

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.



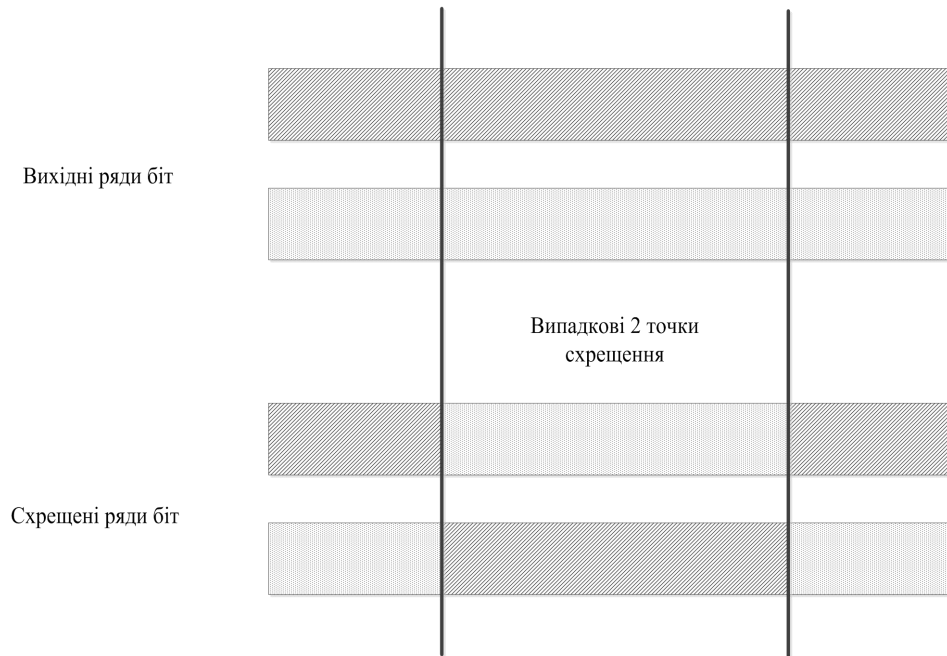
Позиція біта	0	1	2	3	4	5	6	7
До мутації	1	1	0	0	<b>0</b>	0	0	0
Після мутації	1	1	0	0	<b>1</b>	0	0	0

