

*Дипломна робота*

# Оцінка ефективності криптографічних генераторів, заснованих на алгоритмах Фібоначчі

Виконав студент

4го курсу групи

БІ-443

Ілларіонов Ігор

- **Актуальність теми:** застосування генератора псевдовипадкових чисел в тестуванні коректності алгоритмів та програм
- **Мета і завдання дипломної роботи:** вивчити та дослідити криптографічні генератори псевдовипадкових чисел (ГПВЧ), засновані на алгоритмах Фібоначі, а також оцінити ефективність даних генераторів.
- **Об'єктом дослідження** є криптографічні алгоритми генерації псевдовипадкових чисел.
- **Предметом даної дипломної роботи** є аналіз та оцінка ефективності криптографічних ГПВЧ, заснованих на алгоритмах Фібоначі.

# АЛГОРИТМИ ГЕНЕРАЦІЇ ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

- ГПВЧ повинен мати такі властивості:
- 1. Період гами повинен бути досить великим
- 2. Гамма повинна бути важко передбачуваною
- 3. Ймовірності появи (породження) різних значень повинні бути точно рівні
- 4. Генерування гами не повинно бути пов'язане з великими технічними і організаційними труднощами

# ЛІНІЙНИЙ КОНГРУЕНТНИЙ ГЕНЕРАТОР ПСЕВДОВИПАДКОВИХ ЧИСЕЛ

- Цей алгоритм для обчислення числа  $k_i$  використовує формулу:

$$k_i = (a \cdot k_{i-1} + b) \bmod c,$$

- де  $a$ ,  $b$ ,  $c$  — деякі константи, а  $k_{i-1}$  — попереднє псевдовипадкове число.

# МЕТОД ФІБОНАЧЧІ ІЗ ЗАПІЗНЕННЯМ

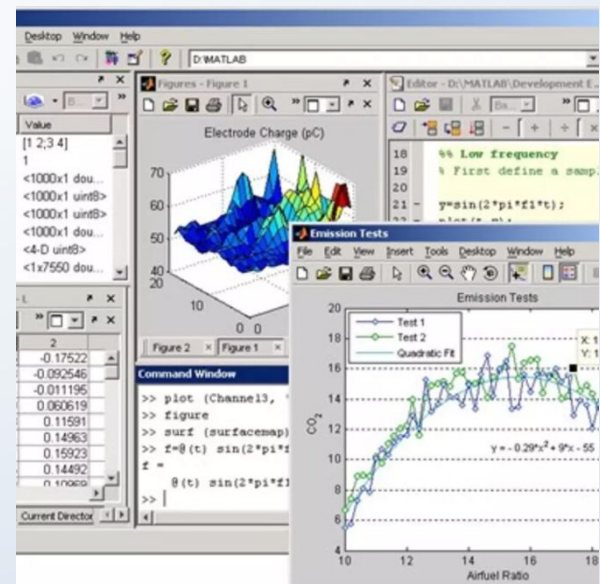
- Послідовність Фібоначчі.

$$X_{n+1} = (X_n + X_{n-1}) \bmod m.$$

$$X_{n+1} = (X_{n-k} + X_{n-j}) \bmod m, j > k \geq 1.$$

- Використання методу Фібоначчі із запізненням

$$k_i = \begin{cases} k_{i-a} - k_{i-b}, & \text{якщо } k_{i-a} \geq k_{i-b}; \\ k_{i-a} - k_{i-b} + 1, & \text{якщо } k_{i-a} < k_{i-b}; \end{cases}$$



- де  $k_i$  — дійсні числа з діапазону  $[0,1]$ ;  $a, b$  — цілі позитивні числа, параметри генератора.

