НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Комп'ютерний практикум № 4

з курсу «Симетрична криптографія»

Побудова генератора псевдовипадкових послідовностей на лінійних регістрах зсуву (генератора Джиффі) та його кореляційний криптоаналіз

Виконали:
студенти групи ФІ-03
Потужний Богдан
Свірш Влада

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.

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

1. За даними характеристичними многочленами написати програму роботи ЛРЗ L_1, L_2, L_3 і побудованого на них генератора Джиффі.

2. За допомогою формул (4) – (6) при заданому α визначити кількість знаків вихідної послідовності N^*, необхідну для знаходження вірного початкового заповнення, а також поріг C для регістрів L_1 та L_2.

3. Організувати перебір всіх можливих початкових заповнень L_1 і обчислення відповідних статистик R з використанням заданої послідовності (z_i), i = 0, N*- 1

4. Відбракувати випробувані варіанти за критерієм R > C і знайти всі кандидати на істинне початкове заповнення L_1.

5. Аналогічним чином знайти кандидатів на початкове заповнення L_2.

6. Організувати перебір всіх початкових заповнень L_3 та генерацію відповідних послідовностей (s_i).

7. Відбракувати невірні початкові заповнення L_3 за тактами, на яких $x_i \neq y_i$, де (x_i), (y_i) – послідовності, що генеруються регістрами L_1 та L_2 при знайдених початкових заповненнях.

8. Перевірити знайдені початкові заповнення ЛРЗ L_1, L_2, L_3 шляхом співставлення згенерованої послідовності (z_i) із заданою при i = 0, N - 1.

Варіант 14

10010111101110000010111100111100011001001010010011100100011010111100101101100
11010010111110000110111010001111010101011010010000001100010011111101000110101
00111111100110011001001101110011000111011100111110001111010110111111010011000
01010101110100100010110111111110100011101000011110100010110001101000010001110
00101000010011110111011101101111100010001000111110010110001101011010001001111
01111010000000110001101100111001011101110101100011000111110101000011111111111
01001100010101001101100000000010000111010011100000010000000100101110100010111
10010101010000001110110110000010010101000011010111101111010000110001101110011
00110101100010110011000010101111001100111001110111000001111001010011110010110
01000001101110110110001001100110110110100010101100010100111000000010010100101
00111011101000100110110100001010110110100001010001011000101000100001011001101
10001010111011001100011101011100111111111111110011100101111010001100101111010
10001000001111010010100110110100110100101000001001101100101001111010111111110
11000101000000011101011101001001101110001100101011001111000110001101110001111
01010111000110111100010110100010001011010101111111010100010010100000110100001
00000100111000110111111101110111010101111110111111010110100000011001000010000
10011000001010101101001111111101101110110101101011011000100000010101001010010
00000110001000110001001001110110011001000110011111011011001111011011101110101
01010111101101100101011100000100001111010100001011000001000000001011110010100
00000000111110111111101101001100010011100101101001010110110110001111000000010
00010111101111011111101000100111101001101111000101110110100111100001110000011
01111010000100100100100110001100110010001101000110110001001111010001010110010
10110110111000011110110001001110100010001000101001101001000111010010001010010
01101000111111100010001000101001000101011010111000000000000000001000110111110
00001010000101110101001101010100011001110001101111110000111010000100011010100
11101101110110101101010111110011100101110011101111001101101101110101110101101
11101100111010000101110001100101000101100000010

Обчислення значення параметрів β, C, N^* для перших двох регістрів

$\beta < \frac{1}{2^n}$

$$C = Np_1 + t_{1-a}\sqrt{Np_1(1 - p_1)}$$

$$N \approx \left(\frac{t_{1-a}\sqrt{p_1(1 - p_1)} + t_{1-\beta}\sqrt{p_2(1 - p_2)}}{p_1 - p_2}\right)^2$$

Для L1:

β = 2.98 * 10^(-8)

C = 71

N = 226

Для L2:

β = 1.49 * 10^(-8)

C = 73

N = 226

Знайдені кандидати на ролі L1, L2:

L1:

Дорогі 368 кандидатів та кандидаток

R = 66, key = [000000101010001111011100]
R = 68, key = [000000101010001111111000]
R = 68, key = [000000101110001011011100]
…
R = 70, key = [111111100101101100100 1010]
R = 67, key = [111111110111110110100 1010]

L2:

Лишень 2 можливі опції

R = 72, key = [001100101001000110010 00100]
R = 64, key = [011100101001001110001 00100]

Початкові заповнення регістрів L_1, L_2 та L_3

L1: [10111110010110010010010 10]
L2: [01110010100100111000100100]
L3: [01010000010000001111101 1000]