

Міністерство освіти і науки України

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря Сікорського»

Фізико-технічний інститут

**КРИПТОГРАФІЯ**

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ №4 (РОЗШИРЕНИЙ)**

|  |  |
| --- | --- |
| Перевірив:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Виконали:  студенти 3 курсу ФТІ  групи ФБ-61  Вовчановський П.П.  Звінський Т. С. |

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

**ВАРІАНТ №3**

**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 *N*\* визначити кількість знаків вихідної послідовності, необхідну для знаходження вірного початкового заповнення, а також поріг *С* для регістрів *L1* та *L2* .

3. Організувати перебір всіх можливих початкових заповнень *L1* i 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* .

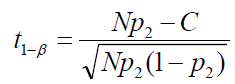
5. Аналогічним чином знайти кандидатів на початкове заповнення *L2* .

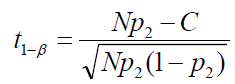
6. Організувати перебір всіх початкових заповнень *L3* та генерацію відповідних послідовностей (*si*).

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*.

**Результати виконання**



*5,419* ***N\*****=222* ***C****=70,629*

**L1**=00100000111100111010101010001101010010110001001111010000010001101010001111110101100101000010010010011000100010111101110000001000000011110101101010011010011011001100101110000010010011010010110000010000110001010011101011000100001100010100100101001000000011000101010001110101011011110001001010011010010010100001001011100010011000111110111010000110011000011000010111101001110100110110111010101011010011100110001111001110011010101011000110101100101110101110001010001100010000110110011010110001000000001010100110110010000011001000010000110101110101111111001100001001110110111110111110011111110001001010010010111010101101001011101000100011001001101110001110010010011110101111011111100100001111100111011001111101100000001110000110001000111110101101110101100000101000000101011110100110000011111100000110101100001001000111000011001100111111001101111010111010100101111111110010011011000011001110001110101011011110111000111111010010010100110101111001100111000111000101111001110100011111111101101001100011000100100010110101000001010000100111111111001110000111011111101000111100110100100001110010001010111100110100001100111110001100111100010011100100101101100110010011101001001011001001011101100111100010100110010001011000110010101000011111111101010111010101100000100010000101011001000110001011000010000000111100100011101111100110110010101110110000101111110101010010101111110101111000011001110011111000111000010111000101010010111111011010001101001001100111101101000000001100100100111110100111001111111000011100001101010101010110010011101010010111111100001101100100001100111011001010101011100011100000110101011110100111111100011001010110101101101011011011101000111101000111010000111110001011010001101101000000101011111000000100100111100000111010001101100011110000010101100000101101101000000000000110000111000100111000000111101100111100111011001110011111000110110000110000101010010110010111101101110001001101001000101110011011001101001101111100001111010011001001110101001000110110001110110010000101100010110111001101110010110100111101100111111000001110101111111000

**L2**=00010000111010110011110000010011001011110110010110111001000101001010100010010000111000110110001111011000001011111111000011111010001100101010000011101110010101110100111101001111001110011101101001101010011011011110111000010010011100100000010100111101000000111100010001011001101010100011101111001101001010011111011111001011010010001100110010010011001000100001110101010000000101000110010111101111101000010110111010010101001001010101010000110100011110000001111111101011001011110111000111000001011001001010100111111111100101001000001111001100000001100110000100111011010110000110101011010001110000110011011001111000101111111011010100001011011110101000010000111010101000010101110101001011110111110101011101101110001010100100101111011000001111101111000000101010001100111001001011100010111101110101111000001011111010101001101101011100101010010111110010000011011100111100010100110001001100011101101111011001011100010111111000001010001001011111010100011100101101100001010010111011111100100000110101100010110010001100010011001100111010010001110111000101010101110100001111100111110111111101101010111001101100100100001000011110111010000100000010100101110100110101010010001011000101101001001111100001101001110100010000011001110110010011101011001001101011100010000111011001000010011011111001011110001000101000100010011001010111100110110110011000101001110101101000000010101110110011101100010100001011101100010111000111011010101011000111010111111110000111111001111110110100000111011100011011000100001010011110011111100001110010101100110110110001110111110011100101000000011111100100110111100110100001110001100001000101101001010111111110110100110100010001110100000100001001001011001111101010010010100000001001011001011100000011010000100001001001011110001100101010010100000001010111110100111100011010000101110100101001101111100101010101101000110010001001100111111100010111010001100010101100001111010110101110111011100110111010110001101100110011101000110110011110000101010111010111000010110111010111110110110111101010000110110100100000000101011101011000001000010000010111

**L3**=10111011011000001010011111000011001001110110000101010000101001111001001110101110011100010111000111000101110011100100101100000001001010011111010101001001101111110101011001101101010110011000011111101011011011111011001110100000000100010101110000100011011010100111100111100000001010110011011101101110101100010111010101100101111100100000100111111111010100010000101110110010010001001001101111000000111001110010010110000101001010101111101010100110100000101010000100110111110101001001110011010011001010010101011011000011010100010001010110101111100100001001011110100111000010000010111001111100001010000110101101001001000001001010001010000111000101011111111101101010110001011000011001011111011110000000011101000101001101001010101101100100110011101110101011010101111001101011011111110010110010010000100110111111011101111001001010011001100100101100000101110110111110110101001011011000010101011111100100011101111010110100010110001010111101100000000010000000110001101011001001010111111111111110101111101100000110000000100001000111011010111000110101010000101101111111100111001010011110111011101111111111010101100001010101111100010001111101101011010000001111001111111111100000101010001011000100001100111001110101000000111000101011101100110000101010001011001000000110010101110101000111001101110000000101110011100100010101110110011010011111001111100100000010011001010111001010000110011000100000011011011010010111010111110110010000101100000110100011100110001110001010101100110010010110000010111011110111011010100101101100011010001001110010001110110111110000001011100101011010101000010000110101100010010101001100100001010100010111011111010100011011101010100011101001001101001111110101110100011010101100100000001101010101100111111100111111010010011110000011111100000010110111111011000100100100001011101100110100101000010011110000000100111011101101011111010110110100110100111110001000001001010110110010100111111011111100101010100101010000101110110100100110010110011111000011011101001001101000010000100001110011010101011100101001001101000000100101101101001010101010100111