

Міністерство освіти і науки України

Державний вищий навчальний заклад
«Донецький національний технічний університет»



«ТАК»

Телекомунікації, автоматизація,
комп'ютерно-інтегровані та інформаційні технології

Збірка доповідей Всеукраїнської науково-практичної
конференції молодих учених
(Луцьк, 5-6 грудня 2023 р.)

Луцьк
ДВНЗ «ДонНТУ»
2023

Рекомендовано до видання Вченою радою ДВНЗ «Донецький національний технічний університет»

Редакційна колегія:

Вікторія Воропаєва, к.т.н., проф., в.о. проректора з науково-педагогічної роботи ДонНТУ;

Гліб Ступак, ст. викл. кафедри автоматики та телекомунікацій, керівник мережної академії Cisco ДонНТУ, голова клубу підприємництва YEP!Club DNTU;

Валерій Поцєпаєв, к.т.н., доц., завідувач кафедри автоматики та телекомунікацій ДонНТУ;

Наталія Маслова, к.т.н., доц., завідувачка кафедри прикладної математики і інформатики ДонНТУ;

Сергій Ковальов, к.т.н., доц., в.о. завідувача кафедри електронної техніки ДонНТУ;

Олександр Колларов, к.т.н., доц., завідувач кафедри електричної інженерії ДонНТУ;

Едуард Петелін, к.т.н., доц., декан факультету комп'ютерно-інформаційних технологій та автоматизації ДонНТУ;

Володимир Ставицький, к.т.н., інженер-програміст вбудованих систем, ТОВ «РЗА СИСТЕМЗ»;

Семен Батир, к.т.н., провідний інженер-розробник Ring Ukraine.

Відповідальність за зміст, новизну та оригінальність наданого матеріалу несуть автори.

Т 15 **«ТАК»:** телекомунікації, автоматика, комп'ютерно-інтегровані технології: зб. доповідей Всеукр. наук.-практ. конф. молодих вчених, 5-6 грудня 2023 р. / ДВНЗ «ДонНТУ»; відп. ред. Г.В. Ступак. – Луцьк: ДВНЗ «ДонНТУ», 2023. – 202 с.

До збірника увійшли матеріали доповідей, представлених на Всеукраїнській науково-практичній конференції молодих учених «ТАК»: телекомунікації, автоматика, комп'ютерно-інтегровані технології. Конференція проводилася кафедрою автоматики та телекомунікацій (АТ) ДВНЗ «Донецький національний технічний університет».

У збірнику представлені результати досліджень та розробок молодих вчених із технічних вузів та наукових закладів України.

Збірник призначений для викладачів, аспірантів і студентів вищих технічних навчальних закладів, а також фахівців з телекомунікацій, автоматизації, інформаційних та комп'ютерно-інтегрованих технологій, електротехніки та електромеханіки.

УДК 621.39+681+004

© ДВНЗ «ДонНТУ», 2023

ПРОГРАМНИЙ ЗАСТОСУНОК ДЛЯ ГЕНЕРАЦІЇ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ ВИСОКОЇ СТІЙКОСТІ

Рудської М.О.¹, студент гр. КІБ-20, mykyta.rudskoi.kita@donntu.edu.ua;

Мороз Є.З.¹, студент гр. КІБ-20, yevhen.moroz.kita@donntu.edu.ua;

Алтухова Т.В.¹, к.т.н., tetiana.altukhova@donntu.edu.ua

¹ Державний вищий навчальний заклад «Донецький національний технічний університет», Луцьк, Україна

З сьогоденним розвитком у сферах криптографії і інформаційної безпеки саме генерація псевдовипадкових чисел високої стійкості вважається однією з важливих і невід'ємних складових в багатьох застосуваннях. Загалом псевдовипадкові числа застосовуються для шифрування даних, генерації ключів, створення електронних підписів та багатьох інших криптографічних операцій. Проте, звичайні алгоритми генерації випадкових чисел, що ґрунтуються, переважно, на детермінованих виразах або недостатньо складних алгоритмах, можуть бути вразливими до криптоаналітичних атак і, в свою чергу, не забезпечують необхідний рівень стійкості. З огляду на це, для забезпечення необхідного рівня безпеки, використовуються різноманітні методи генерації псевдовипадкових чисел високої стійкості, які базуються на складних математичних алгоритмах, криптографічних протоколах та застосуванні криптографічно стійких функціях, що, в свою чергу, надають гарантію того, що послідовності псевдовипадкових чисел будуть максимально незалежними, непередбачуваними і важкими для порушників безпеки.

