Міністерство освіти і науки України
Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Фізико-технічний інститут

ЛАБОРАТОРНА РОБОТА №4

з дисципліни

«Криптографія»

на тему:

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

Виконали:
студенти 3 курсу ФТІ
групи ФБ-73
Шишкін Н.
Вітрович А.
Перевірили:
Чорний О.
Савчук М. М.
Завадська Л. О.

Київ 2019

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 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 (z_i) , 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 (s_i) .
7. Відбракувати невірні початкові заповнення *L3* за тактами, на яких $x_i!=y_i$, 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=0,N-1*.

Результати:

(1,1,0,1,0,1,1,1,0,0,0,1,1,0,1,1,1,1,0,0,0,0)
T=1398102
d[1]= 698368
d[2]= 698368
d[3]= 698368
d[4]= 698368
d[5]= 698368
d[6]= 698368
d[7]= 698368
d[8]= 698368
d[9]= 698368
d[10]= 698368

1 - gramma out	2 - gramma out	3 - gramma out	4 - gramma out	5 - gramma out
[0] = 698709	[00] = 174827	[000] = 58295	[0000] = 21944	[00000] = 8770
[1] = 699392	174737	[001] = 58208	[0001] = 21744	[00001] = 8701
	174318	[010] = 57910	[0010] = 21713	[00010] = 8714
	175168	[011] = 58205	[0011] = 21635	[00011] = 8859
		[100] = 58422	[0100] = 21679	[00100] = 8731
		[101] = 58060	[0101] = 21884	[00101] = 8849
		[110] = 58479	[0110] = 21725	[00110] = 8633
		[111] = 58454	[0111] = 21860	[00111] = 8705

			[1000] = 22121 [1001] = 21900 [1010] = 21525 [1011] = 22041 [1100] = 22047 [1101] = 22061 [1110] = 21768 [1111] = 21878	[01000] = 8670 [01001] = 8823 [01010] = 8694 [01011] = 8586 [01100] = 8794 [01101] = 8604 [01110] = 8761 [01111] = 8630 [10000] = 8714 [10001] = 8650 [10010] = 8610 [10011] = 8692 [10100] = 8815 [10101] = 8771 [10110] = 8722 [10111] = 8735 [11000] = 8875 [11001] = 8833 [11010] = 8700 [11011] = 8774 [11100] = 8811 [11101] = 8836 [11110] = 8735 [11111] = 8823

(1,0,1,0,0,0,0,0,1,1,0,0,0,0,1,0,0,0,1,0,0)
T=2097152
d[1]= 1048576
d[2]= 1048576
d[3]= 1048576
d[4]= 1048576
d[5]= 1048576
d[6]= 1048576
d[7]= 1048576
d[8]= 1048576
d[9]= 1048576
d[10]= 1048576

1 - gramma out_2	2 - gramma out_2	3 - gramma out_2	4 - gramma out_2	5 - gramma out_2
[0] = 1048575 [1] = 1048576	[00] = 262311 [01] = 261600 [10] = 262353 [11] = 262311	[000] = 87596 [001] = 87060 [010] = 87517 [011] = 87242 [100] = 87124 [101] = 87487 [110] = 87656 [111] = 87368	[0000] = 32759 [0001] = 32811 [0010] = 32998 [0011] = 32873 [0100] = 32651 [0101] = 32700 [0110] = 32592 [0111] = 32531 [1000] = 32794 [1001] = 32815	[00000] = 13168 [00001] = 13200 [00010] = 13013 [00011] = 13217 [00100] = 13019 [00101] = 13118 [00110] = 13091 [00111] = 13120 [01000] = 13209 [01001] = 13250

			[1010] = 32623 [1011] = 32875 [1100] = 32666 [1101] = 32800 [1110] = 33032 [1111] = 32767	[01010] = 13015 [01011] = 12825 [01100] = 13118 [01101] = 13109 [01110] = 13028 [01111] = 13128 [10000] = 12997 [10001] = 13144 [10010] = 13027 [10011] = 13155 [10100] = 13045 [10101] = 13218 [10110] = 13064 [10111] = 13134 [11000] = 13134 [11001] = 13101 [11010] = 13012 [11011] = 13328 [11100] = 13158 [11101] = 13124 [11110] = 13121 [11111] = 13040

Висновок:

Під час данного комп’ютерного практикуму, ми ознайомились з деякими принципами побудови криптосистем на лінійних регістрах зсуву та з методом кореляційного аналізу криптосистем на прикладі генератора Джиффі.