановлення, а також директорію, куди буде встановлено додаток. За замовчуванням це папка: C:\Program Files (x86).

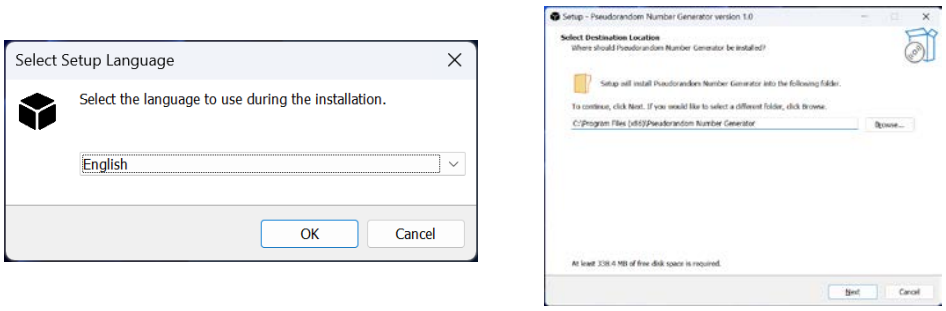
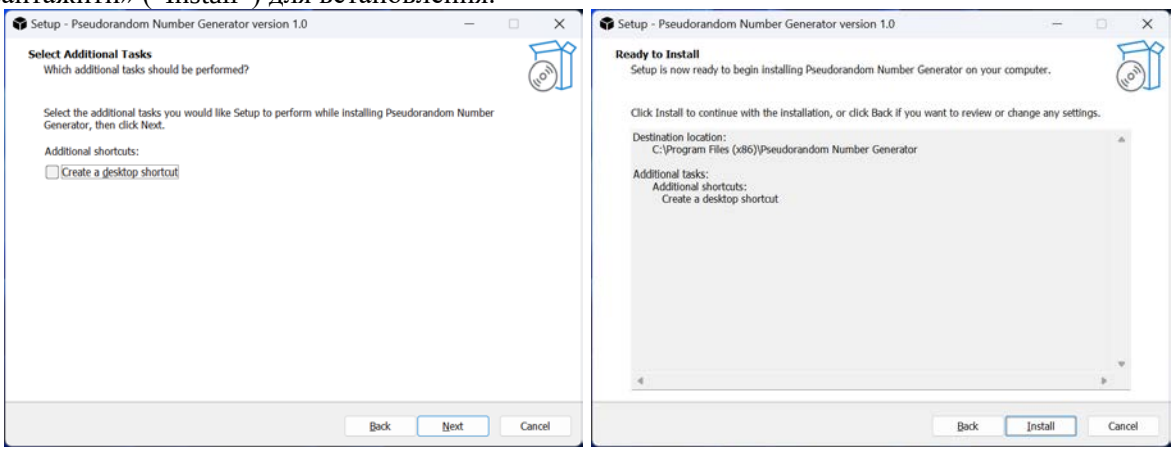


Рисунок 2 – Вибір мови та папки встановлення

3. Вказати необхідність створення ярлика програми на робочому столі та натиснути кнопку «Завантажити» (“Install”) для встановлення.



Рисунки 3 – Створення ярлику та підтвердження налаштувань

Приклад використання програми

Програма володіє інтуїтивно зрозумілим та простим користувацьким інтерфейсом. Початкова сторінка містить поля для конфігурації параметрів генерації псевдо випадкових послідовносте (рисунок 4).