З вище наведеного видно, що головна мета методів генерації псевдовипадкових чисел високої стійкості полягає у забезпеченні надійності та конфіденційності криптографічних систем, тим самим забезпечуючи захищені комунікації, збереження конфіденційної інформації та здійснення безпечних операцій з даними.

Зараз існує багато різних методів генерації псевдовипадкових чисел, до яких відносять хеш-функції, шумові генератори, блочні шифри та методи, що ґрунтуються на фізичних процесах, наприклад, шум радіодіапазону або квантові ефекти. Тому дослідження та розвиток методів генерації псевдовипадкових чисел високої стійкості є постійним завданням для криптографічних дослідників і фахівців з інформаційної безпеки, а забезпечення стійкості і надійності цих методів є критичним для забезпечення безпеки наших особистих даних, фінансових транзакцій, мережевих комунікацій та інших важливих аспектів нашого цифрового життя. Враховуючи це, саме розробка надійного та ефективного методу генерації псевдовипадкових чисел високої стійкості, який дозволить забезпечити непередбачуваність та випадковість генерованих чисел задля необхідного високого рівня безпеки та конфіденційності, вирішить основні проблеми інформаційної безпеки.

Для розробки програмного застосунку для генерації псевдовипадкових чисел високої стійкості, який дозволить створення випадкових та унікальних значень, що зможуть використовуватися для шифрування, розшифрування, електронних підписів та інших криптографічних операцій забезпечити криптографічну стійкість, застосовували об'єднання двох методів генерації, а саме лінійний конгруентний та метод регістрів зсуву.

На даний час лінійний конгруентний метод вважається одним з найпоширеніших методів генерації псевдовипадкових чисел (ПСЧ), який ґрунтується на ітеративному виразі, що генерує послідовність чисел з властивістю псевдо випадковості:

$$X_n = (a \cdot X_{n-1} + c) \bmod m \quad (1)$$

X_n - поточне число у послідовності;

X_{n-1} - попереднє число у послідовності;

a, c, m - параметри методу, які впливають на характеристики генерованих чисел.

Для коректної роботи даного методу, в першу чергу, виникає необхідність обирати відповідні значення параметрів a, c і m , від яких залежить отримання високої якості псевдовипадкових чисел.

Якщо розглядати алгоритм методу регістрів зсуву, то необхідно враховувати основні кроки, які наведені на рис. 1.



Рисунок 1. Основні кроки алгоритму методу регістрів зсуву

На рис. 2 представлений інтерфейс програмного застосунку на основі комбінації вище наведених методів генерації ПВЧ.

