# ПІДВИЩЕННЯ СТІЙКОСТІ КРИПТОАЛГОРИТМУ RSA У СИСТЕМАХ ЗАХИСТУ ІНФОРМАЦІЇ ЗА РАХУНОК ГЕНЕТИЧНОЇ ОПТИМІЗАЦІЇ

Виконав: Цимбал О. І.
Керівник: Яремчук Ю. Є.

# Актуальність

Актуальність вдосконалення криптостійкості алгоритму RSA рівнозначна важливості цілісності комерційних та персональних даних.

RSA – є одним з найпоширенішим криптографічним алгоритмом в світі, що постійно робить його об'єктом атак, це і є основною рушійною силою дослідів по підвищенню криптостійкості даного алгоритму, та знаходження нових можливостей для його вдосконалення.

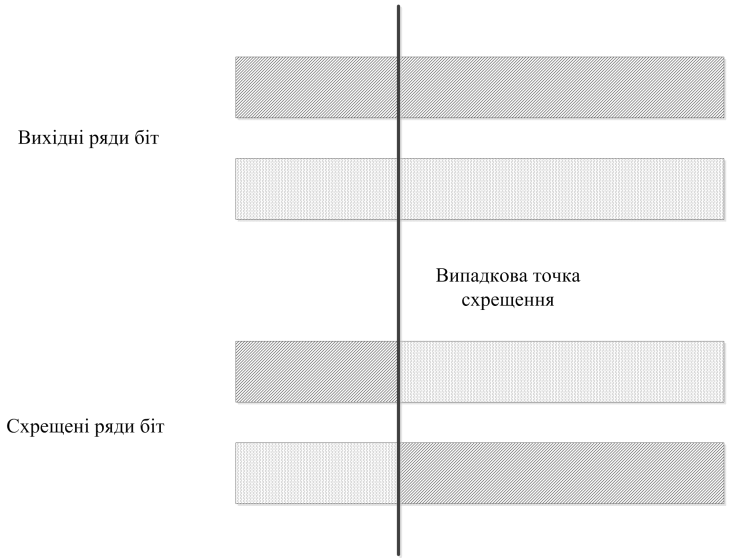
# ПОСТАНОВКА ЗАДАЧІ

1. Виконати аналіз взаємодії сучасних асиметричних алгоритмів шифрування з генетичним алгоритмом.
2. Підвищити криптостійкість симетричного шифру RSA шляхом використання генетичного алгоритму.
3. Представити результати дослідження у вигляді зручному для кінцевого користувача.

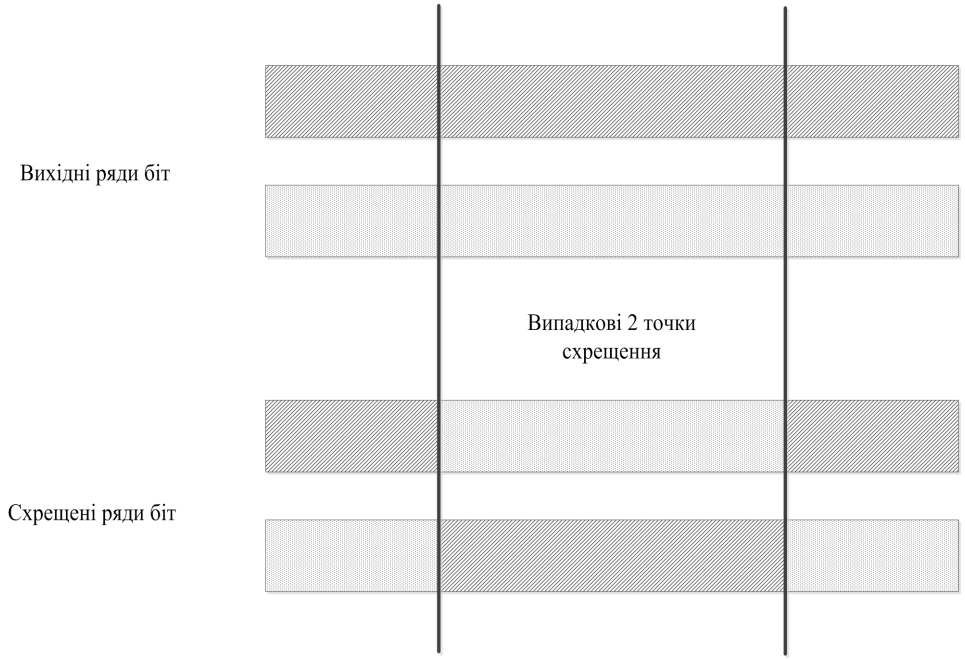
| Позиція біта | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|---|
| До мутації | 1 | 1 | 0 | 0 | **0** | 0 | 0 | 0 |
| Після мутації | 1 | 1 | 0 | 0 | **1** | 0 | 0 | 0 |

