СИМЕТРИЧНА КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4

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

Варіант 6

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 αвизначити 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) , $i = \overline{0, N^* - 1}$.
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 $i = \overline{0, N - 1}$.

Хід роботи:

Реалізовано методи Geffe та LFSR, для лінійних регістрів зсуву та генератора Джиффі відповідно. За даними характеристичними многочленами реалізовано ЛРЗ L1, L2, L3 і побудованого на них генератор Джиффі.

За допомогою формул (4) - (6) для розмірів $n = \{25, 26\}$ визначено мінімальну кількість знаків послідовності N^*.

Виходячи з того що характеристичні поліноми регістрів є примітивними, обчислив повні цикли L_1 & L_2 що містять усі початкові заповнення.

Перебором відібрали кандидати L_1 & L_2.

Згенеровано повний цикл для L_3 і перебором визначено початкове заповнення.

Отримав значення початкових заповнень L_1& L_2& L_3 та згенерувавши послідовність генератором Джиффі з даними значеннями L отримали послідовність, задану варіантом завдання.

Пошук значень b, C, N^* для L_1 & L_2:

$$b = \left(\frac{1}{2}\right)^{25}$$
$$C = \frac{1}{4}N + t_{0.99} * \frac{1}{4}\sqrt{3N}$$
$$C = \frac{N}{2} - t_{1-b} * \frac{1}{2}\sqrt{N}$$
$$\frac{1}{4}N + t_{0.99} * \frac{1}{4}\sqrt{3N} = \frac{N}{2} - t_{1-b} * \frac{1}{2}\sqrt{N}$$
$$\sqrt{N} = \sqrt{3} * t_{0.99} + 2t_{1-b}$$
$$N = \left(\sqrt{3} * t_{0.99} + 2t_{1-b}\right)^2$$
$$C = \frac{\left(\sqrt{3} * t_{0.99} + 2t_{1-b}\right)^2}{4} + t_{0.99} * \frac{1}{4}\sqrt{3}\left(\sqrt{3} * t_{0.99} + 2t_{1-b}\right)$$
$$N = 222$$
$$C = 71$$

Аналогічні обрахунки для L_2 при $b = \left(\frac{1}{2}\right)^{26}$

$$N = 229$$
$$C = 73$$

Початкові заповнення регістрів L1 , L2 та L3:
L1: 11001000110001101110010 01
L2: 10101100101011000100101
L3: 10010001000101100101011111

Тобто
L1: 26316233
L2: 5658149
L3: 38033759