МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №2

з дисципліни

«МЕТОДИ РЕАЛІЗАЦІЇ КРИПТОГРАФІЧНИХ МЕХАНІЗМІВ» на тему: «АНАЛІЗ СТІЙКОСТІ РЕАЛІЗАЦІЙ ПВЧ ТА ГЕНЕРАТОРІВ КЛЮЧІВ ДЛЯ ОБРАНОЇ БІБЛІОТЕКИ»

Виконала:

студентка 6 курсу ФТІ
група ФБ-11мн
Чуракова Єкатєріна

Перевірив:
Байденко П.В.

Київ 2022

Варіант 2А: БІБЛІОТЕКА OPENSSL ПІД WINDOWS ПЛАТФОРМУ

Статистичні тести NIST

Статистичні тести NIST – пакет статистичних тестів, прийнятий Національним інститутом стандартів і технологій (NIST). До його складу входять 15 статистичних тестів, метою яких є визначення міри випадковості двійкових послідовностей, породжених або апаратними або програмними генераторами випадкових чисел. Ці тести ґрунтуються на різних статистичних характеристиках, властивих лише випадковим послідовностям.

Для тестування бібліотеки OpenSSL були використані 5 тестів зі стандартного пакету: частотний побітовий тест, частотний блочний тест, спектральний тест (дискретне перетворення Фур'є), універсальний тест Маурера і тест кумулятивних сум.

Частотний побітовий тест

Суть даного тесту полягає у визначенні співвідношення між нулями та одиницями у всій двійковій послідовності. Мета - з'ясувати, чи дійсно число нулів і одиниць у послідовності приблизно однакові, як це можна було б припустити у випадку випадкової бінарної послідовності. Тест оцінює, наскільки близька частка одиниць до 0,5. Таким чином, число нулів та одиниць має бути приблизно однаковим. Якщо обчислене під час тесту значення ймовірності $\rho < 0,01$, то дана двійкова послідовність не є випадковою. Інакше послідовність має випадковий характер. Всі наступні тести проводяться за умови, що пройдено даний тест.

Отриманий результат:

No fails

Частотний блочний тест

Суть тесту – визначення частки одиниць всередині блоку довжиною m біт. Мета – з'ясувати, чи дійсно частота повторення одиниць у блоці довжиною m біт приблизно дорівнює m/2, як можна було б припустити у випадку абсолютно випадкової послідовності. Обчислене в ході тесту значення ймовірності ρ повинно бути не менше ніж 0,01. В іншому випадку ($\rho < 0,01$) двійкова послідовність не носить істинно випадковий характер.

Отриманий результат:

Функція RAND_bytes, побайтова генерація: 2 failed

Функція RAND_bytes, генерація послідовності: 2 failed

Спектральний тест

Суть тесту полягає в оцінці висоти піків дискретного перетворення Фур'є вихідної послідовності. Мета – виявлення періодичних властивостей вхідної

послідовності, наприклад, близько розташованих один до одного ділянок, що повторюються. Тим самим це явно демонструє відхилення від випадкового характеру послідовності, що досліджується. Ідея полягає в тому, щоб кількість піків, що перевищують граничне значення в 95% за амплітудою, було значно більше 5%. Якщо обчислене під час тесту значення ймовірності $\rho < 0,01$, то ця двійкова послідовність не є абсолютно випадковою. Інакше вона має випадковий характер.

Отриманий результат:

Функція RAND_bytes, побайтова генерація: 1 failed

Функція RAND_bytes, генерація послідовності: 2 failed

Функція RAND_priv_bytes, генерація послідовності: 2 failed

Універсальний тест Маурера

Тут визначається число біт між однаковими шаблонами у вихідній послідовності (міра, що має безпосереднє відношення до довжини стиснутої послідовності). Мета тесту — з'ясувати, чи ця послідовність може бути значно стиснута без втрат інформації. Якщо це можна зробити, то вона не є випадковою. У результаті тесту обчислюється значення ймовірності ρ. Якщо $\rho < 0,01$, то вважається, що вихідна послідовність не є випадковою. Інакше робиться висновок про її випадковість.

Отриманий результат:

Функція RAND_bytes, побайтова генерація: 1 failed

Функція RAND_bytes, генерація послідовності: 3 failed

Тест кумулятивних сум

Тест полягає у максимальному відхиленні (від нуля) при довільному обході, що визначається кумулятивною сумою заданих (-1, +1) цифр у послідовності. Мета даного тесту — визначити, чи є кумулятивна сума часткових послідовностей, що виникають у вхідній послідовності, надто великою чи надто маленькою порівняно з очікуваною поведінкою такої суми для абсолютно випадкової вхідної послідовності. Таким чином, кумулятивна сума може розглядатись як довільний обхід. Для випадкової послідовності відхилення від довільного обходу має бути поблизу нуля. Для деяких типів послідовностей, що не є повною мірою випадковими, подібні відхилення від нуля при довільному обході будуть досить суттєвими. Якщо обчислене в ході тесту значення ймовірності $\rho < 0,01$, то двійкова вхідна послідовність не є абсолютно випадковою. Інакше вона має випадковий характер.

Отриманий результат:

Функція RAND_priv_bytes, побайтова генерація: 2 failed

Функція RAND_priv_bytes, генерація послідовності: 2 failed

Висновки

У даній лабораторній роботі було досліджено процес генерації псевдо випадкових послідовностей за допомогою бібліотеки OpenSSL для ОС Windows. Тестування проводилось на згенерованих послідовностях довжиною 1 000 000 байт. Були використані 5 із 15 статичних тестів NIST для розрахунку міри випадковості двійкових послідовностей. Були використані такі тести: частотний побітовий тест, частотний блочний тест, спектральний тест, тест Маурера і тест кумулятивних сум. Проведено по 100 тестувань функцій RAND_priv_bytes і RAND_bytes при генерації послідовності в цілому, та блоків по 1 байту. Загалом, проведено 400 тестів, 17 з яких виявились неуспішними (тобто значення $\rho < 0.01$), що свідчить про відсутність випадковості у генерації послідовності. Але, слід зауважити, що основний тест (частотний побітовий) завжди був успішним. Можна стверджувати, що бібліотека OpenSSL для ОС Windows генерує дійсно випадкову послідовність із вірогідністю 95,75% згідно проведених тестів.