МІНІСТЕРСТВО ОСВІТИ І НАУКИ

НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Кафедра систем штучного інтелекту



Лабораторна робота №1

З курсу “Технології захисту інформації”

Виконав:  
студент групи КН-310

Бурак Марко

Викладач:

Яковина Віталій Степанович

Львів – 2020

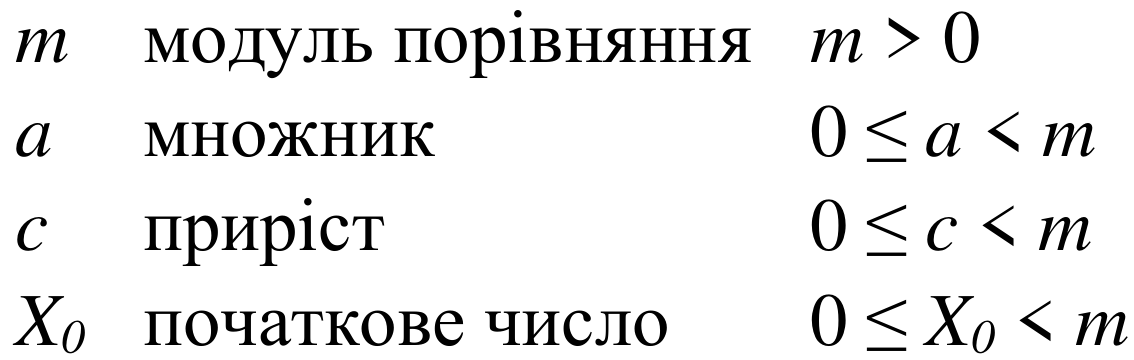
**Тема:** Створення генератора псевдовипадкових чисел.

**Мета:** ознайомитись з джерелами та застосуванням випадкових чисел, алгоритмами генерування псевдовипадкових чисел та навчитись створювати програмні генератори псевдовипадкових чисел для використання в системах захисту інформації.

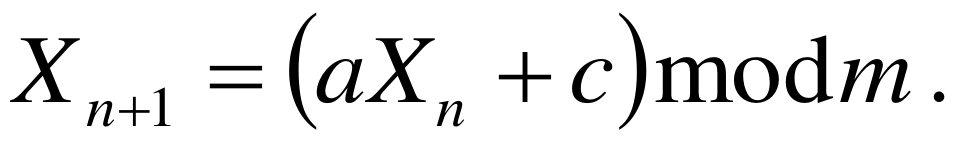
**Теоретичні відомості**

Сучасна інформатика широко використовує випадкові числа в різних програмах – від методу Монте-Карло до криптографії. Ряд алгоритмів захисту мережі, заснованих на засобах криптографії, передбачає використання випадкових чисел. Ці застосування висувають дві вимоги до послідовності випадкових чисел: випадковість і непередбачуваність.

Генератор псевдовипадкових чисел – алгоритм, що генерує послідовність чисел, елементи якої незалежні один від одного і підлягають заданому розподілу. Найбільш популярним алгоритмом для генерування псевдовипадкових чисел є алгоритм, запропонований Лемером, який називається методом лінійного порівняння. Цей алгоритм має чотири наступних параметри.



Послідовність псевдовипадкових чисел {} отримують за допомогою ітерацій наступного співвідношення:



Пропонується три критерії, за якими можна оцінити якість будь-якого генератора псевдовипадкових чисел:

1) Функція генерації повинна бути функцією повного періоду, тобто функція повинна породити усі числа від 0 до m перед тим, як числа почнуть повторюватись.

2) Створена послідовність повинна вести себе як випадкова. Насправді ця послідовність не буде випадковою, оскільки генерується детермінованим алгоритмом, але існує багато статистичних тестів, які можна використовувати для того, щоб оцінити ступінь випадковості поведінки послідовності.

3) Функція генерації повинна ефективно реалізовуватись в рамках 32-бітної арифметики.

Отже, хоча і зручно використовувати хороший генератор псевдовипадкових чисел, бажано подбати про те, що генерована послідовність була дійсно невідтворюваною, щоб знання частини послідовності не давало опоненту можливості визначити наступні елементи послідовності. Ця мета може бути досягнута цілим рядом способів. Наприклад можна змінювати потік псевдовипадкових чисел, використовуючи для цього системний час. Один зі способів на основі системного годинника полягає в ініціалізації нової послідовності після отримання кожних N чисел, використовуючи для початкового числа поточне значення часу (mod m). А можна просто додавати до кожного псевдовипадкового числа поточне значення часу (mod m).

**Завдання**

Згідно до варіанту, наведеного в таблиці, створити програмну реалізацію генератора псевдовипадкових чисел за алгоритмом лінійного порівняння. Програма повинна генерувати послідовність із заданої при вводі кількості псевдовипадкових чисел, результати повинні як виводитись на екран, так і зберігатись у файл. Перевірити період функції генерації, зробити висновок про адекватність вибору параметрів алгоритму. У звіті навести протокол роботи програми, значення періоду функції генерації та зробити висновок про придатність цього генератора для задач криптографії.

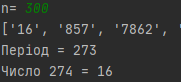
**Хід роботи**

Мій варіант – 4.





Виконував завдання реалізації генератора псевдовипадкових чисел за алгоритмом лінійного порівняння мовою python. Код програми та виконавчий файл додам до архіву. Програма працюватиме таким чином: користувач вводить число псевдовипадкових чисел, яке він хоче отримати, програма в свою ж чергу записує ці числа у масив та виводить на екран. Також на екрані, за допомогою допоміжної функції, програма рахує період функції. Числа з масиву також записуються до файлу text.txt. Після апробації програми період склав 273.



Згори представлена апробація моєї програми. Тут видно, що першим числом у масиві є 16, та 274 число(273 позиція) є 16, також. Отже можна зробити висновок, що функція визначення періоду працює правильно.

У моєму випадку m = 2^13-1, що рівне 8191. Тобто за першим критерієм оцінки якості мало б бути породжено всі числа від 0 до 8191. Іншими словами період мав би бути рівний 8191 для ідеальної функції. У моєму ж випадку було породжено лише 273 унікальних чисел, що є досить мало, для цієї функції.

**Висновок:** Я ознайомився з джерелами та застосуванням випадкових чисел, алгоритмами генерування псевдовипадкових чисел та навчився створювати програмні генератори псевдовипадкових чисел для використання в системах захисту інформації.