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 регістрів зсуву з лінійним зворотним зв'язком та дослідження їх властивостей»

Варіант 2

Виконали:
студенти 3 курсу ФТІ
групи ФБ-73
Танчинець А.Є.
Петренко К.М.

Перевірили:
Чорний О.
Савчук М. М.
Завадська Л. О.

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.

1	$P_1(X)= X^{20}+X^{16}+X^{14}+X^{12}+X^{10}+X^7+X^6+X+1$ $P_2(X)= X^{24}+X^{21}+X^{12}+X^{11}+X^{10}+X^7+X^2+X+1$

P1:
The polynom is primitive
Period: 1048575
autocorrelation for d=0: 0
autocorrelation for d=1: 524288
autocorrelation for d=2: 524288
autocorrelation for d=3: 524288
autocorrelation for d=4: 524288
autocorrelation for d=5: 524288
autocorrelation for d=6: 524288
autocorrelation for d=7: 524288
autocorrelation for d=8: 524288
autocorrelation for d=9: 524288
autocorrelation for d=10: 524288

Кількість n-грам:

Ngram length: 1
{'0': 524287, '1': 524288}

Ngram length: 2
{'00': 262143, '01': 262144, '10': 262143, '11': 262144}

Ngram length: 3
{'000': 131071, '001': 131072, '010': 131072, '100': 131071, '101': 131072, '011': 131072, '111': 131072, '110': 131071}

Ngram length: 4

{'0000': 65535, '0001': 65536, '0010': 65536, '0100': 65536, '1000': 65535, '0101': 65536, '1010': 65536, '1001': 65536, '0011': 65536, '0111': 65536, '1110': 65535, '1100': 65535, '1111': 65536, '0110': 65536, '1101': 65536, '1011': 65536}

Ngram length: 5
{'00000': 32767, '00001': 32768, '00010': 32768, '00100': 32768, '01000': 32768, '10001': 32768, '00101': 32768, '01010': 32768, '10100': 32768, '01001': 32768, '10010': 32768, '10000': 32767, '00011': 32768, '00111': 32768, '01110': 32768, '11100': 32767, '11001': 32768, '10011': 32768, '01111': 32768, '11110': 32767, '11000': 32767, '10101': 32768, '00110': 32768, '01101': 32768, '11010': 32768, '01011': 32768, '10111': 32768, '11011': 32768, '10110': 32768, '11101': 32768, '01100': 32768, '11111': 32768}

P2:
The polynom is reducible
Period: 3355443
autocorrelation for d=0: 0
autocorrelation for d=1: 1677312
autocorrelation for d=2: 1677312
autocorrelation for d=3: 1677312
autocorrelation for d=4: 1677312
autocorrelation for d=5: 1679360
autocorrelation for d=6: 1677312
autocorrelation for d=7: 1677312
autocorrelation for d=8: 1677312
autocorrelation for d=9: 1677312
autocorrelation for d=10: 1677312

Кількість n-грам:

Ngram length: 1
{'0': 1678131, '1': 1677312}

Ngram length: 2
{'00': 839475, '01': 838656, '10': 838655, '11': 838656}

Ngram length: 3
{'000': 420147, '001': 419328, '010': 419328, '100': 419327, '011': 419328, '111': 419328, '110': 419327, '101': 419328}

Ngram length: 4
{'0000': 210483, '0001': 209664, '0010': 209664, '0100': 209664, '1001': 209664, '1000': 209663, '0011': 209664, '0111': 209664, '1110': 209664, '1101': 209664, '1010': 209664, '0101': 209664, '1011': 209664, '1111': 209664, '1100': 209663, '0110': 209663}

Ngram length: 5
{'00000': 105267, '00001': 105216, '00010': 104960, '00100': 104704, '01001': 104704, '10010': 104704, '01000': 104960, '10001': 104448, '00011': 104704, '00111': 104960, '01110': 105216, '11101': 104704, '11010': 104704, '10101': 104704, '01011': 104704, '10111': 104704, '01111': 104448, '11110': 104448, '11100': 104960, '11001': 104960, '00110': 104704, '01101': 104960, '11011': 104960, '10110': 104959, '01100': 104703, '10011': 104960, '01010': 104960, '10100': 104960, '11111': 105216, '00101': 104960, '11000': 104703, '10000': 105215}

Висновок: виконавши роботу, ми набули навичок у побудові лінійних регістрів зсуву з лінійним зворотним зв’язком та їх програмній реалізації; дослідили залежність лінійних рекурентних послідовностей в залежності від характеристичного полінома регістра.