# Процес мутації

# Оператори схрещення




Приклад одиночного схрещення



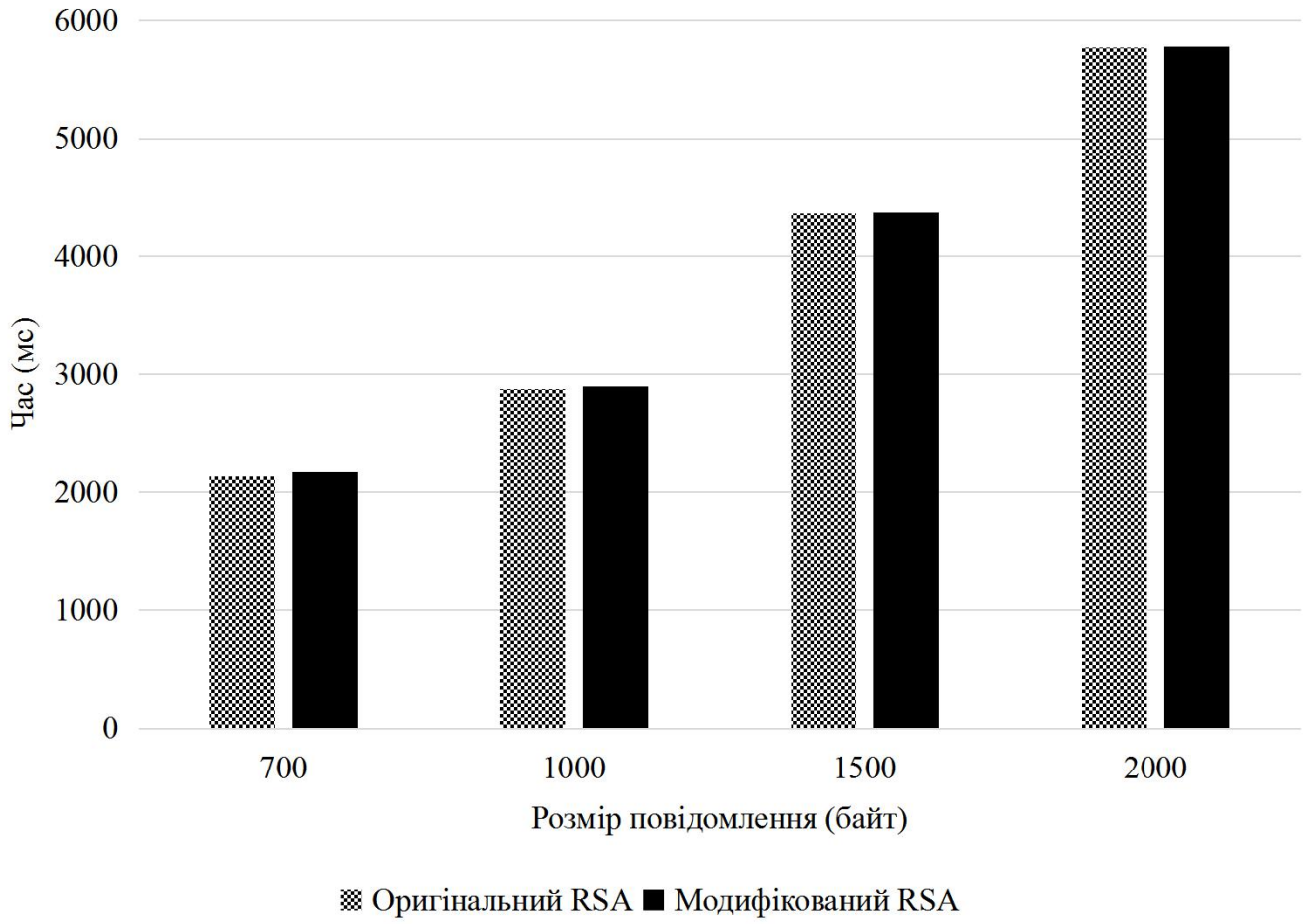

Приклад подвійного схрещення

# Порівняння швидкості шифрування та дешифрування

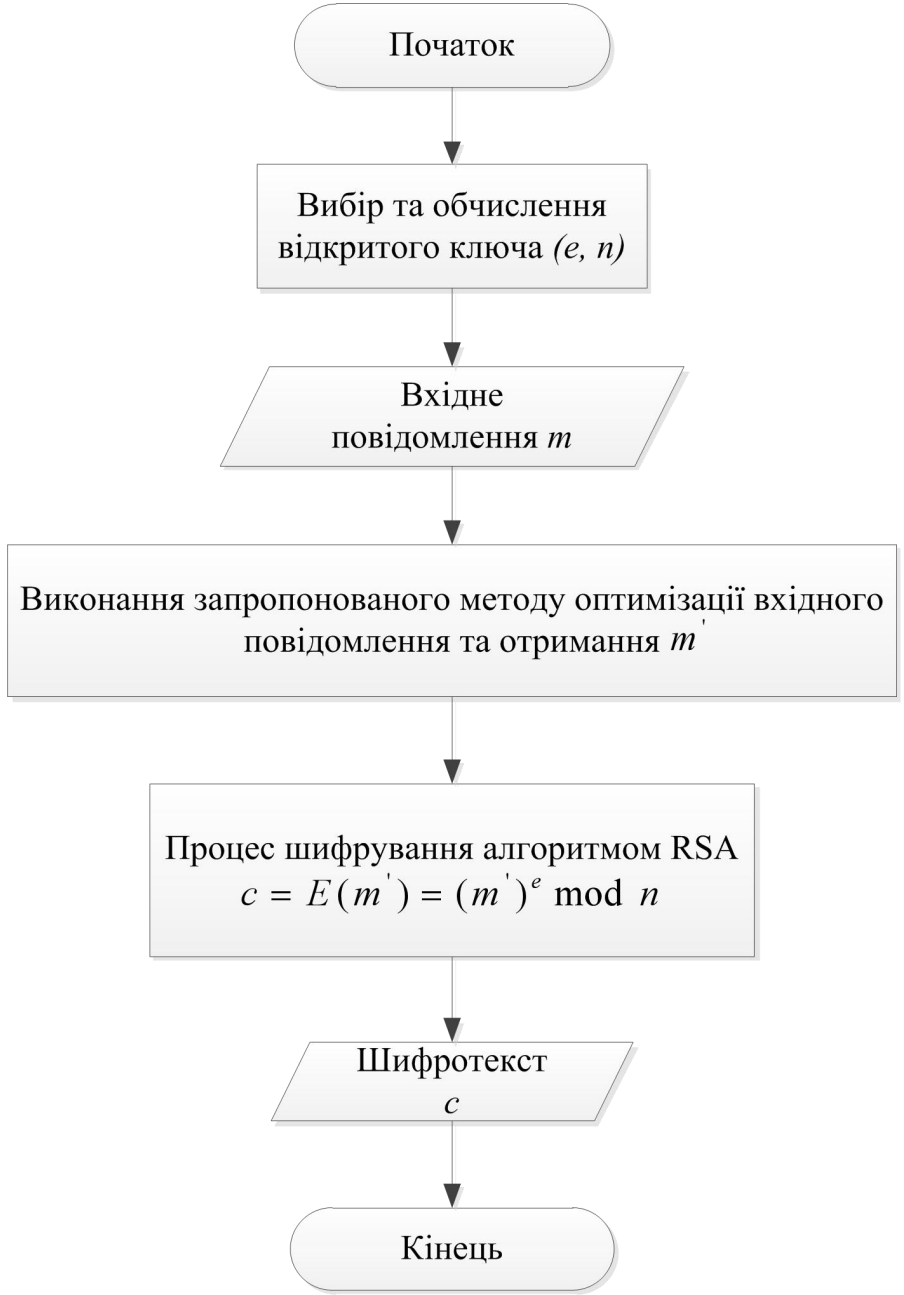
| | Час (мс) | | | |
|---|---|---|---|---|
| Розмір повідомлення (байт) | Шифрування | | Дешифрування | |
| | Оригінальний RSA | Модифікований RSA | Оригінальний RSA | Модифікований RSA |
| 700 | 19 | 23 | 2134 | 2168 |
| 1000 | 23 | 25 | 2874 | 2901 |
| 1500 | 36 | 37 | 4359 | 4372 |
| 2000 | 47 | 47 | 5772 | 5781 |

