НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені Ігоря СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра математичних методів захисту інформації

ЛАБОРАТОРНА РОБОТА №2

на тему: "Реалізація алгоритмів генерації ключів гібридних криптосистем"

Виконали: студенти 5 курсу, групи ФІ-12мп
Бублик Єгор, Волинський Євгеній та Слуцький Андрій

Київ — 2021

1. Мета роботи

Дослідження алгоритмів генерації псевдовипадкових послідовностей, тестування простоти чисел та генерації простих чисел з точки зору їхньої ефективності за часом та можливості використання для генерації ключів асиметричних криптосистем.

2. Завдання на лабораторну роботу

Аналіз стійкості реалізацій ПВЧ та генераторів ключів для обраної бібліотеки (PyCrypto під Windows платформу).

3. Хід роботи

Генератори ключів усіх наявних у PyCrypto криптографічних систем використовують єдиний генератор ПВЧ, який реалізується функцією $Crypto.Random.new()$, яка в свою чергу викликає $os.urandom(size)$, де $size$ — довжина рядка у байтах.

Відповідно до офіційної документації *docs.python.org*: "$os.urandom()$ повертає рядок випадкових байтів, придатний для криптографічного використання". Для Windows платформи виклик функції $os.urandom()$ створить виклик функції $CryptGenRandom()$ — функцію криптографічно стійкого генератора псевдовипадкових чисел, що включена до Microsoft's Cryptographic Application Programming Interface.

В якості джерел ентропії для $CryptGenRandom()$ використовуються такі: ID поточного процесу, ID поточної гілки виконання, число тактів з моменту останнього завантаження, поточний час, різні високоточні лічильники, геш-значення MD4 від персональних даних користувача, таких як логін, ім'я комп'ютера, та ін., що робить цей генератор максимально наближеним до істинно випадкового.

4. Аналіз стійкості

Ми розглядаємо послідовність однаково розподілених випадкових величин $\{Y_i\}, i = \overline{1, m}$, що приймають значення з деякого скінченного алфавіту $\mathcal{A}$, і формулюємо три критерії для перевірки такої послідовності на криптографічну стійкість:

Uniformity. Послідовність $\{Y_i\}$ задовольняє *умові рівноімовірності*, якщо кожний член послідовності має рівноімовірний розподіл на $\mathcal{A}$.

Independency. Послідовність $\{Y_i\}$ задовольняє *умові незалежності*, якщо $P(Y_i \mid Y_{i-1}, Y_{i-2}, .., Y_1) = P(Y_i)$. Оскільки перевірка цієї умови в такому формулюванні є вкрай важкою, ми обмежимося перевіркою умови $P(Y_i \mid Y_{i-1}) = P(Y_i)$.

Homogenity. Послідовність $\{Y_i\}$ задовольняє *умові однорідності*, якщо вибірковий розподіл на всій послідовності збігається з вибірковим розподілом, одержаним із довільної підпослідовності.

Для кожної з цих умов ми за допомогою критерія Пірсона формулюємо статистичну гіпотезу для певного рівня довіри α, вважаючи, що послідовність представлена у вигляді байтів. На основі обчислень статистик для трьох рівнів довіри ми складаємо загальну таблицю для досліджуваного генератора ПВЧ. Результати дослідження стійкості наведені на рисунку 1 (де CB — границя критичної множини, а AS — значення статистики).

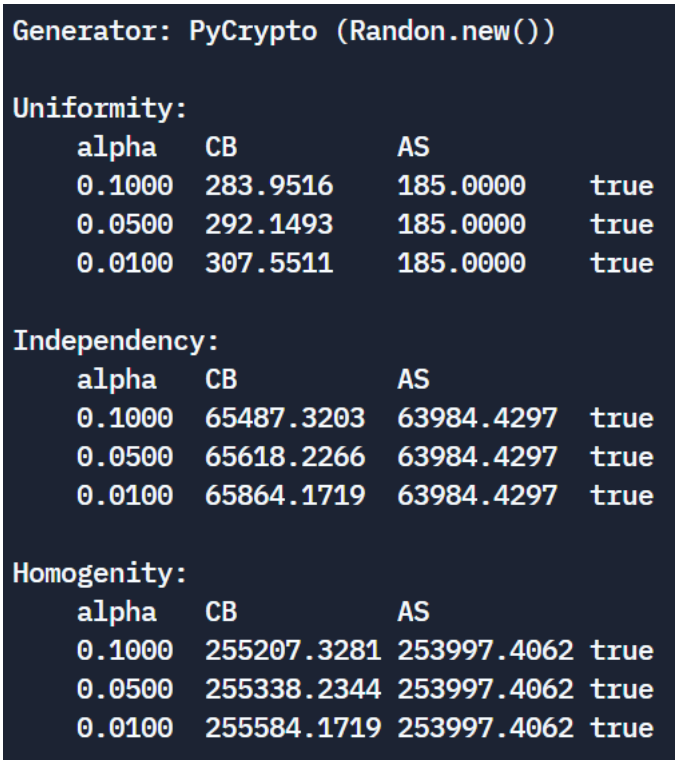

Рис. 1. Результати аналізу стійкості генератора ПВЧ

5. Висновки

Після дослідження вихідного коду бібліотеки було встановлено, що реалізація всіх генераторів ключів використовує єдиний генератор ПВЧ. Відповідно до документацій, даний генератор є стійким та придатним для використання у криптографічних цілях.

Ці факти мі підтвердили на практиці, використовуючи власні тести. Так як генератор пройшов усі тести і дійсно є криптографічно стійким, наша подальша реалізація схеми шифрування та цифрового підпису Ель-Гамаля буде використовувати саме його.

Під час виконання роботи ми набули навичок з дослідження алгоритмів генерації псевдовипадкових послідовностей.