УДК 004.056.55 (681.518.2)

Б. В. Микитченко[1]
Б. Д. Загирняк[2]
Г.В.Крайнічук (Шелепало)[3]

ПОБУДОВА ПСЕВДОВИПАДКОВИХ ПОСЛІДОВНОСТЕЙ НА ОСНОВІ ДВОХ ЛАТИНСЬКИХ КВАДРАТІВ

Вінницький національний технічний університет

Анотація

Ця робота пропонує новий метод для генерації псевдовипадкових послідовностей (ПВП) за допомогою двох будь-яких латинських квадратів одного порядку. Досліджуються властивості отриманих послідовностей для побудови шифрування. На основі методу розроблена програма, результатом якої є статистичні показники.

Ключові слова: латинський квадрат, ортогональні квадрати, псевдовипадкова послідовність чисел, рекурсія, шифр, метод.

Abstract

This paper proposes a new method for generating pseudorandom sequences (PRS) using any two Latin squares of the same order. The properties of the resulting sequences for encryption are investigated. Based on the method, a program has been developed, which results in statistical indicators.

Keywords: Latin square, orthogonal squares, pseudorandom sequence of numbers, recursion, cipher, method.

Вступ

Для реалізації концепції нового методу шифрування, побудованого на основі квазігруп, необхідні специфічні методи генерування послідовностей псевдовипадкових чисел.

У цій роботі досліджуються властивості генератора послідовностей псевдовипадкових чисел (ППВЧ) за допомогою двох латинських квадратів 4-го порядку.

Псевдовипадкова послідовність (ПВП) не є абсолютно випадковою, володіє багатьма властивостями випадкових послідовностей. ПВП використовуються в криптографії, моделюванні, теорії чисел та інших областях [1]. Під максимальною довжиною послідовності розуміємо максимальну кількість елементів, яка може бути згенерована даною парою латинських квадратів порядку N. Розподіл цифр в довжині – це кількість частоти появи кожної можливої цифри в послідовності.

Латинський квадрат – це квадратна матриця n x n, заповнена n різними символами таким чином, що кожен символ зустрічається лише один раз у кожному рядку та кожному стовпчику. Два латинські квадрати є ортогональними, коли пара елементів, один з першого квадрату порядка N, а другий – з іншого квадрату порядка N, зустрічається лише один раз у всій матриці порядка N [2].

Оскільки в основі програмних генераторів як правило лежать рекурентні формули, тому й алгоритм обрано для побудови генетарора рекурсивний, тобто який визначає значення функції через її значення на менших аргументах.

Метод

1. **Формула рекурсії:** ui = ((u_{i-1} * u_{i-2}) * u_{i-3})
2. **Вхідні дані:**
   - Два латинських квадрати порядку N
   - Початкова трійка (u_{i-1}, u_{i-2}, u_{i-3})
3. **Алгоритм:**
   - Починаючи з початкової трійки, використовується формула для генерування наступного елемента послідовності.
   - Координати елемента u_{i-1} * u_{i-2} в першому квадраті та u_{i-3} в другому квадраті використовуються для отримання наступного числа u_i.
   - Процес повторюється, генеруючи послідовність різної довжини.

Результати

Для прикладу реалізації програмного засобу взяті всі латинські квадрати 4-го порядку. Тому

максимальна довжина послідовності становить 64, а мінімальна - 4.

- Кількість повторень цифр у послідовності буде однаковою, якщо два латинських квадрати утворюють найдовшу можливу послідовність.
- Два латинських квадрати, незалежно від порядку розміщення у парі, можуть генерувати:
  - ✓ однакові послідовності з однаковою довжиною;
  - ✓ різні послідовності з різною довжиною;
  - ✓ різні послідовності з однаковою довжиною.
- Більшість трійок генерують послідовність, яка є прокрученою версією іншої послідовності.
- Існують унікальні трійки для кожного квадрату, які генерують послідовність мінімальної довжини (4).

Статистика

- Перевірено 331 776 пар латинських квадратів.
- 17 280 пар генерують послідовність максимальної довжини (64).
- 6 144 пари генерують послідовність мінімальної довжини (4).
- Найчастіше зустрічається довжина послідовності - 9 (21 264 пари).
- 6 912 пар латинських квадратів є ортогональними (768 з них генерують послідовність довжиною 64).

Висновки

Метод генерації ПВП на основі двох латинських квадратів є простим і ефективним і може генерувати послідовності різної довжини. Оскільки для дослідження взяті латинські квадрати 4-го порядку, то мінімальна довжина 4 елементи в послідовності, а максимальна довжина 64 з рівномірним розподілом появи кожного N елемента, що є важливим для криптоаналізу.

Для подальших досліджень: вивчення властивостей ПВП, які генеруються цим методом, на основі латинських квадратів більшого порядку та вивчення залежності ПВП від властивостей латинських квадратів, а також застосування даного методу генерації в криптографії та інших галузях.

Подяка

Автори вдячні за ідею описаного методу генерації ПВП на основі латинських квадратів завідувачу кафедри захисту інформації Вінницького національного технічного університету професору, доктору технічних наук Лужецькому Володимиру Андрійовичу.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Christoffer Olsson Discreet Discrete Mathematics Secret Communication Using Latin Squares and Quasigroups // Bachelor thesis, 15 hp Spring term – 2017. Режим доступу:
2. J. Denes, A. D. Keedwell´ Latin Squares and their Applications // Elsevier, – 2015. https://www.diva-portal.org/smash/get/diva2:1114284/FULLTEXT01.pdf (дата звернення: 07.03.2024).

Микитченко Богдан Валентинович *— студент групи 1БКС-20б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: nif120nif@gmail.com*

Загирняк Богдан Дмитрович — *студент групи 1БКС-20б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: bohdan_2512@ukr.net*

Науковий керівник: ***Шелепало (Крайнічук) Галина Василівна*** — кандидат фізико-математичних наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail: hv.shelepalo@vntu.edu.ua.

Mykytchenko Bohdan Valentynovych *- student of group 1BKS-20b, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: nif120nif@gmail.com*

Zahirniak Bohdan D. — *student of group 1BKS-20b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: bohdan_2512@ukr.net*

Supervisor: ***Shelepalo Halyna (Krainichuk) Vasylivna*** — Candidate of Physical and Mathematical Sciences, Associate Professor of Information Protection, Vinnytsia National Technical University, Vinnytsia.