Звіт до лабораторної роботи 4 з Симетричної Криптографії

ФІ-03 Дигас Богдан, ФІ-03 Антоненко Макар

Варіант-1

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.
1. За даними характеристичними многочленами написати програму роботи ЛРЗ L_1, L_2, L_3 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 L_1 та L_2.
3. Організувати перебір всіх можливих початкових заповнень L_1 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 L_1.
5. Аналогічним чином знайти кандидатів на початкове заповнення L_2.
6. Організувати перебір всіх початкових заповнень L_3 та генерацію відповідних послідовностей (s_i).
7. Відбракувати невірні початкові заповнення L_3 за тактами, на яких $x_i \neq y_i$, де (x_i), (y_i) − послідовності, що генеруються регістрами L_1 та L_2 при знайдених початкових заповненнях.
8. Перевірити знайдені початкові заповнення ЛРЗ L_1, L_2, L_3 шляхом співставлення згенерованої послідовності (z_i) із заданою при $i = \overline{0, N - 1}$

Лабораторна робота №4 з Симетричної Криптографії

ФІ-03 Дигас Богдан, ФІ-03 Антоненко Макар

Значення параметрів β, C, N для L_1 $L_1 : \beta = \frac{1}{2^{25}}$

З рівняння (4) виразили:

$$C = \frac{1}{4}N + t_{0.99} \cdot \frac{1}{4}\sqrt{3N} \tag{1}$$

З іншого боку, з рівняння (5) виражаємо:

$$C = \frac{N}{2} - t_{1-\beta} \cdot \frac{1}{2}\sqrt{N} \tag{2}$$

$$\frac{1}{4}N + t_{0.99} \cdot \frac{1}{4}\sqrt{3N} = \frac{N}{2} - t_{1-\beta} \cdot \frac{1}{2}\sqrt{N} \tag{3}$$

$$\sqrt{N} = \sqrt{3}t_{0.99} + 2t_{1-\beta} \tag{4}$$

$$N = (\sqrt{3}t_{0.99} + 2t_{1-\beta})^2 \tag{5}$$

$$C = \frac{(\sqrt{3}t_{0.99} + 2t_{1-\beta})^2}{4} + t_{0.99} \cdot \frac{1}{4}\sqrt{3}(\sqrt{3}t_{0.99} + 2t_{1-\beta}) \tag{6}$$

Знайдене початкове заповнення регістру L_1:

00100111010110100011111101