Міністерство освіти і науки України

Сумський державний університет

Кафедра

Прикладної математики та моделювання складних систем

Звіт з лабораторної роботи № 4

Дисципліна

Криптографія

Студентка: Пороскун Олена Олегівна

Викладач: Козлова Ірина Іванівна

Суми, Сумська область

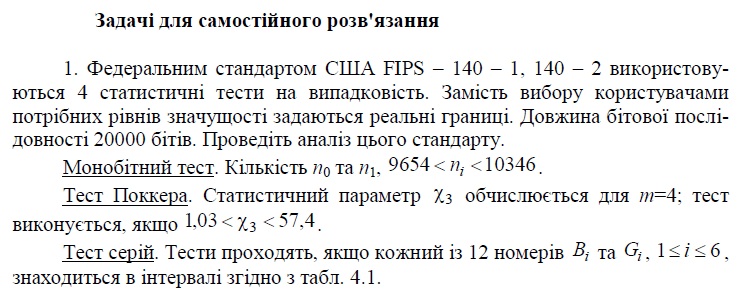
2021

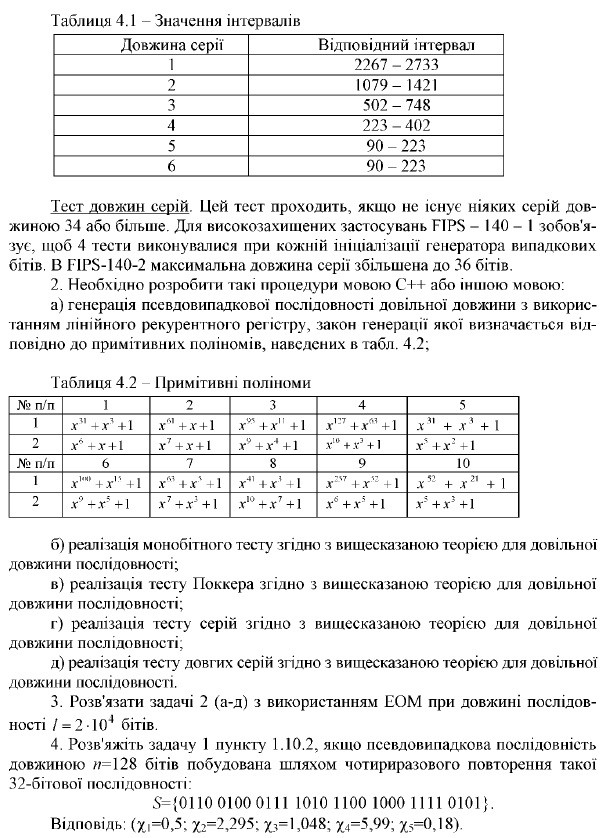
Лабораторна робота №4

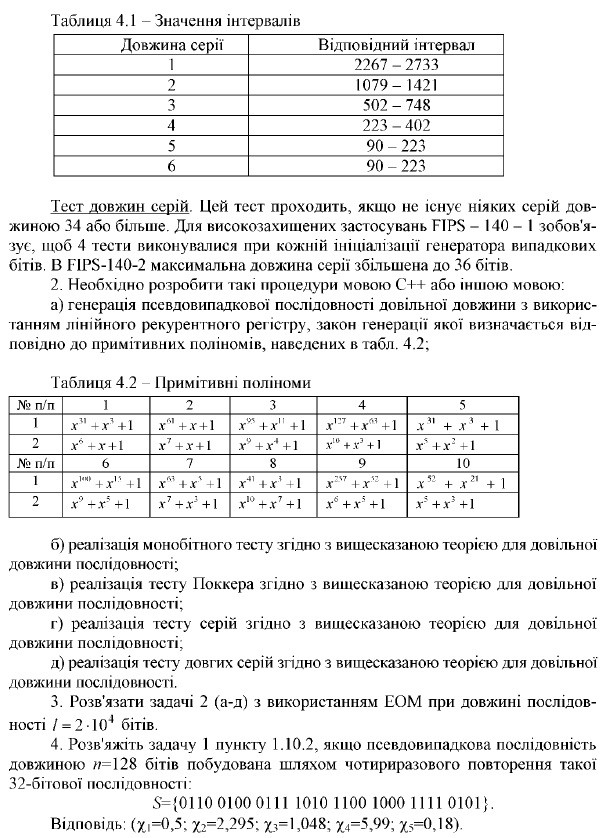
**Тема**: Аналіз алгоритмів формування псевдовипадкових послідовностей

**Мета**: отримати знання про генерацію псевдовипадкових послідовностей та про базові статистичні ймовірнісні тести(частотний(монобітний) тест, тест двох бітових серій, тест Поккера, тест серій(загальний), автокореляційний тест), навчитися застосовувати ці тести.

***Зміст задачі:***

******

******

******

***Програмний код(C++):***

***Прінт-скрін виконання програми:***

***Контрольне питання***

9. Дайте визначення лінійного конгруентного генератора.