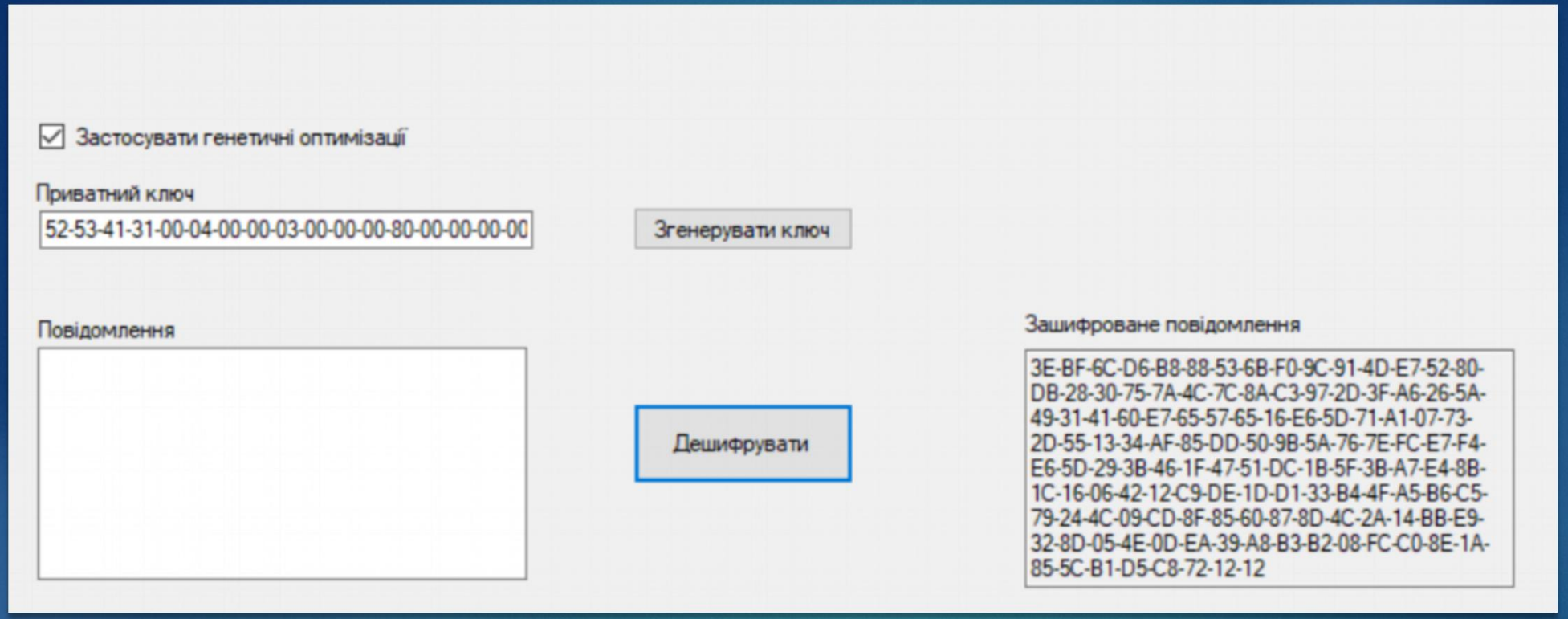
# Результати статистичних замірів швидкості шифрування оригінального алгоритму RSA та модифікованого

# Результати статистичних замірів швидкості дешифрування повідомлення оригінальним алгоритмом RSA та модифікованим



# Блок-схема роботи алгоритму шифрування RSA на основі запропонованого алгоритму оптимізації вихідного повідомлення за допомогою ГА






# Головне вікно програми

# ДЯКУЮ ЗА УВАГУ