СИМЕТРИЧНА КРИПТОГРАФІЯ
КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4

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

Variant 10 для дурників

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 альпха 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 (zi) , 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 (si) .
7. Відбракувати невірні початкові заповнення L3 за тактами, на яких xi != yi , де (xi) , (yi) – послідовності, що генеруються регістрами L1 та L2 при знайдених початкових заповненнях.
8. Перевірити знайдені початкові заповнення ЛРЗ L1 , L2 , L3 шляхом співставлення згенерованої послідовності (zi) із заданою при i = 0, N - 1.

Хід роботи

Почали з реалізації методів для знаходження кандидатів у L1, L2, L3 та самого генератору Джиффі. Окремо прорахували N* та C, розв'язали систему. Далі ми вручну виписали необхідні формули для пошуку N* та C,

виразили і порахували їх, розв’язавши систему. Реалізували пошук кількості невідповідностей x та y з z. Отримали кандидати в L1 та L2, підрахувавши для кожного відповідне R та відсіяли ті, де R перевищувало C. Співставили послідовності з генератору Джиффі з заданими L1, L2, L3. Найскладнішим виявилась відладка програми, а саме перевірка коректності, адже після кожного запуску необхідно витратити достатньо великий об’єм часу та оперативної пам’ятті, що унеможливлює користування ноутбуком на час роботи програми.

Пошук b, C, N* для L1, L2:

b = ½^25
C= ¼ N + t(0.99) * ¼ $\sqrt{3N}$
C= N/2 – t(1-b) * ½ $\sqrt{N}$
¼ N + t(0.99) * ¼ $\sqrt{3N}$ = N/2 – t(1-b) * ½ $\sqrt{N}$
$\sqrt{N}$ = $\sqrt{3}$ * t(0.99) + 2 t(1-b)
N = $\left(\sqrt{3} * t(0.99) + 2\,t(1-b)\right)^2$
C = $\frac{\left(\sqrt{3} * t(0.99) + 2\,t(1-b)\right)^2}{4}$ + t(0.99) * ¼ $\sqrt{3}$ ($\sqrt{3}$ t(0.99)+ 2 t(1-b))
Отримали значення N = 222, C = 71

Для L2 все аналогічно, тільки b = ½^26

N = 229, C = 73

Початкові заповнення регістрів L1 , L2 та L3:
L1: 0011010000101001111100001
L2: 0000000000010001010110011 0
L3: 1001011100100100011101010 00

Тобто
L1: 17798188
L2: 26904576
L3: 11412713

Висновок:

Виконуючи комп’ютерний практикум ознайомились з принципами побудови криптосистем на лінійних регістрах ЗСУву. Написали лінійні регістри. Змогли зламати генератор Джиффі, хоча і за значних енергетичних та часових затрат. За час тестування програми було зроблено дві дз з симетричної криптографії і випито пляшку уайт-спіріту.