Звіт до лабораторної роботи 4 з Симетричної Криптографії

ФІ-03 Буржимський Ростислав, Недождій Максим

Варіант 3

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 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 $i = \overline{0, N - 1}$

Хід роботи, труднощі і шляхи їх розв'язання

На початку роботи були написані L_1, L_2, L_3 і сам генератор Джиффі. Далі ми вручну виписали необхідні формули для пошуку N^* та C, виразили і порахували їх, розв'язавши систему. Маючи N^*, відрізали відповідну кількість елементів вектора z. Далі написали функцію для пошуку R (кількості невідповідностей між x та z, y та z). З цього знаходимо можливі значення L_1 та L_2. Приблизно на цьому етапі виникла проблема з реалізацією лінійних регістрів зсуву, адже було важко перевірити правильність нашої реалізації, і виникала плутанина, як саме має бути пораховане число. Застосувавши у мові Python бібліотеку LFSR ми спробували звірити розв'язок, але це не дуже допомогло через особливості реалізації цієї бібліотеки. Для перебору усіх можливих заповнень було використане розпаралелювання, що значно пришвидшило пошук. Порівняння з порогом значно обмежувало кількість кандидатів. Для спрощення обчислення R ми передобчислюємо ваги усіх векторів довжини 16 біт.

Значення параметрів β, C, N^* для L_1 та L_2

L_1 :

$\beta = \frac{1}{2^{30}}$

З рівняння (4) виражаємо:

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

З іншого боку, з рівняння (5) виражаємо

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

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

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

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

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

Отримали значення $N = 257.54$, $C = 80.55$. При округленні N вгору отримуємо 258.

Підрахунки для L_2 аналогічні, тому наведемо виключно результати.

$\beta = \frac{1}{2^{31}}$

$N = 264.74$, $C = 82.58$

$N = 265$

Знайдені початкові заповнення регістрів L_1, L_2, L_3

У десятковому форматі:

L_1 : 2525291

L_2 : 2591274

L_3 : 5528480

У двійковому форматі:

	#26	#25	#24	#23	#22	#21	#20	#19	#18	#17	#16	#15	#14	#13	#12	#11	#10	#9	#8	#7	#6	#5	#4	#3	#2	#1	#0
L1	-	-	0	0	0	1	0	0	1	1	0	1	0	0	0	1	0	0	0	0	1	1	0	1	0	1	1
L2	-	0	0	0	0	1	0	0	1	1	1	1	0	0	0	1	0	1	0	0	0	1	0	1	0	1	0
L3	0	0	0	0	1	0	1	0	1	0	0	0	1	0	1	1	0	1	1	1	0	1	0	0	0	0	0

Висновки

Лінійні регістри зсуву зламали нам як мінімум дві ноги. Ми змогли їх пофіксити, але пережити це емоційне ушкодження буде важко. Генератор Джиффі поламати вдалось, але дешифрування було досить трудомістким процесом, що на непоганому залізі обчислення йшли за «адекватний час» згідно норм, встановленими на уроках теоретико-числових алгоритмів і симетричної криптографії (тобто менше часу існування Всесвіту). За час обчислення деяких початкових заповнень було випито не менше 3 чашок чаю.