UNIVERSITY OF INFORMATION TECHNOLOGY
FACULTY OF COMPUTER NETWORK AND COMMUNICATION

CRYPTOGRAPHY

Report Lab 3

RSA-OAEP Cipher using Crypto++

Lecturer:	Nguyễn Ngọc Tự
Class:	NT219.O21.ANTT.2
Student:	Trần Thế Hữu Phúc
Student ID Number:	22521143

Hồ Chí Minh City, June 2024

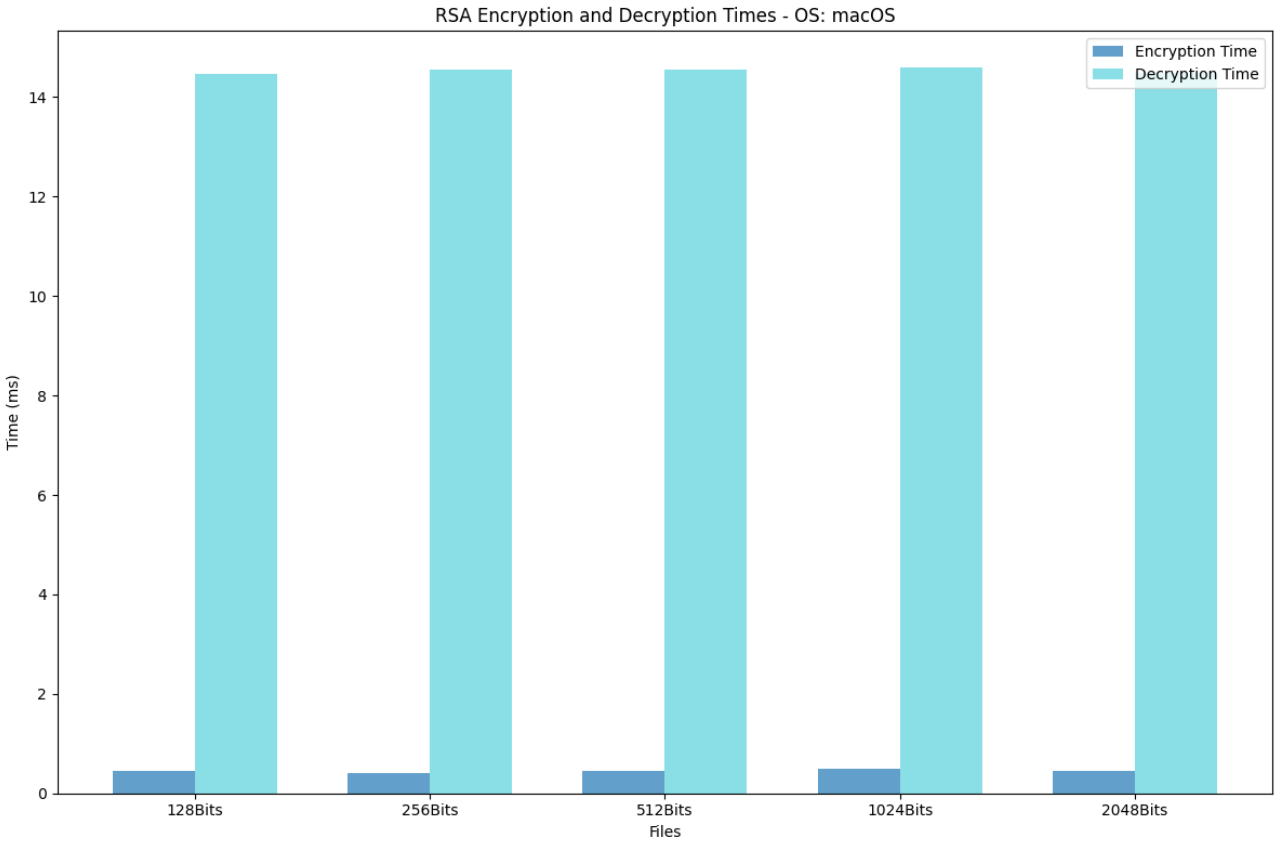
1. Hardware Resources

Device	MacBook Pro
Chip	Apple M1 • 8-core CPU • 8-core GPU • 16-core Neural Engine
Memory	8GB LPDDR4
Storage	256GB SSD
Operating Systems	• macOS 14.5 Sonoma • Windows 11 Pro Version 23H2 • Ubuntu 22.04.4 LTS