# ГЕНЕРАТОР ПСЕВДОВИПАДКОВИХ ЧИСЕЛ НА ОСНОВІ АЛГОРИТМУ VBS

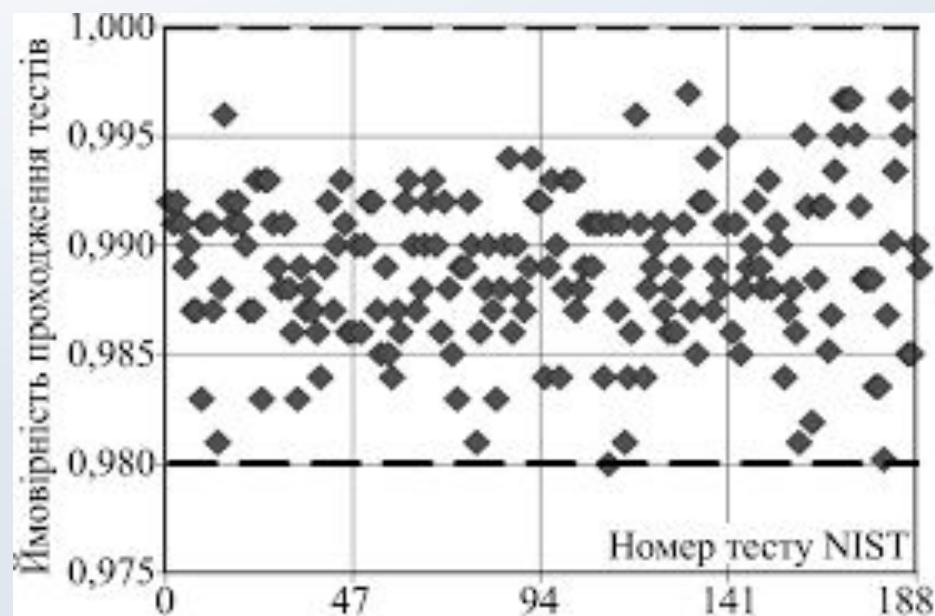
- Найцікавіша властивість цього методу для отримання з послідовності  $n$ -го числа не потрібно обчислювати всі попередні  $n$  чисел  $x_i$ .

$x_n$  можна відразу отримати за формулою:

