

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 реалізують 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 .

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

$$\beta M < 1 \Rightarrow \beta = \frac{1}{2n_i}, \quad n_i = \{30, 31\}$$

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

$n = 30$:

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

$$\Rightarrow C = 80,4$$

$$n = 31 : \quad N = 265, \quad C = 83,6$$

Для Варіанту для дурників значення будуть наступні:

$N_1 = 222, C_1 = 71$

$N_2 = 119, C_2 = 74$

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:

```
L1 finished with: 385 candidates
L2 finished with: 3 candidates
L3 finished

L1 candidate: 5133948      0010011100101011001111100
L2 candidate: 3832581      00001110100111101100000101
L3 candidate: 14449981     000110111000111110100111101

Testing results...
Generated sequence:
001111000110101001110110000010101111001011010000101001111010011101111100100110100000110111010000101100100000100111010001110000100010101110000110101100111001110011100000101
1101111111010110011001101011011011101101000010100001001000001011101010001011101001000110101000101011000010111000011101000110010001100000111101011
00100001000100000101011111110101011001100100011100111011000110001000010101010101010111000011101101000111001111011010110011000100100000100100011001000011100010
10100010011011111001101110101100000011100001000011110101110101111011101001011010000100001010110100010000100110101111110101100000001100110111110101100000001100110111001100110011001
111100101011100011100011101001101000101010100011110101101010110001100000001000001011100010110000101011100100000100010101100010011010101100111010111001110001001001110100110
111100101011100100110111101110111010110101010110110111011001000101011000100010111011101010101011011111000011011101010001101101111100001011101010001101101111100010100111001
10111110101101010011011111010011001101010110100001011010010000111001100010000011100110101111110111110001100110011001111000111100011110001110100110100001010001110001001100110
00101000011100001000001110001001100011000010111110100011001011100111000111101011010110011100011110101100110111001101110011011001100110000110000110000010000010011
01101100110001000101010010001110000110010001000001000110101000011100100101101011101101111010001001100001010100011100101011100011110001001111001011010000111010100011001010
11111100110110011110001110000100101101011100110011011101110011110100100010100100011011000010110110110010101100110110111000110111011100011011101110011001000001011010001110000
0001100101010100000110001100000010101000111101010001000011001001010000110000101001000011101100111011011110100011001001010110111001110001011010010110011
Expected sequence:
0011110001101010011101100000101011110010110100001010010011110100111011111100100110100000110111101000010110010010000100111010001110000100010100111100011010110100111001110011001100000101
1101111111010110011001101011011011011010100001010000100100000101110101000101110100100011010100010101100001011100011101000111000101101001100100111000011101011
00100001000100000101011111110101010110011001000111001101100011000100001010100101101001010111000011101101000111011011010101001100010010000100100011100010
101000100110111110011011101011000000111000010000111101011110101111011010010110100001000010101101000100010011101011111101011000000001110011011101100110100010100110011001
10100010110001110001111010001010001010101000111101011101010101000110000000100000101110001011000010111001000000000100101010001001101011001100111001100110011001100110
11110010101110010011011110111011011011010101000101101101010101101011001000101011011101010101010111011101010101101111100001101110101000110110110111100010100110111001
101111101101101001101111101001010011001101010101010000101101001000011100110010000111001001011010111011011110100011001001110010011100100111000111000010000100011
00101000111000010000011100010011000100001011110100011001011001110001111010101001010011100111000111101011001101110011011001101100110011001100011100001100000100011
011011001100010001010100100011100001100100010000010001101010000111001001011010111010111101000100110000100100011000110100111000111000100111100101110100001111010100011001010
11111100110110011100011100001001011010110011100110111010110011101001000101000001100100001101110000101101011010010101100110110110001110111001110011100110010000010111010001110000
0001100101001010000110001100000010101000111110101000100001100100101000011000010100100001110110011101101111010001100100101101111001110001011010010110011
```

Execution time: 267 seconds

Отримані початкові заповнення:

L1: 0010011100101011001111100

L2: 00001110100111101100000101

L3: 000110111000111110100111101

Час виконання в середньому: 260 секунд

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