Практичне завдання:

**«Тестування ключів на випадковість за стандартом FIPS-140»**

**Мета практичного завдання:** отримати практичний досвід з програмної реалізації тестів на випадковість та застосування їх для перевірки послідовностей, що потенційно можуть використовуватись в якості таємних ключів.

# 1 Теоретичні відомості

Федеральні стандарти обробки інформації (Federal Information Processing Standards) Сполучених Штатів – це набір публічно оголошених стандартів, які Національний інститут стандартів і технологій (NIST) розробив для використання в комп’ютерних системах невійськових американських урядових установ і підрядників. Стандарти FIPS встановлюють вимоги щодо забезпечення комп’ютерної безпеки та сумісності та призначені для випадків, коли відповідних галузевих стандартів ще не існує. Багато специфікацій FIPS є модифікованими версіями стандартів, які використовують технічні спільноти, такі як Американський національний інститут стандартів (ANSI), Інститут інженерів з електротехніки та електроніки (IEEE) і Міжнародна організація стандартизації (ISO).

FIPS-140 – це стандарт, розроблений Національним інститутом стандартів і технологій США (NIST) для оцінки та сертифікації криптографічних модулів. Цей стандарт встановлює вимоги до апаратного та програмного забезпечення, що використовується для шифрування, розшифрування, підпису, перевірки цифрових підписів та генерації випадкових чисел.

Тестування бітових послідовностей на випадковість відповідно до FIPS-140 виконується з метою перевірки, наскільки послідовності, що використовуються в криптографічних системах, є статистично випадковими. Відповідно до FIPS-140, тестування складається з різних статистичних тестів, які оцінюють властивості послідовностей з точки зору випадковості.

Деякі з основних тестів, використовуваних в FIPS-140 для оцінки випадковості бітових послідовностей, включають:

* Монобітний тест перевіряє, чи зберігається баланс між нулями та одиницями в послідовності.
* Тест максимальної довжини серії перевіряє, чи містяться в послідовності серії однакових бітів занадто великої довжини.
* Тест Поккера перевіряє, чи рівномірно розподілені біти в блоках послідовності.
* Тест довжин серії: перевіряє, чи містить послідовність надто довгі або надто короткі серії однакових бітів.

Ці тести дозволяють оцінити статистичну випадковість бітових послідовностей. Якщо послідовність не пройшла тести на випадковість, це може свідчити про наявність деяких закономірностей або відхилень від випадкового розподілу, що може загрожувати безпеці криптографічних систем. Тому важливо, щоб бітові послідовності були перевірені перед тим як використовувати їх для створення таємних ключів.

Ці і подібні тести застосовуються для перевірки на випадковість генераторів випадкових (псевдовипадкових) чисел. Тести використовуються для оцінки якості генераторів випадкових чисел, які є ключовим елементом у криптографічних системах. Вони допомагають виявити генератори, що є недостатньо випадковими та уникнути використання слабких ключів, що є потенційною вразливосттю.

2 Хід роботи

Для виконання практичного завдання вам треба програмно реалізувати стандарт тестування бітових послідовностей на випадковість (FIPS-140 третьої версії). Вхідними даними до функцій тестування має бути послідовність довжиною 20 000 бітів. Вихідними даними кожної функції тестування має бути логічне значення (true / false), тест пройдений та не пройдений відповідно. У разі якщо послідовність вдало проходить усі чотири функції тестування, програма має звітувати, що 20 000 бітів є достатньо випадковими. В іншому випадку послідовність бітів відхиляється.

Також для зручності тестування програми бажано реалізувати генератор випадкових послідовностей. Принципи його роботи оберіть на власний розсуд, головне щоб у вас вийшло згенерувати послідовність, яка успішно пройде тести на випадковість.

Зберігати і обробляти дані бітової послідовності бажано найбільш ефективним методом з точки зору швидкодії та використання памʼяті. Тобто таким самим чином, як в попередніх завданнях з великими числами. Отже вхідними даними до функцій тестування має бути масив з двох з половиною тисяч байтів.

Етапи виконання практичного завдання:

| Етап | Стисле формулювання задачі | Максимальна кількість балів |
| --- | --- | --- |
| 1 | Реалізація монобітного тесту | 2 |
| 2 | Реалізація тесту максимальної довжини серії | 2 |
| 3 | Реалізація тесту Поккера | 3 |
| 4 | Реалізація тесту довжин серій | 3 |

## 2.1 Реалізація монобітного тесту

Метою монобітного тесту є перевірка того, чи є число двійкових символів «0» та «1» в послідовності приблизно таким, як у випадкової послідовності. Тобто чи є загальна кількість одиниць приблизно рівною загальній кількості нулів в послідовності.

Для цього тесту достатньо пройтись по кожному біту в кожному з двох з половиною тисяч байтів і підрахувати кількість одиниць (або нулів). А потім порівняти цю кількість з константами, що зазначені в стандарті. Послідовність з двадцяти тисяч бітів вважається випадковою, якщо кількість однакових бітів потрапляє в діапазон (9654, 10346).

## 2.2 Реалізація тесту максимальної довжини серії

Серія – це послідовність одиничних (або нульових) бітів, що з обох боків обрамлена нульовими бітами (або одиничними). Приклади серій можна побачити нижче.