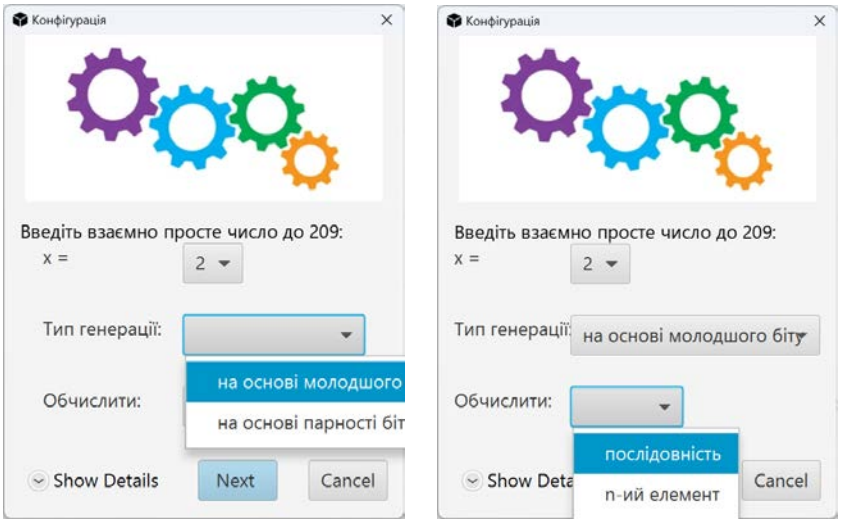


Рисунок 4 – Діалогове вікно конфігурації

За потреби в поясненні параметрів налаштування, користувач може ознайомитися з деталями, натиснувши кнопку “Show Details”.

Якщо користувач вирішив обчислити послідовність, то натиснувши “Next”, програма перейде до наступної сторінки. На цій сторінці потрібно вказати розрядність бінарної послідовності, яку користувач бажає згенерувати. Також, якщо була обрана додаткова обробка, то необхідно вказати розмірність блоку, в межах якого здійснюється додаткова перестановка бінарної послідовності.

При генерації кожної послідовності відбувається запис згенерованих даних до текстового файлу, що буде створено в директорії C:\Users\<username>\AppData\Local\Pseudorandom Number Generator.

Висновки

Отже, результатом виконання поставленого в роботі завдання є програмний комплекс, що реалізує алгоритм генерації псевдовипадкових чисел та псевдовипадкових бітових послідовностей, на основі алгоритму BBS, з можливістю додаткової пост обробки для підвищення рівномірності розподілу та мінімізації очевидних закономірностей вихідної послідовності.

У програмі реалізовано інтуїтивно зрозумілий та простий користувацький інтерфейс для конфігурації параметрів генератора.

За результатами даної програмної реалізації було отримане свідоцтво про реєстрацію авторського права на твір [4].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Белзецький Р. С. Обґрунтування вибору генератора псевдовипадкових величин для потокового шифрування аудіоповідомлення [Електронний ресурс] / Р. С. Белзецький, Медяна І. Л.// Матеріали XLIX науково-технічної конференції підрозділів ВНТУ, Вінниця, 27-28 квітня 2020 р. – Електрон. текст. дані. – 2020. – Режим доступу: https://conferences.vntu.edu.ua/index.php/all-fksa/all-fksa-2020/paper/view/9593.
2. Зуєв А. О., Караман Д. Г. Програмна реалізація спеціалізованих алгоритмів генерації псевдовипадкових чисел на платформах для вбудованих систем. Системи управління, навігації та зв'язку. 2023. № 74 С. 85–90. DOI: https://doi.org/10.26906/SUNZ.2023.4
3. Шевчук М. С., Мандрона М. М., Максимович В. М. Дослідження генератора псевдовипадкових бітових послідовностей Джиффі на основі FCSR. Міжнародний науковий журнал "Інтернаука". 2018. № 19. С. 130–135.
4. Свідоцтво про реєстрацію авторського права на твір № 1132658 від 13 січня 2025 р. «Комп`ютерна програма «Генератор псевдовипадкових чисел»»/ Белзецький Р. С., Поліщук В. Л. ДО «Український національний офіс інтелектуальної власності та інновацій» (УКРНОІВІ). – 2 с.

Поліщук Володимир Леонідович – студент групи 1КН-21б, кафедри комп'ютерних наук, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, м. Вінниця.

Белзецький Руслан Станіславович – канд. техн. наук, доцент, доцент кафедри комп'ютерних наук, Вінницький національний технічний університет, e-mail: belzetskiy@vntu.edu.ua.

Polishchuk Volodymyr L. – student of the 1KN-21b group, Department of Computer Science, Faculty of Intelligent Information Technologies and Automation, Vinnytsia National Technical University, Vinnytsia, Ukraine.

Belsetskyi Ruslan S. — PhD (Eng.), Assosiate Professor of Department for Computer Science, Vinnytsia National Technical University, Vinnytsia, email: belzetskiy@vntu.edu.ua.