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

Лабораторна робота №4

З предмету «Криптографія»

Виконали:
Студенти 3 курсу,
ФТІ, групи ФБ-72
Курт Олег, Вовчук Роман

Київ 2019

Варіант 2

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 властивостей 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.

P1(X)= X22 + X17 + X16 + X15 + X14 + X12 + X11 + X7 + X6 + X5 + X3 + X + 1

Період: 1398101 - звідний

Автокореряція

d=0: 0

d=1: 698368

d=2: 699392

d=3: 699392

d=4: 698368

d=5: 699392

d=6: 698368

d=7: 699392

d=8: 699392

d=9: 698368

d=10: 698368

Монограми	Біграми	3-грами	4-грами	5-грами
1: 699392 0: 698709	00: 174827 01: 174737 10: 174318 11: 175168	000: 58295 001: 58208 010: 57910 011: 58205 100: 58422 101: 58060 110: 58479 111: 58454	1000: 22121 1101: 22061, 1100: 22047, 1011: 22041, 0000: 21944, 1001: 21900, 0101: 21884, 1111: 21878, 0111: 21860,	'00001': 8891, '11101': 8883, '11100': 8872, '11000': 8832, '01100': 8820, '10111': 8797, '01000': 8792, '11011': 8787, '11001': 8785, '11110': 8778, '11111': 8761, '10000': 8757, '10100': 8754, '00011': 8746,

			1110: 21768, 0001: 21744, 0110: 21725, 0010: 21713, 0100: 21679, 0011: 21635, 1010: 21525	'01010': 8731, '00101': 8730, '10101': 8724, '01101': 8723, '00110': 8708, '00100': 8705, '01011': 8699, '10001': 8698, '01110': 8686, '10110': 8679, '10011': 8679, '00010': 8677, '01111': 8674, '10010': 8670, '00111': 8661, '00000': 8648, '11010': 8640, '01001': 8633

P2(X)= X21+X18+X14+X9+X8+X2+1

Період: 2097151 – примітивний

Автокореляція:

d=0: 0

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

Монограми	Біграми	3-грами	4-грами	5-грами
1: 1048576 0: 1048575	00: 262311 01: 261600 10: 262353 11: 262311	000: 87596 001: 87060 010: 87517 011: 87242 100: 87124 101: 87487 110: 87656	1110: 33032 0010: 32998 1011: 32875 0011: 32873 1001: 32815 0001: 32811 1101: 32800	01000: 13356, 10011': 13351, 10101': 13340, 01001': 13230, 00001': 13220, 11100': 13182, 00111': 13173, 10110': 13172, 00101': 13142, 01011': 13138, 10001': 13134, 11011': 13132,

		111: 87368	1000: 32794 1111: 32767 0000: 32759 0101: 32700 1100: 32666 0100: 32651 1010: 32623 0110: 32592 0111: 32531	01100': 13128, 11111': 13125, 11001': 13111, 00010': 13097, 01101': 13085, 11000': 13083, 10010': 13080, 01111': 13075, 00110': 13060, 01110': 13059, 10111': 13049, 10000': 13048, 00000': 13021, 10100': 13021, 11110': 13013, 00100': 13009, 11101': 13002, 11010': 12959, 01010': 12931, 00011: 12904

Програмний код:

```
arr1 = [1, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 1, 1, 1, 0, 0, 0, 0]
arr2 = [1, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0]
file1 = open("D:/Files/Python/cp4/file1.txt", "w", encoding='utf-8')
file2 = open("D:/Files/Python/cp4/file2.txt", "w", encoding='utf-8')
import collections
def auto(ans, per, files):
    d = 0
    while d != 11:
        summ = 0
        i = 0
        while i != per:
            summ += (int(ans[i]) + int(ans[(i + d) % per])) % 2
            i += 1
        print('Autocaleration for d=' + str(d) + ': ' + str(summ))
        files.write('Autocaleration for d=' + str(d) + ': ' + str(summ) + '\n')
        d += 1
def ngrams(ans, n, files):
    buf = ''
    dict = collections.Counter()
    for number in ans:
        if len(buf) == n:
            dict[buf] += 1
            buf = ''
            buf += number
        else:
            buf += number
```

```
    files.write(str(n) + '-grams:     ' + str(dict) + '\n')
def lfsr(arr, files):
    b = [0] * (len(arr) - 1)
    b.append(1)
    i = 0
    stroka1 = ''  # Исходное состояние d
    while i != len(b):
        stroka1 += str(b[i])
        i += 1
    answer = ''  # Битовый рядок L
    stro = '0'  # Текущее значение d
    j = 0
    while stro != stroka1:
        c = 0
        stro = ''
        i = 0
        while i != len(b):
            c += b[i] * arr[i]
            if i > 0:
                b[i-1] = b[i]
            stro += str(b[i])
            i += 1
        c = c % 2
        b[i-1] = c
        if j == 0:
            stro += '7'
        j += 1
        answer += stro[0]
    files.write(answer[:-1] + '\n\n')
    print('Period: ' + str(j-1))
    files.write('Period: ' + str(j-1) + '\n\n')
    i = 1
    while i != len(b)+1:
        ngrams(answer, i, files)
        i += 1
    auto(answer, j-1, files)
lfsr(arr2, file2)
lfsr(arr1, file1)
```

Висновок:

В даному комп'ютерному практикумі було набуто навичок роботи з лінійними регістрами зсуву, а саме: їх програмна реалізація, дослідження властивостей характеристичного полінома регістра. Окрім цього було досліджено властивості лінійних рекурентних послідовностей.