МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ЛЬВІВСЬКА ПОЛІТЕХНІКА»

Інститут комп'ютерних наук та інформаційних технологій
Кафедра систем штучного інтелекту

Звіт

Лабораторна робота №1

з курсу “Захист інформації”

Виконав:
студент групи ШІ-33
Біляк Андрій

Викладач:
Данчак О. І.

Львів 2024

Мета:

Метою лабораторної роботи є створення програмної реалізації генератора псевдовипадкових чисел за допомогою алгоритму лінійного порівняння (Linear Congruential Generator, LCG), а також перевірка якості цього генератора за допомогою теореми Чезаро та оцінка періоду генерації. Результати порівнюються з вбудованим генератором псевдовипадкових чисел Python. Також обчислюється оцінка числа π на основі теореми Чезаро.

Завдання:

1. Реалізувати генерацію послідовності псевдовипадкових чисел за алгоритмом LCG.
2. Перевірити період генератора та оцінити ймовірність за теоремою Чезаро.
3. Порівняти результати з вбудованим генератором Python.
4. Зробити висновки щодо придатності цього генератора для криптографічних задач.

Умови задачі:

1. Алгоритм LCG використовує наступні параметри:
    - Модуль m = 2^10 - 1
    - Множник a = 2^5
    - Початкове значення X0 = 2,
    - Приріст c=0
2. Необхідно згенерувати задану кількість псевдовипадкових чисел.
3. Для кожної послідовності необхідно визначити період і провести тестування за теоремою Чезаро.

Опис програми:

Програма реалізована на Python з використанням графічного інтерфейсу Tkinter. Основні функції:

- linear_congruential_generator: Генерує псевдовипадкові числа за алгоритмом LCG.
- gcd: Обчислює найбільший спільний дільник двох чисел за алгоритмом Евкліда.

- cesaro_test: Реалізує тест Чезаро для випадковості послідовності, обчислюючи ймовірність того, що два випадково вибрані числа є взаємно простими.
- find_period: Визначає період послідовності.

Протокол роботи програми:

Програма генерує дві послідовності псевдовипадкових чисел — одну за допомогою алгоритму LCG, іншу за допомогою вбудованої функції Python. Результати виводяться на екран та записуються у файл. Окрім того, виконується тестування випадковості за теоремою Чезаро, і розраховується період кожної послідовності.

Висновки:

1. Генератор псевдовипадкових чисел на основі LCG має дуже малий період (2), що робить його непридатним для більшості практичних застосувань, особливо у криптографії.
2. Вбудований генератор Python показав значно кращу випадковість, оскільки його період не визначений у межах згенерованої послідовності, а оцінка числа π досить близька до відомого значення.
3. Тестування за теоремою Чезаро підтвердило низьку якість генератора LCG для задач, що потребують високу випадковість.

Контрольні питання:

1. Вимоги до послідовності ПВЧ:

- Детермінованість, широкий період, рівномірний розподіл, незалежність.

2. Вимоги до випадковості ПВЧ:

- Непередбачуваність, статистична випадковість, стійкість до криптоаналізу.

3. Пряма і зворотна непередбачуваність:

- **Пряма**: неможливо передбачити наступне число.
- **Зворотна**: неможливо відновити попередні числа.

4. Тести NIST SP 800-22:

- Частотні, на послідовність, кореляція, пропорції.

5. Генератор ПВЧ:

- Алгоритм, що генерує детерміновані числа з властивостями випадкових.

6. Період ПВЧ:

- Кількість чисел до повторення послідовності.

7. Критерії якості ПВЧ:

- Довжина періоду, рівномірність, статистичність, швидкість, непередбачуваність.

8. Параметри для повного періоду LCG:

- m і c взаємно прості; a−1 кратне простим дільникам mmm.

9. Переваги LCG:

- Простота, швидкість, відтворюваність.

10. Недоліки LCG:

- Погана випадковість, короткий період, непридатність для криптографії.