



Міністерство освіти і науки, молоді та спорту України  
Національний технічний університет України  
“Київський політехнічний інститут”  
Фізико-Технічний інститут

**КОМП’ЮТЕРНИЙ ПРАКТИКУМ №4**  
**за семестровий курс предмету**  
**«Симетрична криптографія»**

**Роботу виконав:**  
Студент групи ФІ-04  
Беш Радомир

**Приймав:**  
Чорний Олег Миколайович

Київ-2023

## КОМП'ЮТЕРНИЙ ПРАКТИКУМ №4

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

### 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  $L_1$ ,  $L_2$ ,  $L_3$  і побудованого на них генератора Джиффі.
2. За допомогою формул (4) – (6) при заданому  $\alpha$  визначити кількість знаків вихідної послідовності  $*N$ , необхідну для знаходження вірного початкового заповнення, а також поріг  $C$  для регістрів  $L_1$  та  $L_2$ .
3. Організувати перебір всіх можливих початкових заповнень  $L_1$  і обчислення відповідних статистик  $R$  з використанням заданої послідовності  $( )_i$  і  $z$ ,  $0, 1 * i = N - 1$ .
4. Відбракувати випробувані варіанти за критерієм  $R > C$  і знайти всі кандидати на істинне початкове заповнення  $L_1$ .
5. Аналогічним чином знайти кандидатів на початкове заповнення  $L_2$ .
6. Організувати перебір всіх початкових заповнень  $L_3$  та генерацію відповідних послідовностей  $( )_i$  і  $s$ .
7. Відбракувати невірні початкові заповнення  $L_3$  за тактами, на яких  $i$  і  $x \neq u$ , де  $( )_i$  і  $x$ ,  $( )_i$  і  $u$  – послідовності, що генеруються регістрами  $L_1$  та  $L_2$  при знайдених початкових заповненнях.
8. Перевірити знайдені початкові заповнення ЛРЗ  $L_1$ ,  $L_2$ ,  $L_3$  шляхом співставлення згенерованої послідовності  $( )_i$  і  $z$  із заданою при  $i = 0, N - 1$ .

Хід роботи:

Спочатку було обраховано початкові значення:

Обчислимо  $\beta, c, N^*$

$$L_1: \quad \beta < \frac{1}{2^n}$$

$$n = 25$$

$$\beta_1 < 2,98 \cdot 10^{-8}$$

$$t_{1-\beta_1} = t_{0,99} = 2,32$$

$$t_{1-\beta_1} = t_{0,9999999702} = 5,49$$

$$\begin{cases} t_{1-\beta_1} = \frac{\frac{N}{2} - c}{\sqrt{\frac{N}{4}}} \\ c = \frac{N}{4} + t_{1-\alpha} \sqrt{\frac{3N}{16}} \end{cases}$$

$$\begin{cases} 5,49 = \frac{\frac{N}{2} - c}{\sqrt{\frac{N}{4}}} \\ c = \frac{N}{4} + 2,32 \sqrt{\frac{3N}{16}} \end{cases}$$

$$\frac{N}{2} - c = 5,49 \sqrt{\frac{N}{4}}$$

$$c = \frac{N}{2} - 5,49 \sqrt{\frac{N}{4}}$$

$$\frac{N}{2} - 5,49 \sqrt{\frac{N}{4}} = \frac{N}{4} + 2,32 \sqrt{\frac{3N}{16}} \quad | \cdot 4$$