$$x_n = x_0 \cdot 2^{n \bmod ((p-1)(q-1))} \bmod M$$

- + алгоритму :
- послідовність ПВЧ із великим періодом

- алгоритму:
- недостатня швидкодія





# РЕГІСТР ЗСУВУ З ЛІНІЙНИМ ЗВОРОТНИМ ЗВ'ЯЗКОМ



- Рисунок 1. Схема роботи РЗЛЗЗ

# Використання нелінійної функції фільтрації

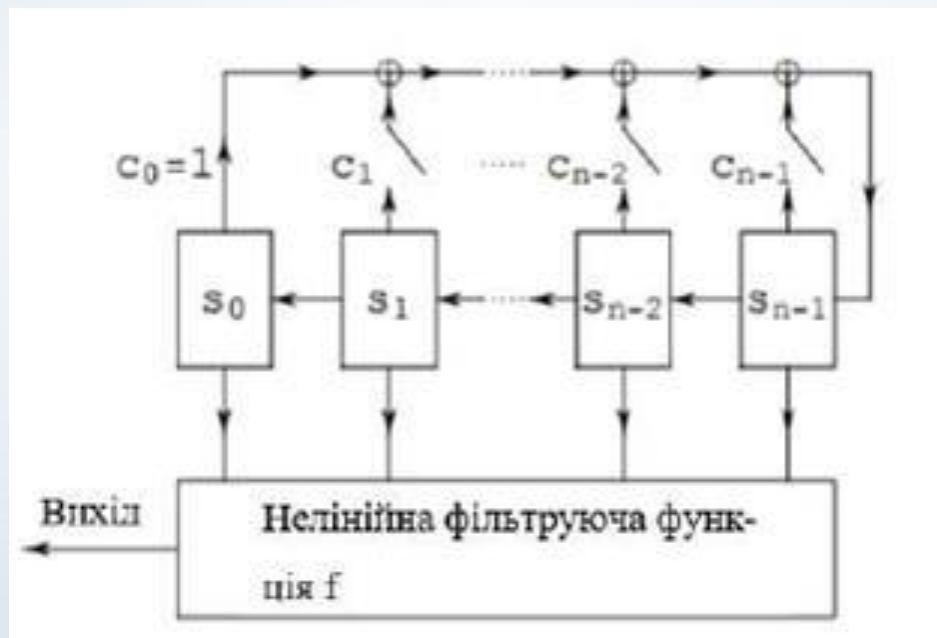
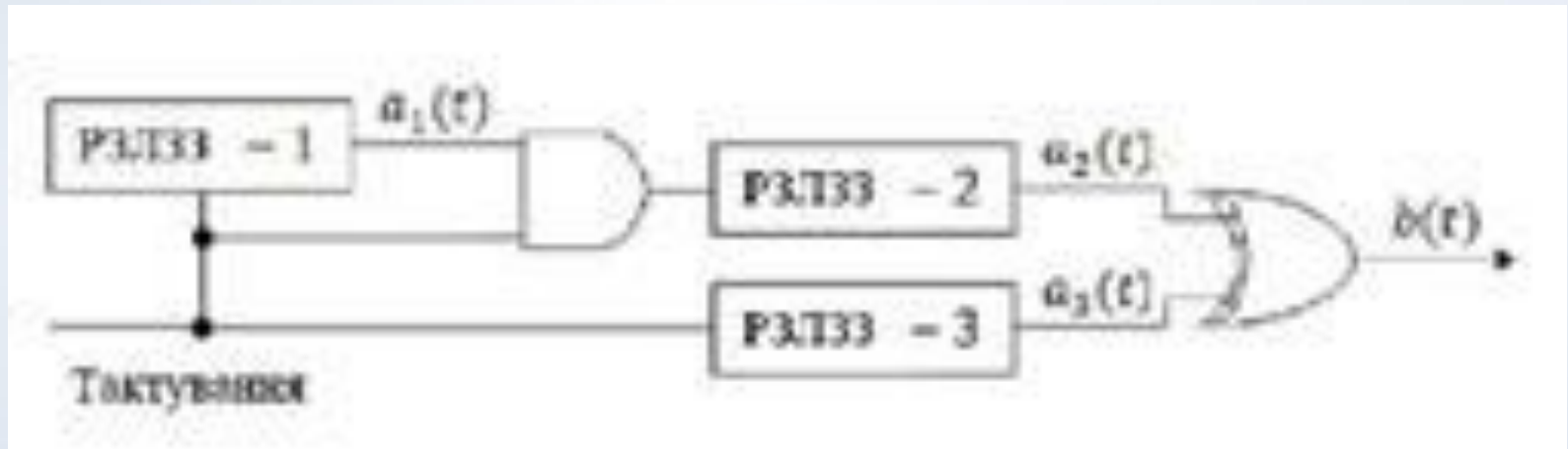


Рисунок 2. Генератор на нелінійному фільтрі

# Генератори, засновані на управлінні синхроканалом



- Рисунок 3. Генератор «стоп-вперед»

