Міністерство освіти і науки, молоді та спорту України
Національний технічний університет України
“Київський політехнічний інститут”
Фізико-Технічний інститут

КОМП’ЮТЕРНИЙ ПРАКТИКУМ №4
за семестровий курс предмету «Симетрична криптографія»

Роботу виконали:
Студенти групи ФІ-03
Починок Юрій

Приймав:
Чорний Олег Миколайович

Київ-2023

СИМЕТРИЧНА КРИПТОГРАФІЯ

КОМП'ЮТЕРНИЙ ПРАКТИКУМ No4

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

ВАРІАНТ - 15(dummies)

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 L1 ,L2 ,L3 і побудованого на них генератора Джиффі.

2. За допомогою формул (4) – (6) при заданому визначити кількість знаків вихідної послідовності N* , необхідну для знаходження вірного початкового заповнення, а також поріг C для регістрів L1 та L2 .

3. Організувати перебір всіх можливих початкових заповнень L1 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 L1 .

5. Аналогічним чином знайти кандидатів на початкове заповнення L2 .

6. Організувати перебір всіх початкових заповнень L3 та генерацію відповідних послідовностей (s_i) .

7. Відбракувати невірні початкові заповнення L3 за тактами, на яких x_i =/= y_i , де(x_i), (y_i) – послідовності, що генеруються регістрами L1 та L2 при знайдених початкових заповненнях.

8. Перевірити знайдені початкові заповнення ЛРЗ L1, L2, L3 шляхом співставлення згенерованої послідовності(z_i) із заданою при i =[0,N*–1].

Хід роботи

Багато проблем з часом…

Обчислення констант:

L1:
N = 222
C = 71

L2:
N = 229
C = 73

Знайдені L1, L2, L3:

L1: 10000101001001010010010 01

L2: 01010100100010110111000111

L3: 11000000101011100010101 1011

Висновок:

Dummies все що я зміг осилити. Й так йшло по 3+ години на обрахунки (запуск). Круто-класно-цікаво, не робіть так знову будь ласка.