НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені Ігоря СІКОРСЬКОГО»
Фізико-технічний інституту

ЛАБОРАТОРНА РОБОТА №4
з кредитного модуля «Симетрична криптографія»

на тему:
«Побудова генератора псевдовипадкових послідовностей на лінійних регістрах зсуву (генератора Джиффі) та його кореляційний криптоаналіз»
Варіант №6

Виконали:
студенти групи ФІ-03
Гілевський Олександр
Кузьменко Анна

Київ-2023

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 $_1L$,$_2L$, $_3L$ 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 $_1L$ та $_2L$.
3. Організувати перебір всіх можливих початкових заповнень $_1L$ і обчислення відповідних статистик R з використанням заданої послідовності $(\ )_i z$, $0, 1^* i = N -$.
4. Відбракувати випробувані варіанти за критерієм $R > C$ і знайти всі кандидати на істинне початкове заповнення $_1L$.
5. Аналогічним чином знайти кандидатів на початкове заповнення $_2L$.
6. Організувати перебір всіх початкових заповнень $_3L$ та генерацію відповідних послідовностей $(\ )_i s$.
7. Відбракувати невірні початкові заповнення $_3L$ за тактами, на яких $_{i\,i}x \neq y$, де $(\ )_i x$, $(\ )_i y$ – послідовності, що генеруються регістрами $_1L$ та $_2L$ при знайдених початкових заповненнях.
8. Перевірити знайдені початкові заповнення ЛРЗ $_1L$, $_2L$, $_3L$ шляхом співставлення згенерованої послідовності $(\ )_i z$ із заданою при $i = 0,N-1$.

Визначимо мінімальну кількість знаків вихідної послідовності N* для знаходження заповнення послідовності та значення порогу критерію

$$C = Np_1 + t_{1-\alpha}\sqrt{Np_1(1-p_1)} = \frac{N}{4} + 2{,}33\sqrt{\frac{3N}{16}}$$

$$\beta M \leq 1 \Rightarrow \beta = \frac{1}{2^{n_i}},\ n_i = \{30{,}31\}$$

$$C = Np_2 + t_{1-\frac{1}{2^{n_i}}}\sqrt{Np_2(1-p_2)} = \frac{N}{2} - 6\sqrt{\frac{N}{4}}$$

$$n = 30{:}\ \frac{N}{4} + 2{,}33\frac{3N}{16} = \frac{N}{4} - 6\sqrt{\frac{N}{4}} \Rightarrow N = 258 \Rightarrow C = 80{,}4$$

$$n = 31{:}\ \Rightarrow N = 265 \Rightarrow C = 83{,}6$$

Для варіанту для дурників:
N1=222, C1=71
N2=119, C2=74

Результати роботи на варіанті для дурників:

L1: 1100100011000110111001001
L2: 00010101100101011000100101
L3: 01001000100010110010101111

Висновок

Під час виконання даної лабораторної роботи ми ознайомились з принципами побудови криптосистем на лінійних регістрах зсуву (ЛРЗ) та навчилися програмно реалізовувати такі регістри за допомогою мови програмування Python. Також ми дослідили метод кореляційного аналізу криптосистем на прикладі генератора Джиффі.

Під час роботи ми виконували такі кроки: визначили кількість знаків вихідної послідовності та поріг для регістрів, організували перебір можливих початкових заповнень регістрів та обчислили статистики R. Далі ми відібрали кандидатів на істинне початкове заповнення шляхом порівняння отриманих статистик з встановленими критеріями. На останньому етапі ми перевірили знайдені початкові заповнення шляхом порівняння згенерованих послідовностей з вихідною послідовністю.

Ця лабораторна робота дозволила нам отримати практичні навички роботи з лінійними регістрами зсуву та методом кореляційного аналізу, що має значення в області симетричної криптографії.