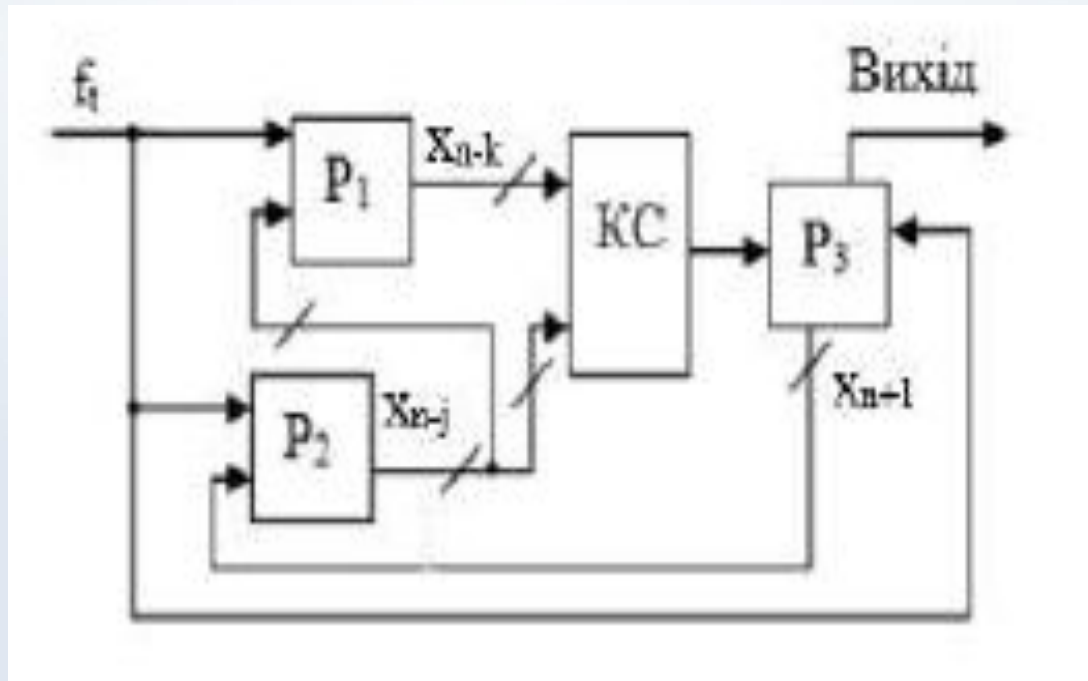
# Комбінуючі генератори



Рисунок 4. Генератор за декількома регістрами зсуву

# ОЦІНКА ЕФЕКТИВНОСТІ АДИТИВНОГО ГЕНЕРАТОРА ФІБОННАЧЧІ

- $x_{n+1} = (x_{n-k} + x_{n-j}) \bmod m$



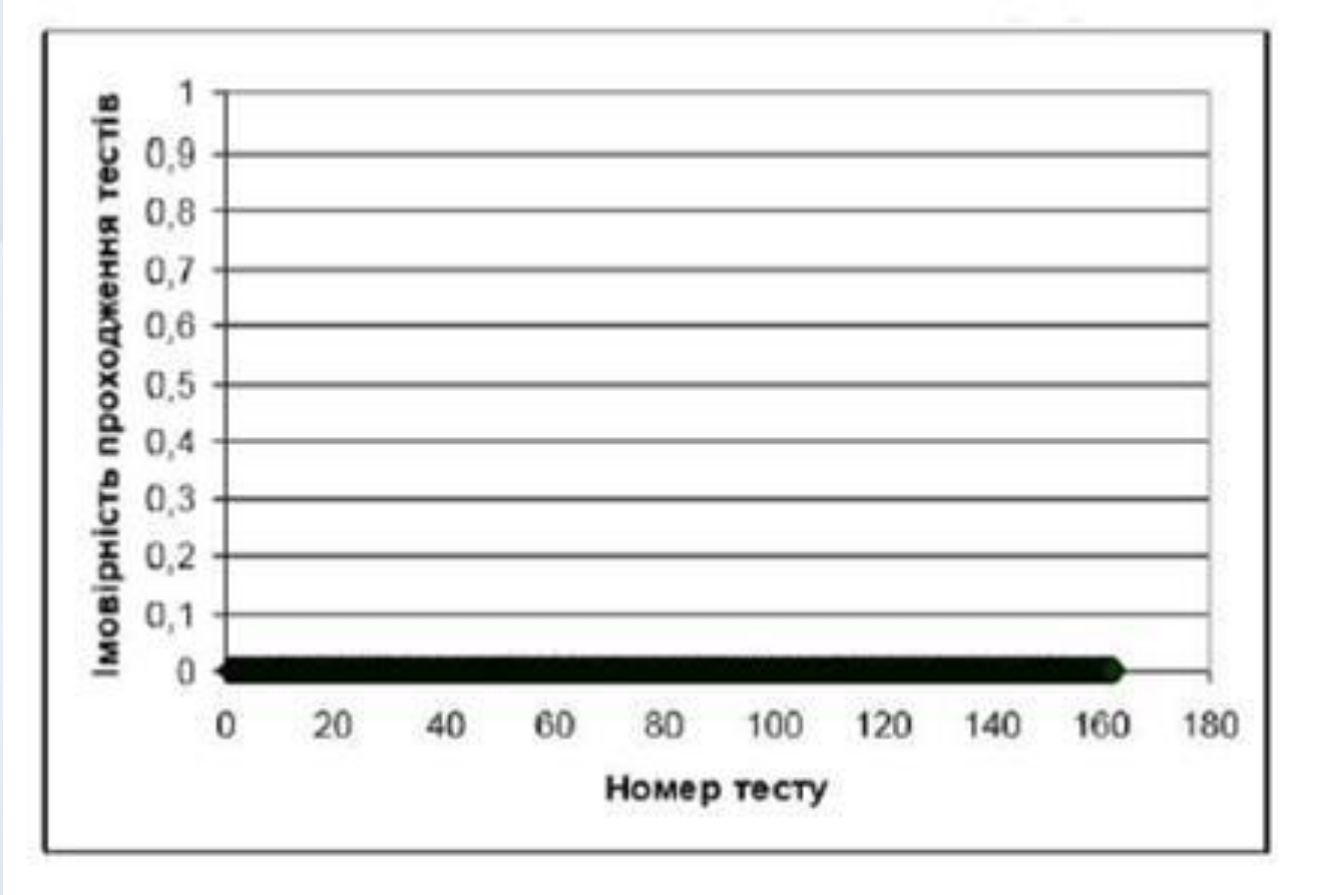


Рисунок 5. Статистичний портрет АФЗЗ

# Результати дослідження класичного генератора Фібоначчі

<i>Алгоритм роботи</i>	<i>Кількість регістрів</i>	<i>Кількість не пройдених тестів NIST з 162</i>	<i>Період повторення</i>
