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

Симетрична криптографія

Лабораторна робота №4

Виконала:
студентка гр. ФІ-04
Бабич А. А.

Київ – 2023

КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4

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

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 α 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 $x_i \neq y_i$, 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.

Варіант №1 (for dummies)

Хід роботи:

1. Реалізація ЛРЗ L1, L2, L3 і генератора Джиффі.

2. Обчислення значень параметрів β, C та N* для перших двох регістрів.

3. Перебір всіх можливих початкових заповнень L1 і обчислення відповідних статистик R з використанням заданої послідовності (z_i), i=0,…, N*-1.

4. Відбракування випробувані варіанти за критерієм R > C і знаходження всіх кандитатів на початкове заповнення L1.

5. Аналогічно знаходження кандидатів на початкове заповнення L2.

6. Перебір всіх початкових значень L3.

7. Відбракування невірних початкових заповнень L3.

8. Перевірка знайдених заповнень ЛРЗ L1, L2, L3 співставленням згенерованої послідовності.

Опис труднощів:

Труднощі виникали у оптимізації програми, тому що великий обсяг даних, які вимагають великої кількості пам’яті і довго обраховуються. Багато часу займає реалізація програми. Для вирішення цього було використано bytearray і операції над бітами.

Результати:

Обчислення та значення параметрів β, C та N* для перших двох регістрів:

L1:

$\beta = 1 / (2 \wedge n) = 1 / (2 \wedge 25) = = 2.9802322387695312e-08$

$t_\alpha = 2.3263478740408408$

$t_\beta = 5.419983174916869$

Отримуємо систему:

$t_\beta = (N / 2 - C) / \text{sqrt}(N / 4)$
$C = N / 4 + t_\alpha * \text{sqrt}(3N / 16)$

Підставляємо значення t_α і t_β:

$5.419983174916869 = (N / 2 - C) / \text{sqrt}(N / 4)$
$C = N / 4 + 2.3263478740408408 * \text{sqrt}(3N / 16)$

Знаходимо значення:
C = 71
N = 222

L2:

$\beta = 1 / (2 \wedge n) = 1 / (2 \wedge 26) = = 1.4901161193847656e-08$

$t_\alpha = 2.3263478740408408$

$t_\beta = 5.54259405780294$

Отримуємо аналогічну систему:

$t_\beta = (N / 2 - C) / \text{sqrt}(N / 4)$
$C = N / 4 + t_\alpha * \text{sqrt}(3N / 16)$

Підставляємо значення t_α і t_β:

$5.54259405780294 = (N / 2 - C) / \text{sqrt}(N / 4)$
$C = N / 4 + 2.3263478740408408 * \text{sqrt}(3N / 16)$

Знаходимо значення:
C = 73
N = 229

Початкові заповнення регістрів L1 , L2 та L3:

L1: 10101011111110000001011100
L2: 10111100110010101111101110

L3: 11001011110011001000100010 1

Висновки:

під час виконання цієї лабораторної роботи ознайомилася з деякими принципами побудови криптосистем на лінійних регістрах зсуву; освоїла програмну реалізацію лінійних регістрів зсуву (ЛРЗ); ознайомилася з методом кореляційного аналізу криптосистем на прикладі генератора Джиффі.