Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №4

з дисципліни

«Криптографія»

на тему:

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

Виконали:
студенти 3 курсу ФТІ
групи ФБ-73
Пазон Б.Р.
Лутак А.О.
Перевірили:
Чорний О.
Савчук М. М.
Завадська Л. О.

Київ 2019

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*.

Результати виконання роботи:

p1 = [1, 1, 0, 1, 0, 0, 0, 1, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 0, 0]
T1 = 8388607
A1[1] = 4194304
A1[2] = 4194304
A1[3] = 4194304
A1[4] = 4194304
A1[5] = 4194304
A1[6] = 4194304
A1[7] = 4194304
A1[8] = 4194304
A1[9] = 4194304
A1[10] = 4194304

p2 = [1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0]
T2 = 349525
A2[1] = 174592
A2[2] = 174592
A2[3] = 174592
A2[4] = 174592
A2[5] = 174592
A2[6] = 174592

A2[7] = 175104
A2[8] = 174592
A2[9] = 174592
A2[10] = 174592

Висновок:

Під час данного комп’ютерного практикуму, ми ознайомились з деякими принципами побудови криптосистем на лінійних регістрах зсуву та з методом кореляційного аналізу криптосистем на прикладі генератора Джиффі.