$x_n = (x_6 + x_1)$	7	(-162)	111104
	8	(-162)	261632
	9	(-162)	7680
	10	(-162)	304640
	11	(-162)	419328

- $x_{n+1} = (x_{n-k} + x_{n-j} + a) \bmod m$

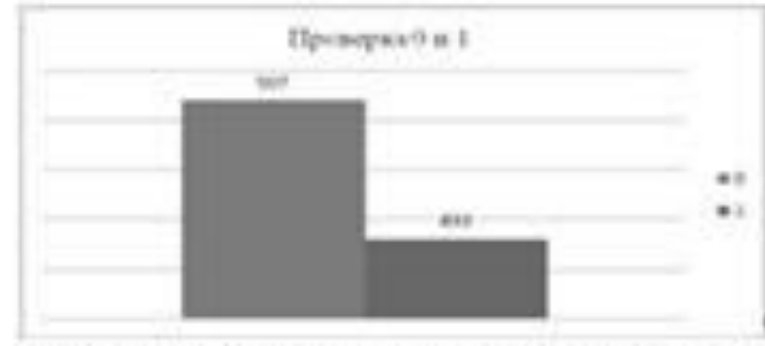
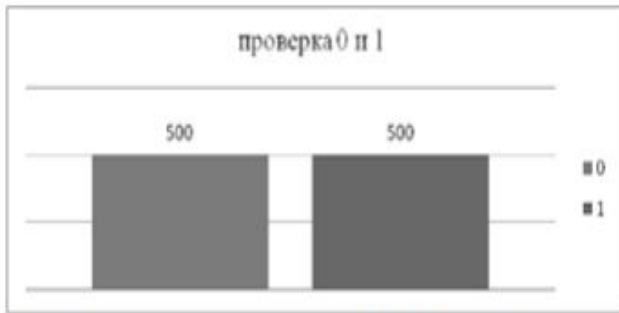


Рисунок 6 Проверка серий для генератора Гейфа (схема Фибоначи) та Гоффа (схема Галуа)

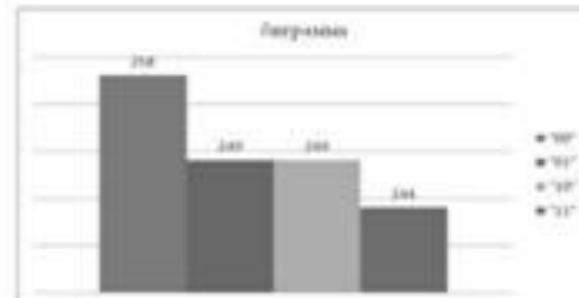
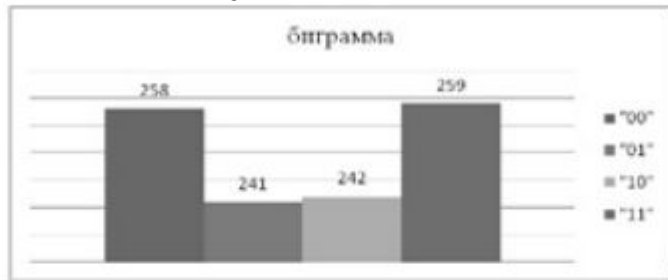