$$2N - 21,96 \sqrt{\frac{N}{4}} = N + 9,28 \sqrt{\frac{3N}{16}}$$

$$N = 21,96 \sqrt{\frac{N}{4}} + 9,28 \sqrt{\frac{3N}{16}}$$

$$\boxed{N = 225}$$
$$\boxed{c = 71}$$

$$L_2: n=26 \quad \beta_2 < \frac{1}{2^n} = 1,49 \cdot 10^{-8}$$

$$t_{1-2} = t_{0,99} = 2,32$$

$$t_{1-\beta_2} = t_{0,9999999851} = 5,61$$

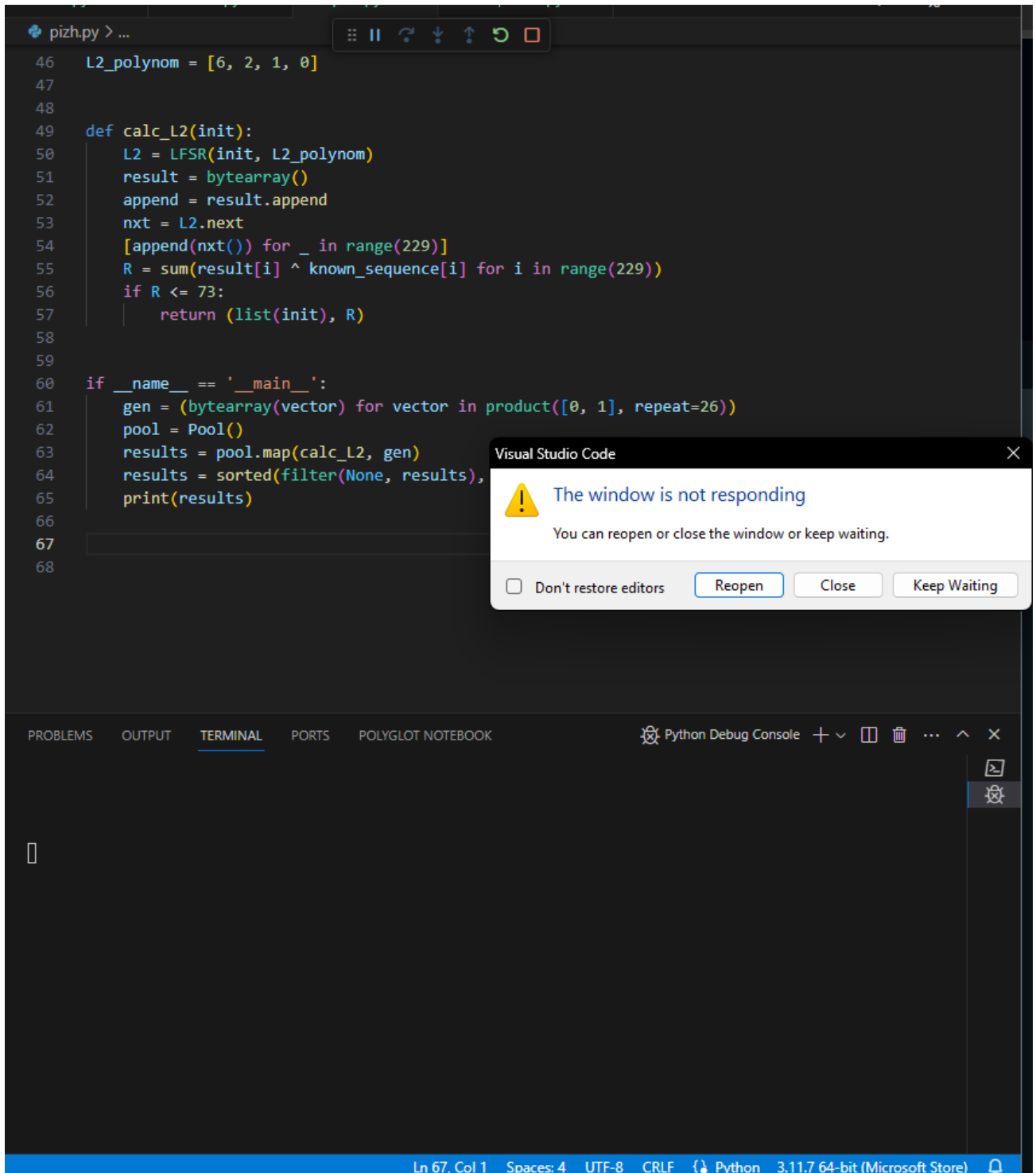
$$\left\{ \begin{array}{l} 5,61 = \frac{\frac{N}{2} - C}{\sqrt{\frac{N}{4}}} \end{array} \right.$$

$$\left\{ \begin{array}{l} C = \frac{N}{4} + 2,32 \sqrt{\frac{3N}{16}} \end{array} \right.$$

$$\boxed{\begin{array}{l} N = 232 \\ C = 43 \end{array}}$$

Далі було написано функції `lsfr_generate_bit()` і генератор Джиффі `geffe_generate_bit()`.

Після цього була написана функція обрахунку кандидатів `L_1`, але на превеликий жаль мій комп'ютер не зміг впоратися з навантаженням і постійно видав таку річ:



The screenshot shows a Visual Studio Code editor window with a Python file named `pizh.py`. The code defines a function `calc_L2` and a main block. The `calc_L2` function uses an LFSR to generate a sequence of 229 bits and calculates a value `R` based on a known sequence. The main block generates a pool of candidates and prints the results. A dialog box titled "Visual Studio Code" is overlaid on the editor, displaying a warning icon and the message "The window is not responding". Below the message, it says "You can reopen or close the window or keep waiting." and provides three buttons: "Don't restore editors", "Reopen", and "Close". The status bar at the bottom indicates the current position is line 67, column 1, with 4 spaces, UTF-8 encoding, CRLF line endings, and Python 3.11.7 64-bit (Microsoft Store) interpreter.

```
46 L2_polynom = [6, 2, 1, 0]
47
48
49 def calc_L2(init):
50     L2 = LFSR(init, L2_polynom)
51     result = bytearray()
52     append = result.append
53     nxt = L2.next
54     [append(nxt()) for _ in range(229)]
55     R = sum(result[i] ^ known_sequence[i] for i in range(229))
56     if R <= 73:
57         return (list(init), R)
58
59
60 if __name__ == '__main__':
61     gen = (bytearray(vector) for vector in product([0, 1], repeat=26))
62     pool = Pool()
63     results = pool.map(calc_L2, gen)
64     results = sorted(filter(None, results),
65                      print(results))
66
67
68
```

Visual Studio Code

The window is not responding

You can reopen or close the window or keep waiting.

☐ Don't restore editors

PROBLEMS OUTPUT TERMINAL PORTS POLYGLOT NOTEBOOK Python Debug Console

Ln 67, Col 1 Spaces: 4 UTF-8 CRLF Python 3.11.7 64-bit (Microsoft Store)

Через це фінальний результат не був отриманий.

**Висновки:** Ознайомився з деякими принципами побудови криптосистем на лінійних регістрах зсуву; ознайомився з програмною реалізацією лінійних регістрів зсуву (ЛРЗ). Та нажаль не зміг отримати якісних результатів.