Міністерсво освіти і науки України
Національний технічний університет України
Київський політехнічний інститут імені Ігоря Сікорського
Навчально-науковий фізико-технічний інститут

Симетрична криптографія
Комп’ютерний практикум №4

Побудова генератора псевдовипадкових послідовностей на лінійних регістрах зсуву та його кореляційний аналіз

Виконали:
Медведцький Костянтин ФІ-04
Сковрон Роман ФІ-04

Київ 2023

Варіант 11

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.

План 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 ( ) i z , 0, 1 * i N .
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 ( ) i s .
7. Відбракувати невірні початкові заповнення L3 за тактами, на яких i i x y , де ( ) i x , ( )i y – послідовності, що генеруються регістрами L1 та L2 при знайдених початкових заповненнях.
8. Перевірити знайдені початкові заповнення ЛРЗ L1 , L2 , L3 шляхом співставлення згенерованої послідовності ( ) i z із заданою при i 0,N 1.

Хід роботи:

При проведенні обрахунків вийшли такі дані:

N1 = 222

N2 = 229

C1 = 71

C2 = 73

Для L1 відібрали 186 кандидатів, а для L2 - 5.

Результат:
L1 = 11101010010110000111101101
L2 = 01111111000101111110101111
L3 = 10000111110001110100101010110

Висновок:
У цій лабораторній роботі ми навчились працювати з лінійними резістрами зсуву. На кожен запуск програми потрібно було витратити від 2.5 до 4 годин...