Рисунок 7 Частота зустрічних біграмм для генератора Гейфа (схема Фибоначи) та Гоффа (схема Галуа)

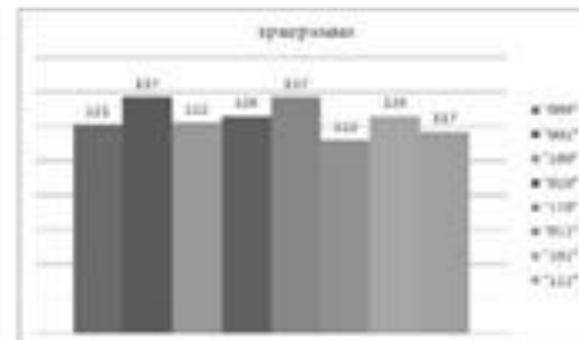
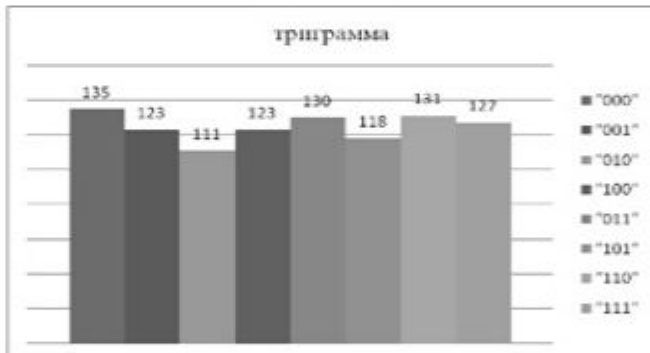


Рисунок 8 Частота зустрічних триграмм для генератора Гейфа (схема Фибоначи) та Гоффа (схема Галуа)



