МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ

«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»

ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Кафедра інформаційної безпеки

Лабораторна робота №4

з дисципліни Криптографія

Тема: Побудова регістрів зсуву з лінійним зворотним зв'язком

та дослідження їх властивостей

Варіант 17

Перевірив:

Чорний О. М.

_____

Виконав:

Студенти групи ФБ-71

Карташ І.В.
Ткачук В.О.

Київ 2019

Мета роботи

Ознайомлення з принципами побудови регістрів зсуву з лінійним зворотним зв'язком; практичне освоєння їх програмної реалізації; дослідження властивостей лінійних рекурентних послідовностей та їх залежності від властивостей характеристичного полінома регістра.

Порядок виконання роботи

0. Уважно прочитати методичні вказівки до виконання комп'ютерного практикуму.

1. Вибрати свій варіант завдання згідно зі списком. Варіанти завдань містяться у файлі Crypto_CP4 LFSR_Var.

2. За даними характеристичними многочленами p1(x), p2(x) скласти лінійні рекурентні співвідношення для ЛРЗ, що задаються цими характеристичними многочленами.

3. Написати програми роботи кожного з ЛРЗ L1 , L2 . 4. За допомогою цих програм згенерувати імпульсні функції для кожного з ЛРЗ і підрахувати їх періоди.

5. За отриманими результатами зробити висновки щодо влавстивостей кожного з характеристичних многочленів p1(x), p2(x): многочлен примітивний над F2 ; не примітивний, але може бути незвідним; звідний.

6. Для кожної з двох імпульсних функцій обчислити розподіл k-грам на періоді, k≤ni, де ni - степінь полінома fi(x), i=1,2 а також значення функції автокореляції A(d) для 0≤ d ≤ 10. За результатами зробити висновки.

Опис роботи та основні труднощі:

Програма написана на мові C++. Особливих труднощів під час роботи над комп'ютерним практикумом не виникло, за виключенням того, що декілька разів доводилось змінювати подхід до основного алгоритму програми задля збільшення її оптимізації.

Рекурентні співвідношення:

17	$P_1(X)= X^{21} + X^{20} + X^{19} + X^{17} + X^{16} + X^{15} + X^{10} + X^8 + X^7 + X^6 + +X^5 + X^4 + 1$ $P_2(X)= X^{22} + X^{21} + X^{19} + X^{17} + X^{16} + X^{15} + X^{14} + X^{13} + X^{11} + X^{10} + X^8 + X^7 + 1$

Поліном **P2 -- { 1,0,0,0,0,0,0,1,1,0,1,1,0,1,1,1,1,1,0,1,0,1 };**

Період: **4194303**

Значення автокореляції

Крок	1	2	3	4	5	6	7	8	9	10
Знач	2097152	2097152	2097152	2097152	2097152	2097152	2097152	2097152	2097152	2097152

Розподіл к-грам для кроків (2,3,4,5)

Крок	К	К-грамма	Значення
2	2	00	524359
		01	525086
		10	523347
		11	524359

Крок	К	К-грамма	Значення
3	3	000	174677
		001	174848
		010	174848
		011	175360
		100	174848
		101	174336
		110	174336
		111	174848

Крок	К	К-грамма	Значення
4	4	0000	65597
		0001	65228
		0010	65639
		0011	65486
		0100	65618
		0101	65733
		0110	65693
		0111	65717
		1000	65629
		1001	65579
		1010	65147
		1011	65065
		1100	65564
		1101	65785
		1110	65448
		1111	65647

Крок	К	К-грамма	Значення
5	5	00000	26107
		00001	26345
		00010	26324
		00011	26141
		00100	26167
		00101	26355
		00110	26510
		00111	26473
		01000	26146
		01001	26037
		01010	26116
		01011	26036
		01100	26280
		01101	26284
		01110	26113
		01111	26134
		10000	26075
		10001	26014
		10010	26206
		10011	26267
		10100	26364
		10101	26109
		10110	26212
		10111	26258
		11000	26196
		11001	26068
		11010	26639
		11011	26209
		11100	26249
		11101	26068
		11110	26160
		11111	26198

Поліном P1 **--{ 1,0,0,0,1,1,1,1,1,0,1,0,0,0,0,1,1,1,0,1,1 };**

Період**: 299593**

Значення автокореляції

Крок	1	2	3	4	5	6	7	8	9	10
Знач	149632	150080	149632	150080	150080	149440	149632	149632	150080	149632

Розподіл к-грам для кроків (2,3,4,5)

Крок	К	К-грамма	Значення
2	2	00	37612
		01	37476
		10	37261
		11	37447

Крок	К	К-грамма	Значення
3	3	000	12609
		001	12401
		010	12503
		011	12437
		100	12459
		101	12474
		110	12497
		111	12484

Крок	К	К-грамма	Значення
4	4	0000	4637
		0001	4732
		0010	4634
		0011	4730
		0100	4759
		0101	4675
		0110	4640
		0111	4586
		1000	4741
		1001	4775
		1010	4589
		1011	4691
		1100	4742
		1101	4634
		1110	4602
		1111	4731

Крок	К	К-грамма	Значення
5	5	00000	1856
		00001	1878
		00010	1848
		00011	1877
		00100	1886
		00101	1920
		00110	1885
		00111	1951
		01000	1859
		01001	1942
		01010	1771
		01011	1836
		01100	1912
		01101	1871
		01110	1186
		01111	1863
		10000	1944
		10001	1845
		10010	1856
		10011	1909
		10100	1807
		10101	1879
		10110	1869
		10111	1832
		11000	1943
		11001	1905
		11010	1847
		11011	1856
		11100	1850
		11101	1888
		11110	1900
		11111	1847

Висновки:

Поліном P1: степінь полінома 21

Макс можливий період: 2^21-1 = 2 097 151

Період полінома P1: 299593

Відношення 2 097 151 : 299593 = 7

Так як послідовність поліному P1 має період, що ділить Макс можливий період, то поліном P1 – незвідний у полі F_2.

Поліном P2: степінь полінома 22

Макс можливий період: 2^22-1 = 4 194 303

Період полінома P2: 4194303

Відношення 4 194 303 : 4 194 303 = 1

Так як послідовність поліному P1 має період, що дорівнює Макс можливий період, то поліном P1 – незвідний і примітивний у полі F_2.

В ході лабораторної роботи ми ознайомились з принципами побудови регістрів зсуву з лінійним зворотним зв’язком Практично засвоїли їх програмну реалізацію. Дослідили властивості лінійних рекурентних послідовностей та їх залежності від властивостей характеристичного полінома регістра.