***Лінійний конгруентний генератор*** - це алгоритм, який дає послідовність псевдовипадкових чисел, обчислених за допомогою розривного кусочно-лінійного рівняння.

Цей метод являє собою один з найстаріших і найбільш відомих алгоритмів генератора псевдовипадкових чисел. Теорія, що лежить в їх основі, відносно проста для розуміння, і вони легко реалізуються і швидкі, особливо на комп'ютерному обладнанні, яке може забезпечити модульну арифметику шляхом усічення бітів пам'яті.

**Метод лінійного порівняння (конгруентний спосіб)**

Цілочисельні константи, що визначає генератор:

***т***модуль порівняння ***m******> 0****,*

(натуральне число, відносно якого

обчислюють остачу від ділення)

***а***множник ***0 ≤ a < m,***

***c*** приріст  ***0 ≤ c < m,***

***X0***початкове число ***0 ≤ X0 < m.***

Послідовність випадкових чисел **{Х}**отримується за допомогою ітерацій:

***Xn+1*= (*aXn* + *c*) mod *m.***

1. Якщо ***т, а, с*** і ***X0***є цілими, то буде отримана послідовність цілих чисел з діапазону ***0≤ Xn<m.***

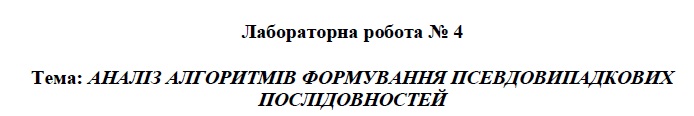
2***.*** При ***c = 0***, найбільший період складе ***m/4*** при ***а = 3+8j*** або ***а******= 5+8j*** і непарному початковому числі. Якщо ***c = 0***, генератор часто називають мультиплікативним конгруентним генератором.

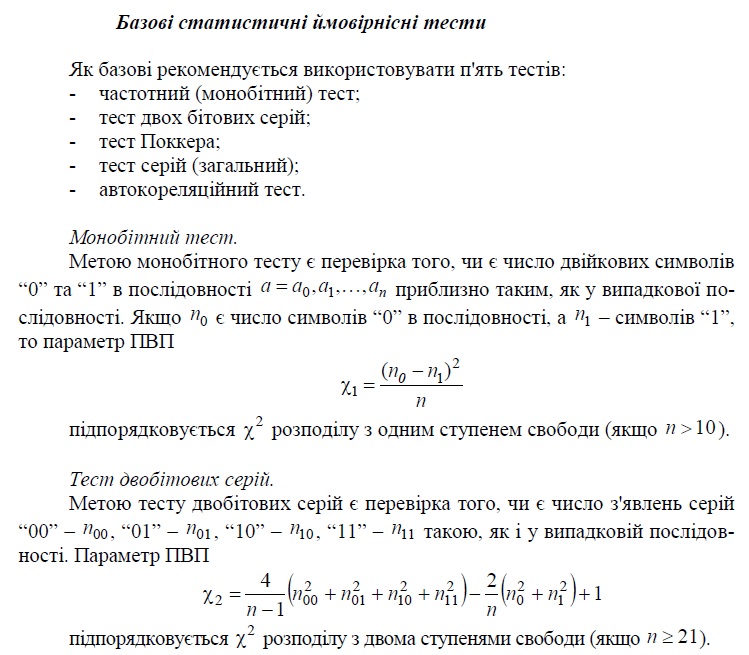
3. Якщо ***c*** непарне, а ***а******= 1+4 j***, то період можна збільшити до числа 

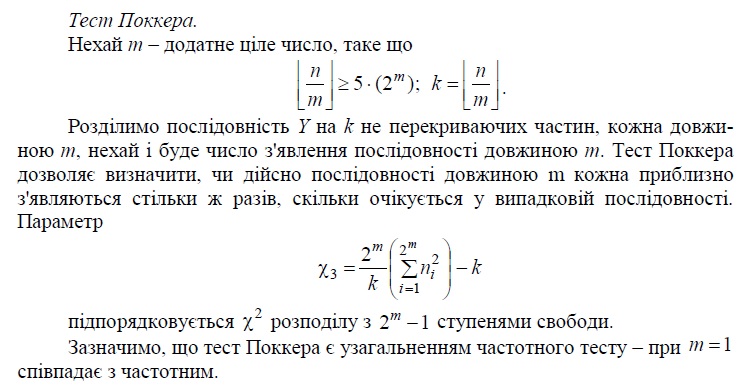
***Висновок***

Виконуючи лабораторну роботу, отримали знання про генерацію псевдовипадкових послідовностей та про базові статистичні ймовірнісні тести(частотний(монобітний) тест, тест двох бітових серій, тест Поккера, тест серій(загальний), автокореляційний тест).

***Додаток***



******

******

