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
Піжук Богдан
Швець Катерина

Приймав:
Чорний Олег Миколайович

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 №13 (для дурників)

Хід роботи

- Написання классів LFSR та Geffe та відповідних методів у них.
- Розрахунок порогових значень N та C у відповідності із заданими α та β параметрами для L1 та L2.
- Прогонка усіх двійкових векторів відповідної довжини для L1 та L2 та підрахунок значень R для кожного з них.
- Відкидання векторів, значення R для яких вище за порогове значення C.
- Прогонка усіх двійкових векторів відповідної довжини для L3 та кандидатів на початкове заповнення для L1 та L3.
- Співставлення послідовності отриманої генератором Джиффі із заданими L1, L2 та L3 і відомої послідовності.
- Якщо послідовності співпали – початкові заповнення L1, L2 та L3 знайдені.

Опис труднощів

Найбільші труднощі пов'язані з оптимізацією та пришвидшенням обчислень та зменшенням необхідного об'єму оперативної пам'яті для роботи програми.
Для пришвидшення обчислень був використаний мультипроцесинг, що дозволило проводити розрахунки паралельно на усіх доступних потоках процесора. Крім того, був використаний вбудований клас мови програмування Python – bytearray та бітові операції що позитивним чином вплинуло не лише на швидкість роботи, а й на обсяг використаної пам'яті.

Обчислені значення

L1:

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

$t_\alpha = 2.3263478740408408$

$t_\beta = 5.419983174916869$

Вирішуємо систему:

$C = N / 4 + 2.3263478740408408 * \sqrt{3N / 16}$
$5.419983174916869 = (N / 2 - C) / \sqrt{N / 4}$
Отримаємо:
$N = 221.097 \Rightarrow 222$
$C = 70.2526 \Rightarrow 71$
L2:

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

$t_\alpha = 2.3263478740408408$

$t_\beta = 5.54259405780294$

Вирішуємо систему:

$C = N / 4 + 2.3263478740408408 * \sqrt{3N / 16}$
$5.54259405780294 = (N / 2 - C) / \sqrt{N / 4}$
Отримаємо:
$N = 228.449 \Rightarrow 229$
$C = 72.3378 \Rightarrow 73$

Початкові заповнення регістрів L1, L2 та L3

L1 = 00011101000110101110101000
L2 = 00000111000010010011100111
L3 = 01010111101011110001001111 0

Висновки

В даному комп’ютерному практикумі ми ознайомилися з принципами побудови криптосистем на лінійних регістрах зсуву та програмно реалізували ЛРЗ та генератор Джиффі. Ознайомились та застосували метод кореляційного аналізу криптосистем на прикладі генератора Джиффі.