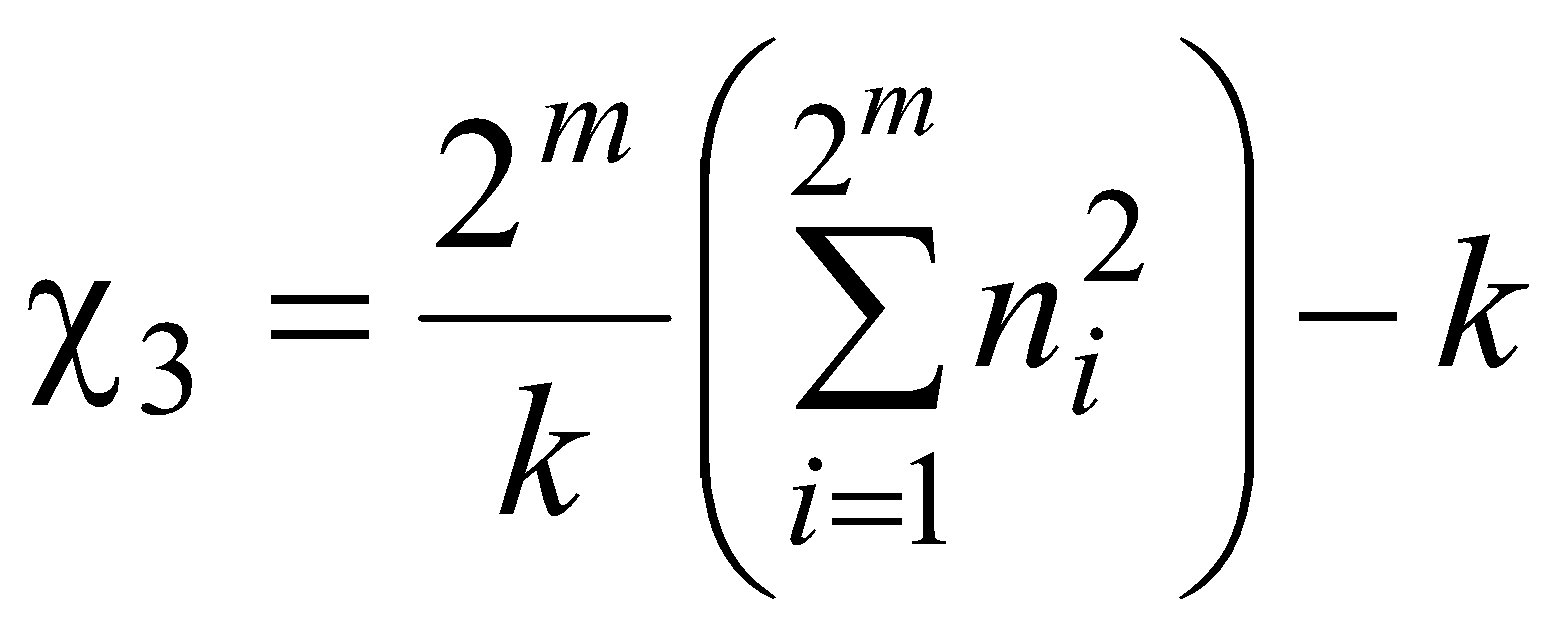
…011110… – серія одиниць довжиною 4 біти

…10000001… – серія нулів довжиною 6 бітів

Метою тесту на максимальну довжину серії є знаходження кількості бітів в найдовшій серії нулів, та кількості бітів в найдовшій серії одиниць, і порівняння цих кількостей з максимально припустимою у випадкових послідовностях. Згідно зі стандартом (FIPS-140-3) максимальна довжина серії складає 36 бітів. Якщо тестова послідовність має серію більшої довжини, то ця послідовність відхиляється, як не випадкова.

## 2.3 Реалізація тесту Поккера

Для реалізації тесту Поккера треба розділити послідовність бітів Y на k не перекриваючих частин, кожна довжиною m. Нехай i буде ітератор послідовностей довжиною m. Мета тесту Поккера полягає у перевірці, чи дійсно послідовності довжиною m кожна приблизно з'являються стільки ж разів, скільки очікується у випадковій послідовності. Для цього треба обчислити параметр X3:



Y – довжина всієї тестової послідовності

k – кількість блоків Поккера в послідовності

m – довжина блоку Поккера

i – ітератор блоків Поккера

ni – кількість зустрічання i-го блоку Поккера в послідовності

В процесі тестування послідовності відповідно до тесту Поккера вам треба підрахувати кількість зустрічання кожного з можливих блоків довжиною m. В межах цього завдання використовуйте m = 4. Потім підставити кількості зустрічання блоків до формули розрахунку параметра X3, отримайте значення параметра і порівняйте його з константою, що зазначена в стандарті.

Відповідно до тесту Поккера послідовність вважається випадковою, якщо параметр X3 входить до діапазону (1.03, 57.4). В іншому випадку послідовність відхиляється, як не випадкова.

## 2.4 Реалізація тесту довжин серій

Мета тесту довжин серій полягає у перевірці, чи дійсно число нулів та одиниць в усіх серіях послідовності є такими, як і у випадковій послідовності. Для цього треба підрахувати кількість всіх серій одиниць довжиною 1, 2, 3, 4, 5, 6 (та більше) і перевірити кожне число, чи потрапляє воно в відповідний інтервал. Те саме зробити для всіх серій з нулями.

Тестова послідовність вважається випадковою, якщо кількості всіх серій потрапляють у відповідні інтервали згідно з наступною таблицею.

| Довжина серії | Відповідний інтервал |
| --- | --- |
| 1 | 2267 – 2733 |
| 2 | 1079 – 1421 |
| 3 | 502 – 748 |
| 4 | 223 – 402 |
| 5 | 90 – 223 |
| 6+ | 90 – 223 |