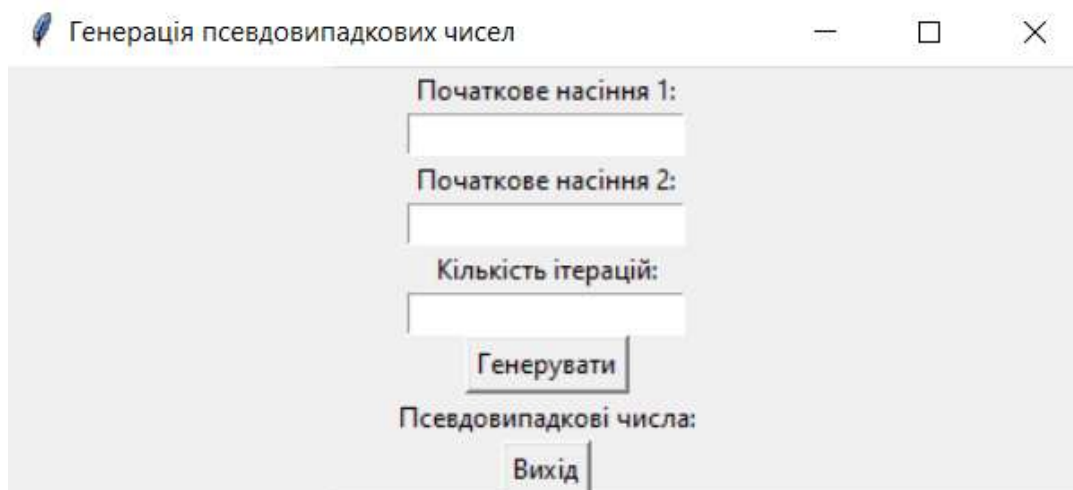


Рисунок 2. Інтерфейс розробленого додатку для генерації псевдовипадкових чисел

В програмі комбінація даних методів забезпечується використанням операції XOR наступним чином: у функції `generate_random_numbers` кожної ітерації генерується число з допомогою лінійного конгруентного методу (`lcg.next()`) і число з допомогою методу з урахуванням регістру зсуву (`shift_register.next()`), потім обидва генерованих числа комбінуються за допомогою операції XOR (`lcg_output ^ shift_register_output`), і, надалі, результат буде додаватися до списку `random_numbers`. Операція XOR виконує побітове виключення АБО між двома числами. Якщо відповідні біти в числах різні, тобто один біт 0, а інший біт 1, то результат буде 1, в іншому випадку - 0. Це дозволяє комбінувати псевдовипадкові числа, отримані з різних методів, для створення нової послідовності псевдовипадкових чисел з урахуванням їх відмінностей.

Таким чином, в результаті виконання функції `generate_random_numbers` буде отримана послідовність псевдовипадкових чисел, яка буде об'єднувати вклади обох методів, що дозволить їх широке застосування в різних, де вимагається безпека, непередбачуваність та стохастичність, в тому числі задля захисту інформації, надійності криптографічних систем та точність моделювання. Дослідження криптографічної стійкості виконувалося на основі тестування статистичних властивостей отриманих псевдовипадкових чисел, а саме визначалося, що застосунок на основі комбінації методів здатен генерувати значення з приблизно однаковою ймовірністю на всьому діапазоні можливих значень:

$$P(X = x) = \frac{1}{b - a}, \text{ якщо } a \leq x \leq b \quad (1)$$

$P(X = x)$ - ймовірність того, що змінна X набуде значення x .

Література

1. Подорожняк А. О. Метод генерації псевдовипадкових чисел високої стійкості / А. О. Подорожняк, М. Г. Токарев // Вісник Нац. техн. ун-ту "ХПІ" : зб. наук. пр. Сер. : Інформатика та моделювання. – Харків : НТУ "ХПІ", 2017. – № 50 (1271). – С. 36-45.
2. Математичні основи криптографії: конспект лекцій / укладачі: В. А. Фільштинський, А. В. Бережний. – Суми: Сумський державний університет, 2011. – 138 с.
3. С.О. Сушко, Г.В. Кузнецов, Л.Я. Фомичова, А.В. Корабльов. Математичні основи криптоаналізу. - Д.: Національний гірничий університет, 2010. – 465 с.
4. Прикладна криптологія : системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – Житомир : ДУТ, 2014. - 448 с.
5. Дональд Еге. Кнут. Глава 3. Випадкові числа // Мистецтво програмування. The Art of Computer Programming. - 3-тє вид. - М.: Вільямс, 2000. - Т. Отримані алгоритми. - 832 с. - 7000 прим. - ISBN 5-8459-0081-6
6. М. А. Іванов, І. В. Чавунков. Розділ 4. Методика оцінки якості генераторів ПСП // Теорія, застосування та оцінка якості генераторів псевдовипадкових послідовностей. - М.: Кудиць-Образ, 2003 - 240 с. ISBN 5-93378-056-1
7. Класичні методи криптології: методичні рекомендації для здобувачів спеціальностей «Прикладна математика» та «Системний аналіз» / М.М. Повідайчик, І.Я. Шпонтак. - Ужгород: Видавництво УжНУ «Говерла», 2020. - 28 с.

Анотація

В роботі розглянуто питання розробки та програмної реалізації програмного застосунку на основі комбінації методів генерації псевдовипадкових чисел високої стійкості задля надійного і ефективного забезпечення необхідного рівня криптографічної стійкості при шифруванні, розшифруванні інформації, створенні і використанні електронних підписів та інших криптографічних операцій.

Ключові слова: генерація, псевдовипадкові числа, криптографічна стійкість, лінійний конгруентний метод, метод регістрів зсуву, алгоритм.

Abstract

The paper considers the development and software implementation of a software application based on a combination of methods for generating pseudorandom numbers of high stability to reliably and efficiently ensure the required level of cryptographic security when encrypting, decrypting information, creating and using electronic signatures and other cryptographic operations.