- Один поліном виду

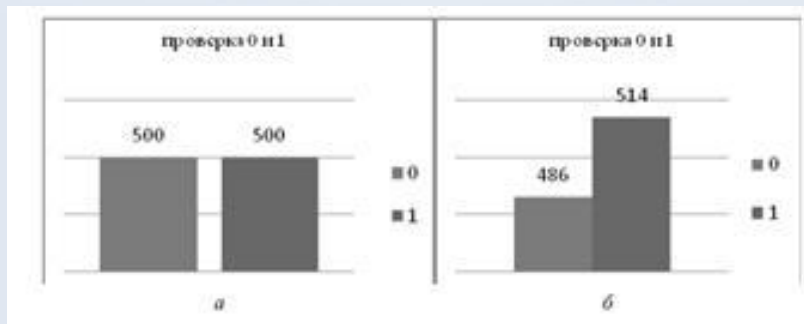
$$x^{24} + x^4 + x^3 + x + 1,$$

- Три різних полінома виду

$$x^{19} + x^{18} + x^{17} + x^{14} + 1,$$

$$x^{22} + x^{21} + 1,$$

$$x^{23} + x^{22} + x^{18} + x^7 + 1.$$



# ВИСНОВКИ

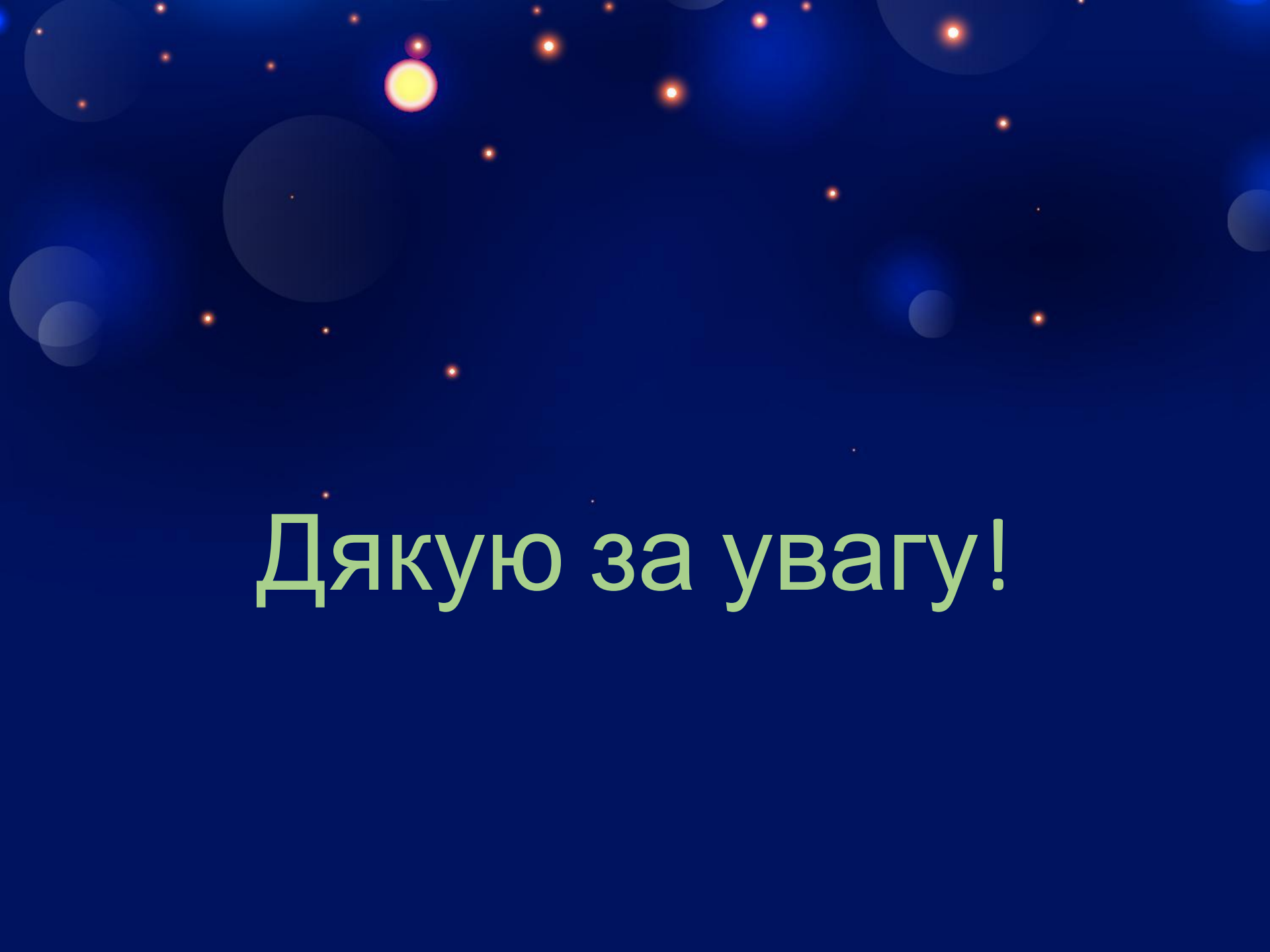
- Можна зробити наступні висновки про ефективність такого алгоритму Фібоначі

## Переваги:

- висока швидкодія криптографічних алгоритмів, що створюються на основі РСЛОС (наприклад, поточкових шифрів);
- застосування тільки найпростіших бітових операцій додавання і множення, апаратно реалізованих практично у всіх обчислювальних пристроях;
- хороші криптографічні властивості (РСЛОС можуть генерувати послідовності великого періоду з хорошими статистичними властивостями);
- завдяки своїй структурі, РСЛОС легко аналізуються з використанням алгебраїчних методів.

## Недоліки:

- Одна з головних проблем РСЛОС в тому, що їх програмна реалізація вкрай неефективна: доводиться уникати розріджених многочленів зворотного зв'язку, так як вони призводять до полегшення злому реляційним розкриттям, а щільні многочлени дуже повільно прораховуються. Тому програмна реалізація такого генератора працює не швидше, ніж реалізація DES.
- Лінійність послідовності на виході регістра дозволяє однозначно визначити многочлен зворотного зв'язку  $C(x)$  по  $2L$  послідовним бітам за допомогою алгоритму Берлекемпа - Мессі або алгоритму Евкліда.
- Відносна легкість аналізу алгебраїчними методами не тільки полегшує розробку, але і збільшує шанси на злом генератора на базі РСЛОС.



Дякую за увагу!