НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ» ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Лабораторна робота №4

Виконали:
студенти ФІ-04

Кравченко Антон

Давидюк Данил

Київ – 2023

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 необхідну кількість знаків вихідної послідовності N* для знаходження заповнення послідовності та значення порогу критерію C

Для Варіанту для дурників значення будуть наступні:

N1 = 222, C1 = 71

N2 = 119, C2 = 74

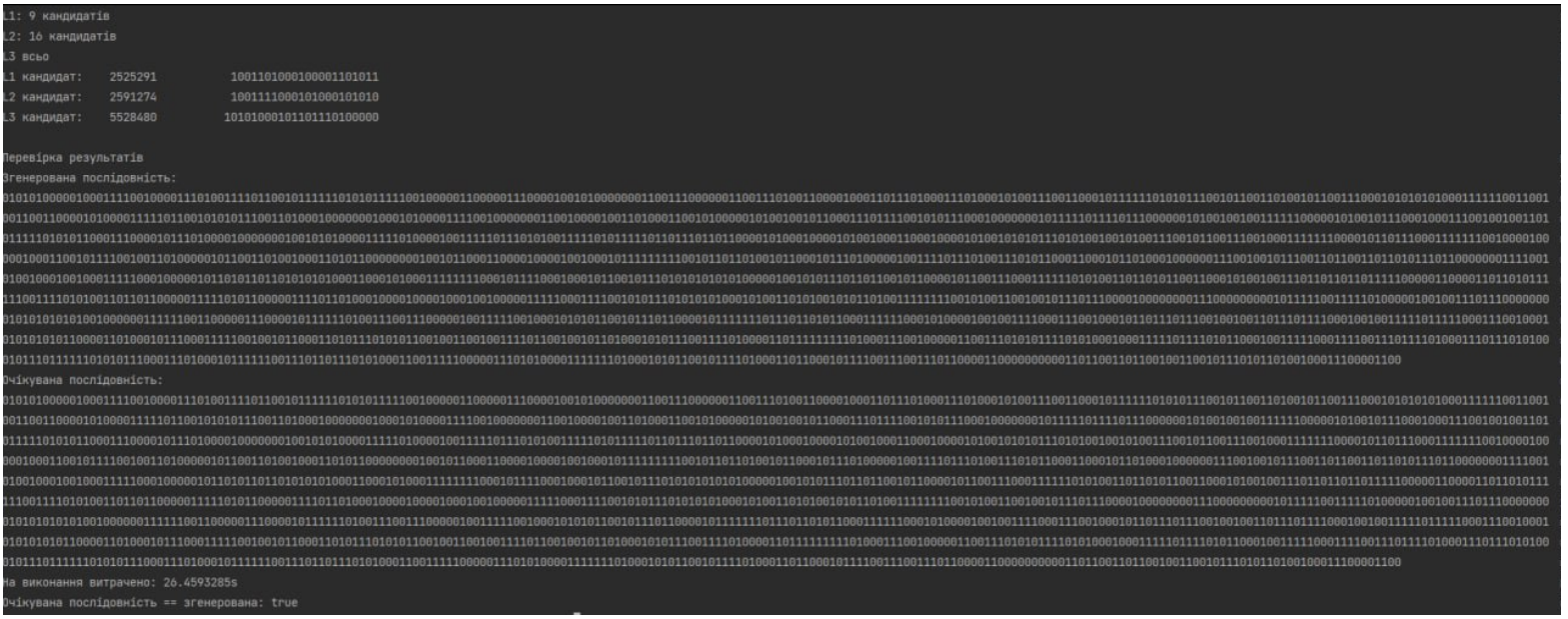
3. Користуючись тим фактом, що характеристичні поліному регістрів – примітивні, обчислено повні цикли для L1 та L2, які містять в собі усі можливі початкові заповнення. З цього можна ефективніше обчислити значення статистики R для кожного початкового заповнення.

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 кандидат:    2525291          10011010001000011010 11
L2 кандидат:    2591274          1001111000101000101010
L3 кандидат:    5528480         10101000101101110100000
```

Висновок:

Під час виконання цієї лабораторної роботи ознайомились з деякими принципами побудов криптосистем на лінійних регістрах зсуву; освоїли програмну реалізацію лінійних регістрів зсуву (ЛРЗ); ознайомились з методом кореляційного аналізу криптосистем на прикладі генератора Джиффі.