Процес мутації

# Оператори схрещення



Приклад одиночного схрещення



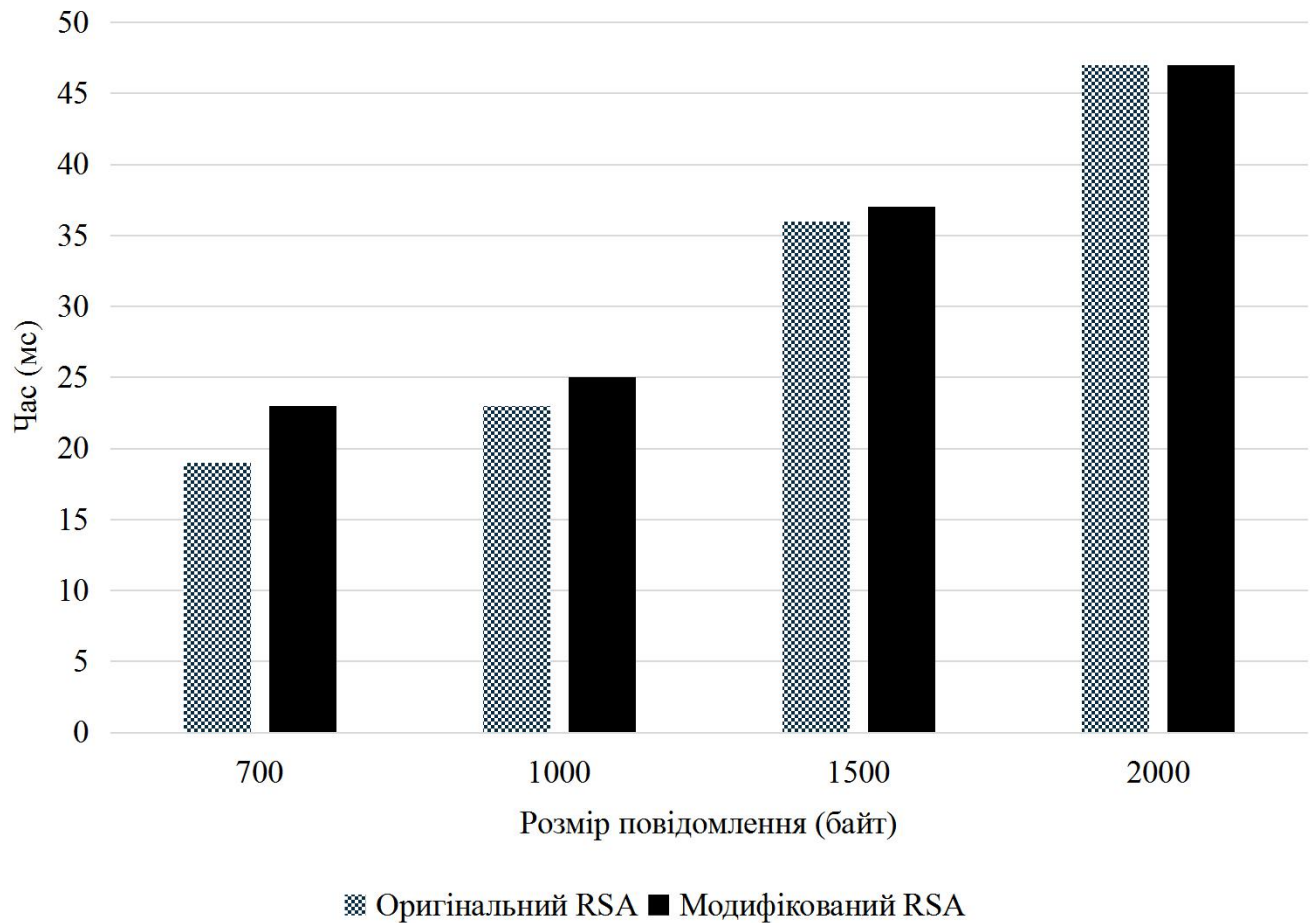
Приклад подвійного схрещення

# Порівняння швидкості шифрування та дешифрування

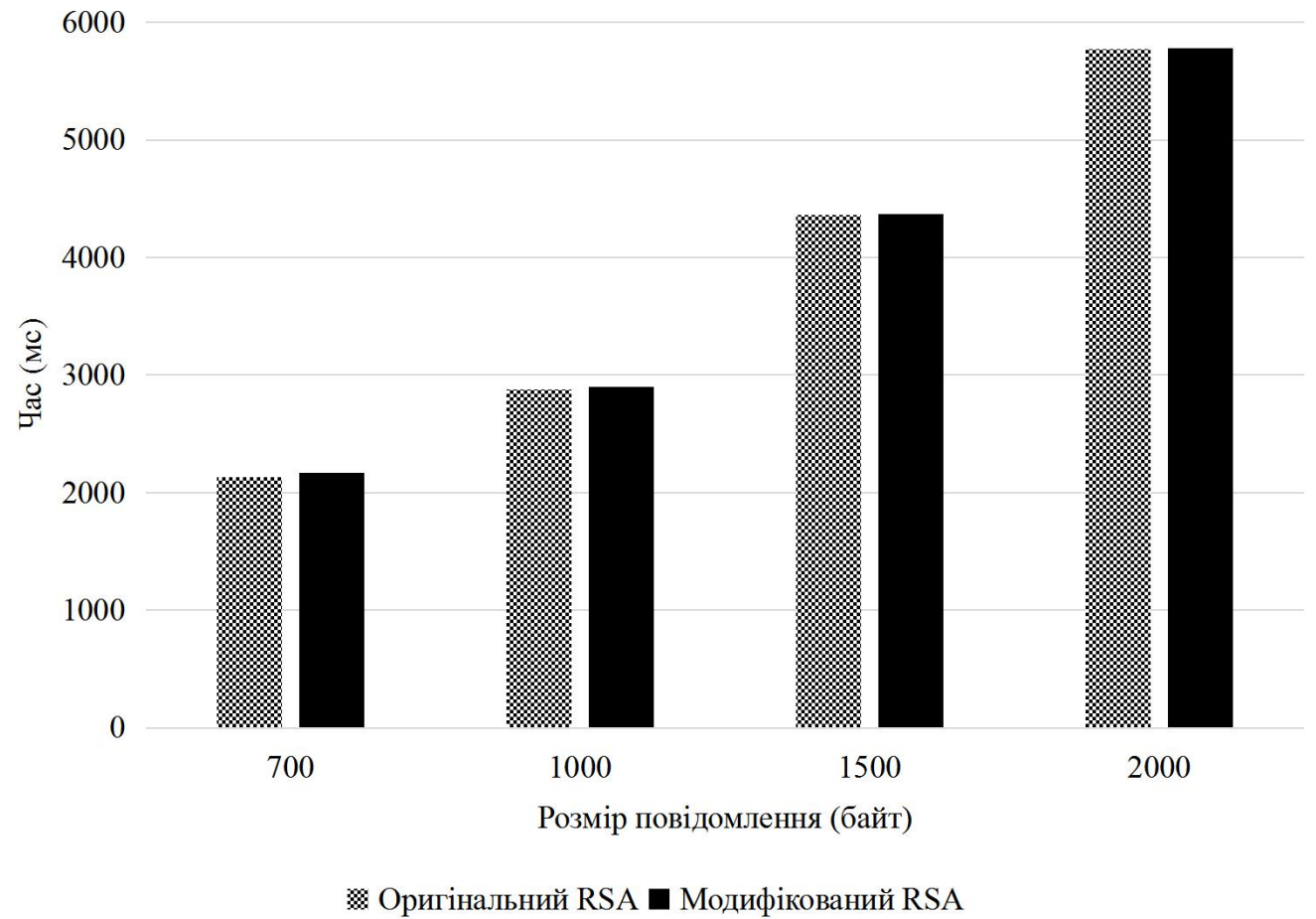
Розмір повідомлення (байт)	Час (мс)			
	Шифрування		Дешифрування	
	Оригінальний RSA	Модифікований RSA	Оригінальний RSA	Модифікований RSA
700	19	23	2134	2168
1000	23	25	2874	2901
1500	36	37	4359	4372
2000	47	47	5772	5781



Результати  
статистичних  
замірів швидкості  
шифрування  
оригінального  
алгоритму RSA  
та модифікованого