Keywords: generation, pseudorandom numbers, cryptographic strength, linear congruent method, shift register method, algorithm.

ЗМІСТ

СЕКЦІЯ 1. «Інформаційні технології, телекомунікації та кібербезпека»....	3
ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ПАРАЛЕЛЬНИХ МЕТОДІВ РОЗВ'ЯЗАННЯ ЖОРСТКИХ ЗАДАЧ КОШІ, Назарова І.А., Бервін М.С.	4
КОНФІДЕНЦІЙНІСТЬ ДАНИХ У МЕДИЧНИХ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ І ЗАСОБИ ЇЇ ЗАБЕЗПЕЧЕННЯ, Ковальчук В.І.....	7
АНАЛІЗ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, Тютюнник М.В., Мороз Є.З., Рудської М.О., Маслова М.О.,	11
РОЗРОБКА СИСТЕМИ КОМПЛЕКСНОГО ОЦІНЮВАННЯ ПРОДУКТИВНОСТІ РОЗРОБНИКІВ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ, Криволап В.В., Алтухова Т.В.....	14
УДОСКОНАЛЕНИЙ МЕТОД ВИБОРУ МАРШРУТУ В БЕЗДРОТОВИХ МЕРЕЖАХ НА ОСНОВІ ВИКОРИСТАННЯ ANFIS, Здоренко Ю.М., Поляков О.Л., Гуска В.А.....	18
МІЖДИСЦИПЛІНАРНІ АСПЕКТИ АНАЛІЗУ РОЙОВОЇ ПОВЕДІНКИ Байтельман Я.Л.....	21
ІНТЕРАКТИВНІ ІДЕЇ ДЛЯ НАВЧАННЯ, Коверсун Д.В., Любименко О.М., Штепа О.А.	24
ВИЛУЧЕННЯ ІНФОРМАЦІЇ З ОСВІТНІХ ДЖЕРЕЛ НА ОСНОВІ NATURAL LANGUAGE PROCESSING, Худік Б.О., Золотухіна О.А....	27
ЗАСТОСУВАННЯ МЕРЕЖ ПЕТРІ В ПРОЦЕСІ ДОСЛІДЖЕННЯ ВПЛИВУ ІНФОРМАЦІЙНИХ ЗАГРОЗ, Мерзлікін В.В., Алтухова Т.В.	30
ПРОГРАМНИЙ ЗАСТОСУНОК ДЛЯ ГЕНЕРАЦІЇ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ ВИСОКОЇ СТІЙКОСТІ, Рудської М.О., Мороз Є.З., Алтухова Т.В.	33
РОЗРОБКА МОДЕЛІ ЗАХИСНОГО МЕХАНІЗМУ ОПЕРАЦІЙНИХ СИСТЕМ, Пономаренко В.В., Паращевін М.М., Алтухова Т.В.	37
ВПЛИВ ЗОВНІШНІХ ФАКТОРІВ НА ПРОЦЕС ДЕТЕКЦІЇ СИГНАЛІВ В ГЛИБОКИХ НЕЙРОННИХ МЕРЕЖАХ, Колесник С.Є., Ковальов С.О.	40
ТЕЛЕГРАМ – БОТ «ЗВЕРНЕННЯ ГРОМАДЯН», Алдохіна Н.Ю., Ступак Г.В.....	44
ПРОГНОЗУВАННЯ ПОВЕДІНКИ СПОЖИВАЧІВ З ВИКОРИСТАННЯМ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ, Скринник Д.В.	47

НАУКОВЕ ВИДАННЯ

**«ТАК»:
Телекомунікації, автоматизація,
комп'ютерно-інтегровані та інформаційні технології**

Збірка доповідей Всеукраїнської науково-практичної
конференції молодих учених
(Луцьк, 5-6 грудня 2023 р.)

Редагування, коректура та комп'ютерна верстка *Гліб Ступак*

Формат 60x84/16.
Ум. друк. арк. 15,4
Тираж 300 прим.



Видавець та виготовлювач: Державний вищий навчальний заклад «Донецький національний технічний університет», юридична адреса: пл. Шибанкова, 2, м. Покровськ, Донецька обл., 85300, фактична адреса: вул. Софії Ковалевської, 29, м. Луцьк, Волинська обл., 43012, Україна

Свідоцтво про державну реєстрацію суб'єкта видавничої справи: серія ДК №4911 від 09.06.2015