Звіт до лабораторної роботи 4

Варіант 2

Виконали:
Бондар Петро
Кістаєв Матвій

Група: ФІ-03

Мета роботи:
Ознайомлення з деякими принципами побудови криптосистем на лінійних регістрах зсуву; практичне освоєння програмної реалізації лінійних регістрів зсуву (ЛРЗ); ознайомлення з методом кореляційного аналізу криптосистем на прикладі генератора Джиффі.

Хід виконання роботи:

1. Реалізовано класи Geffe та LFSR, які реалізовують функціонал лінійних регістрів зсуву та генератора Джиффі. За даними характеристичними многочленами реалізовано ЛРЗ L1, L2, L3 і побудованого на них генератора Джиффі.
2. За допомогою формул (4) – (6) для розмірів n = 30, 31. визначено мінімальну необхіднук кількість знаків вихідної послідовності N* для знаходження заповнення послідовності та значення порогу критерію C.

$$C = Np_1 + t_{1-\alpha}\sqrt{Np_1(1-p_1)} = \frac{N}{4} + 2{,}33\sqrt{\frac{3N}{16}}$$

$$BM < 1 \Rightarrow B = \frac{1}{2^{n_i}}, \quad n_i = \{30, 31\}$$

$$C = Np_2 - t_{1-\frac{1}{2^{n_i}}} \cdot \sqrt{Np_2(1-p_2)} = \frac{N}{2} - 6\sqrt{\frac{N}{4}}$$

$n = 30$:

$$\frac{N}{4} + 2{,}33\sqrt{\frac{3N}{16}} = \frac{N}{2} - 6\sqrt{\frac{N}{4}} \Rightarrow N = 258 \Rightarrow$$

$$\Rightarrow C = 80{,}4$$

$n = 31$: $N = 265$, $C = 83{,}6$

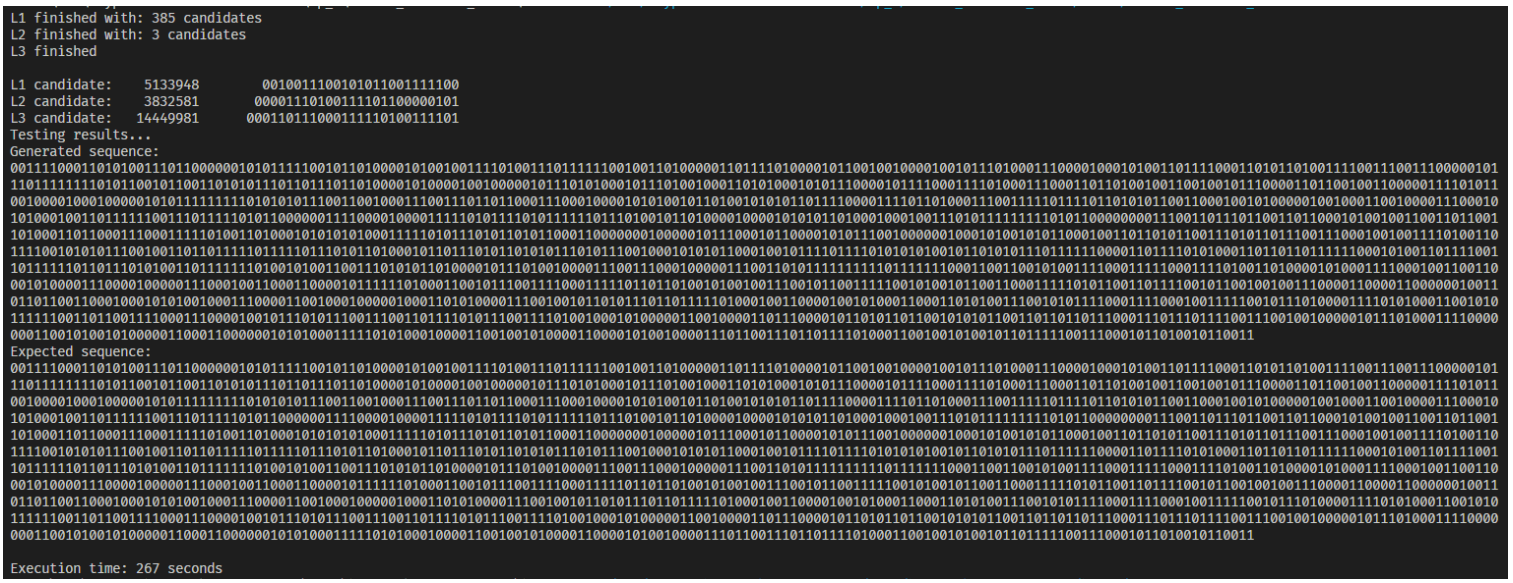
Для Варіанту для дурників значення будуть наступні:
N1 = 222, C1 = 71
N2 = 119, C2 = 74

3. Користуючись тим фактом, що характеристичні поліному регістрів – примітивні, обчислено повні цикли для L1 та L2, які містять в собі усі можливі початкові

заповнення. З цього можна ефективніше обчислити значення статистики R для кожного початкового заповнення.

4. Під час перебору відібрано лише підходящі кандидати для L1 та L2
5. Так само згенеровано повний цикл для регістра L3 і перебором знайдено початкове заповнення, яке буде узгоджуватись з найкращими кандидатами на L1, L2 та з заданою послідовністю Z.
6. В результаті отримано початкові заповнення для L1, L2 та L3. Згенерувавши перші 2048 бітів послідовності генератором Джиффі з ключем із цих заповнень, отримали повністю ідентичну до заданої послідовності.

Запуск на варіанті для дурників:



Отримані початкові заповнення:

L1: 00100111001010111001111100

L2: 00001110100111101100000101

L3: 00011011100011111010011110 1

Час виконання в середньому: 260 секунд

Запуск на ускладненому варіанті в середньому займає 2.5 години, що закономірно (без перебору на фінальному етапі)