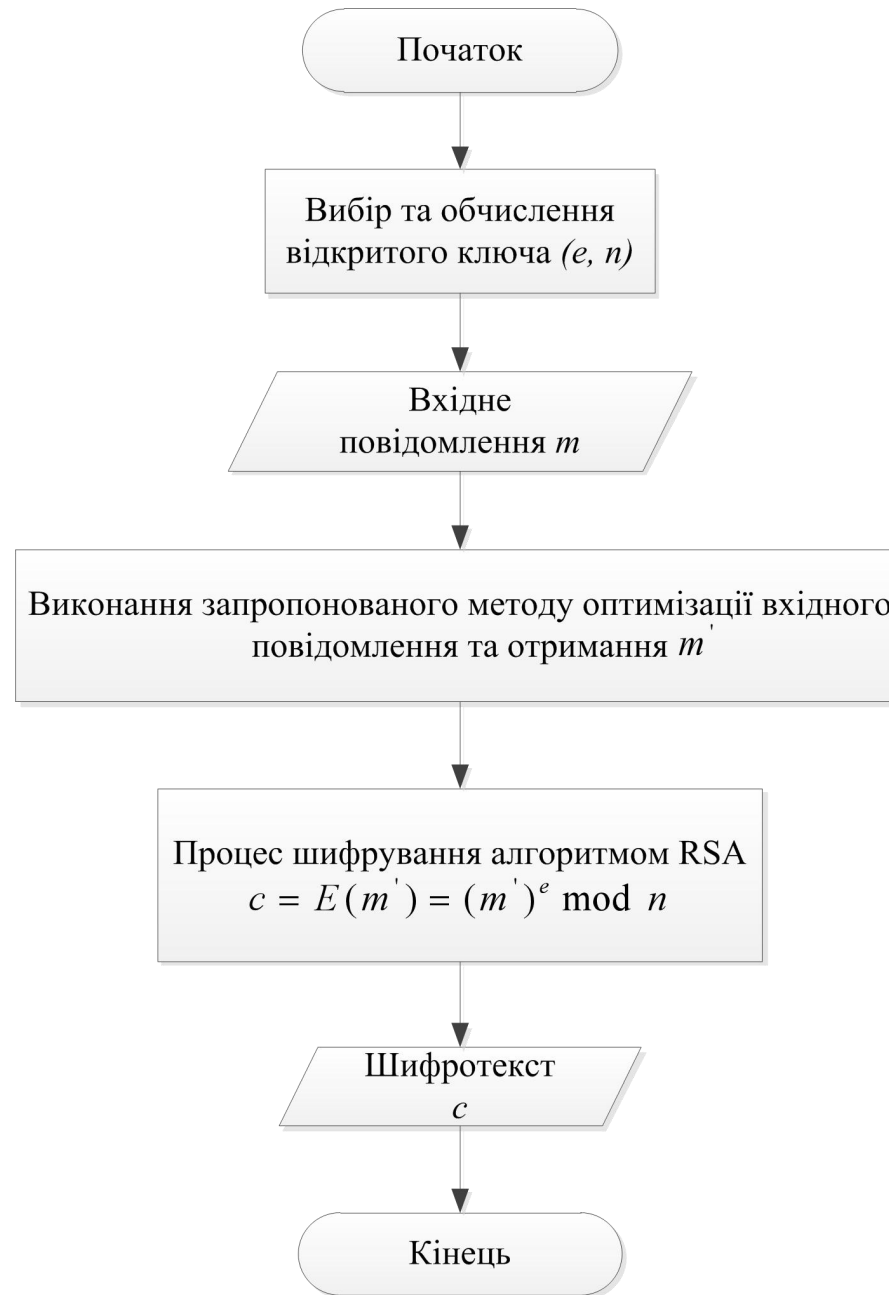


Результати  
статистичних  
замірів швидкості  
дешифрування  
повідомлення  
оригінальним  
алгоритмом RSA  
та модифікованим





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



Застосувати генетичні оптимізації

Приватний ключ

52-53-41-31-00-04-00-00-03-00-00-00-80-00-00-00-00

Згенерувати ключ

Повідомлення

Дешифрувати

Зашифроване повідомлення

3E-BF-6C-D6-B8-88-53-6B-F0-9C-91-4D-E7-52-80-  
DB-28-30-75-7A-4C-7C-8A-C3-97-2D-3F-A6-26-5A-  
49-31-41-60-E7-65-57-65-16-E6-5D-71-A1-07-73-  
2D-55-13-34-AF-85-DD-50-9B-5A-76-7E-FC-E7-F4-  
E6-5D-29-3B-46-1F-47-51-DC-1B-5F-3B-A7-E4-8B-  
1C-16-06-42-12-C9-DE-1D-D1-33-B4-4F-A5-B6-C5-  
79-24-4C-09-CD-8F-85-60-87-8D-4C-2A-14-BB-E9-  
32-8D-05-4E-0D-EA-39-A8-B3-B2-08-FC-C0-8E-1A-  
85-5C-B1-D5-C8-72-12-12

Головне вікно програми





ДЯКУЮ ЗА УВАГУ