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

Комп’ютерний практикум 4

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

Виконали:

Толмачов Євгеній

Котович Анна

Перевірив: Деркач О.Г.

Київ 2021

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.

Постановка задачі

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

Визначити кількість знаків вихідної послідовності * N , необхідну для знаходження вірного початкового заповнення, а також поріг C для регістрів L_1 та L_2.

Організувати перебір всіх можливих початкових заповнень L1 і обчислення відповідних статистик R з використанням заданої послідовності (z_i).

Відбракувати випробувані варіанти за критерієм R > C і знайти всі кандидати на істинне початкове заповнення L_1, L_2.

Організувати перебір всіх початкових заповнень L_1 та генерацію відповідних послідовностей.

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

Перевірити знайдені початкові заповнення ЛРЗ L_1, L_2, L_3шляхом співставлення згенерованої послідовності (z_i) із заданою

Хід роботи:

Варіант 12

Пошуки регістрів L_1 та L_2 не викликали ніяких труднощів, але перебір займає доволі тривалий час – і справа не в генерації, а в сумуванні R для кожної послідовності. Треба було б придумати метод оптимізації що відкинув би малоймовірні початкові заповнення. Пошук L_3 викликали деякі труднощі, більшість з яких можна віднести до не повного розуміння ходу роботи до самого написання. Але це не завадило закінчити роботу за достатньо короткий час. Код та можливі значення регістрів можна знайти за

посиланням
https://github.com/ZheZheDoshka/labs_2021_5/tree/main/%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%B04TheNewHope

Результати:

57.0352 61.0352 61.0352 – номера С (на 1-2 більше необхідно ставити). N3 = 236, - найбільший з них

z =

000011001110000111000111010110001111001111111000010001001000000000
000110000110011100000001010100010010000100001111000001000001100111
111100110100000010000100101001110011010100111100110101001011000001
111101100001011110001101111001011111110001011011101100001001110100
010001111001001010110110110000101110001110010100100100100010010110
001011011011010000011000100100110100000010000000110010000100001011
100001011101001010111101000000000101001011111011100000000010011010
110101111011010011100010011100101100100110000000110101100110101101
001011100110011001100001111001100110110011001010000011010011110100
101001011010000001010001110101010000000101111111111110110111100111
010000010100001010111001101011001110110010010011111001100111000011
100000000100111010001110011110100111100111111110000001010111001111
100100001010111110100011111001100101111100000110100111010110000101
101111010011101101110101111100000111000001010001111110111110000010
111111101110110011111100001000011110111100011010001110111000100010
111101010110011011100010000000001101

z found =

000011001110000111000111010110001111001111111000010001001000000000
000110000110011100000001010100010010000100001111000001000001100111
111100110100000010000100101001110011010100111100110101001011000001
111101100001011110001101111001011111110001011011101100001001110100
010001111001001010110110110000101110001110010100100100100010010110
001011011011010000011000100100110100000010000000110010000100001011
100001011101001010111101000000000101001011111011100000000010011010
110101111011010011100010011100101100100110000000110101100110101101
001011100110011001100001111001100110110011001010000011010011110100
101001011010000001010001110101010000000101111111111111011011110011
010000010100001010111001101011001110110010010011111001100111000011
100000000100111010001110011110100111100111111110000001010111001111
100100001010111110100011111001100101111100000110100111010110000101
101111010011101101110101111100000111100000101000111111011111000010
111111101110110011111100001000011110111110001101000111011100010010
111101010110011011100010000000 1101

Були знайдені початкові значення регістрів.

L_1 = 10000110111000111000011110

L_2 = 00111000010100011110001110

L_3 = 01110101101100001010010011 1