

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

Шишкін Н.

Вітрович А.

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.

1. За допомогою формул (4) – (6) при заданому  визначити кількість знаків вихідної послідовності *N\** , необхідну для знаходження вірного початкового заповнення, а також поріг *С* для регістрів *L1* та *L2* .
2. Організувати перебір всіх можливих початкових заповнень *L1* i обчислення відповідних статистик *R* з використанням заданої послідовності (*zi)* , i=0,N\*-1 4. Відбракувати випробувані варіанти за критерієм *R* > *C* і знайти всі кандидати на істинне початкове заповнення *L1* .
3. Аналогічним чином знайти кандидатів на початкове заповнення *L2* .
4. Організувати перебір всіх початкових заповнень *L3* та генерацію відповідних послідовностей (*si)* .
5. Відбракувати невірні початкові заповнення *L3* за тактами, на яких *xi!=yi* , де

(*xi*), (*yi*) – послідовності, що генеруються регістрами *L1* та *L2* при знайдених початкових заповненнях.

1. Перевірити знайдені початкові заповнення ЛРЗ L1, L2 , L3 шляхом співставлення згенерованої послідовності (*zi)* із заданою при *i=0,N-1*.

**Результати:**

[1, 1, 0, 0, 0, 0, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 0, 0,1]

T=1048575

d[1]=524288

d[2]=524288

d[3]=524288

d[4]=524288

d[5]=524288

d[6]=524288

d[7]=524288

d[8]=524288

d[9]=524288

d[10]=524288

[1, 1, 1, 0, 0, 0, 0, 1, 0, 0, 1, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0,1]

T=3355443

d[1]=1677312

d[2]=1677312

d[3]=1677312

d[4]=1677312

d[5]=1679360

d[6]=1677312

d[7]=1677312

d[8]=1677312

d[9]=1677312

d[10]=1677312

**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.