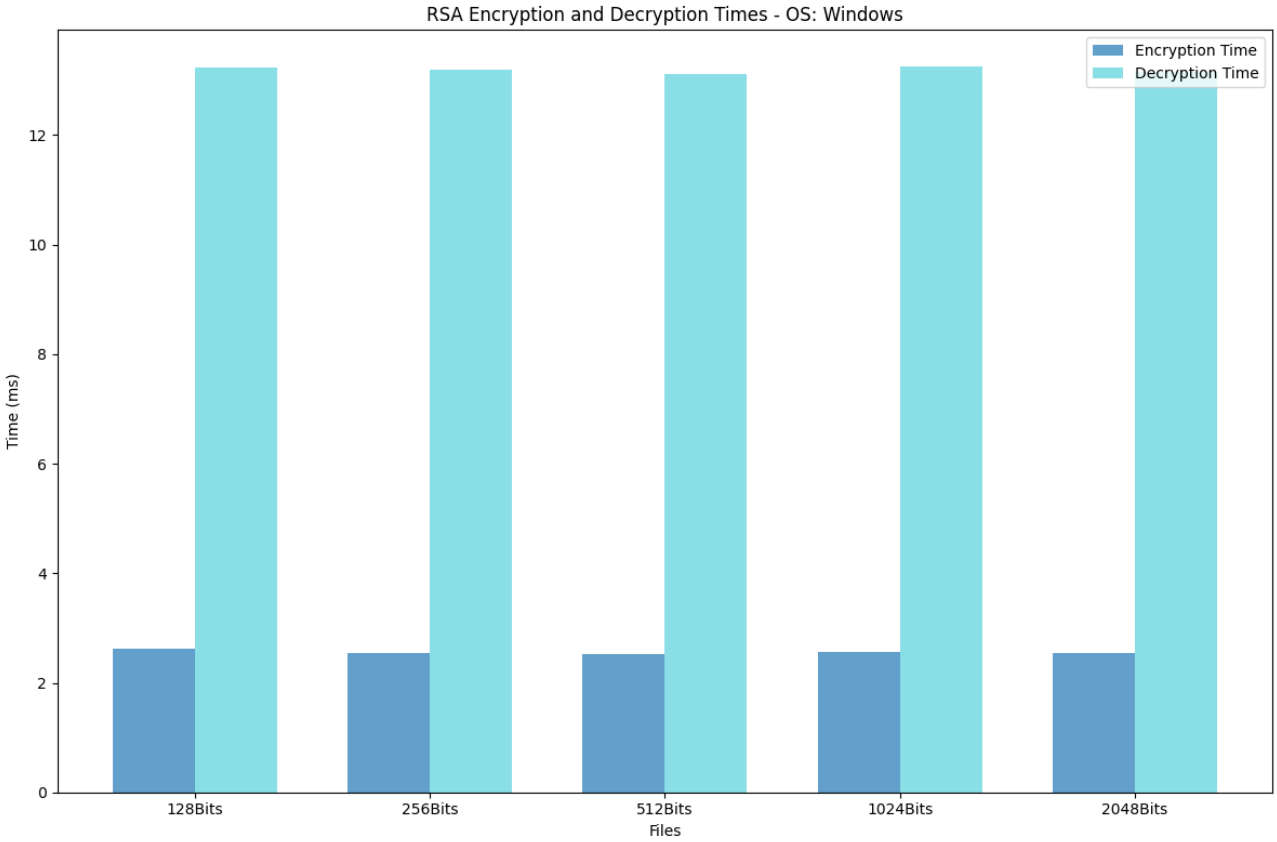
2. Computation performance on macOS, Windows and Linux

RSA on all platforms (miliseconds)						
OS		Input Size				
		128 Bits	256 Bits	512 Bits	1024 Bits	2024 Bits
macOS	Encrypt	0.455	0.416	0.450	0.501	0.444
	Decrypt	14.455	14.554	14.542	14.599	14.480
Windows	Encrypt	2.628	2.549	2.519	2.563	2.548
	Decrypt	13.225	13.197	13.109	13.256	13.151
Linux	Encrypt	0.768	0.792	0.785	0.805	0.775
	Decrypt	12.110	12.419	12.324	12.158	12.174

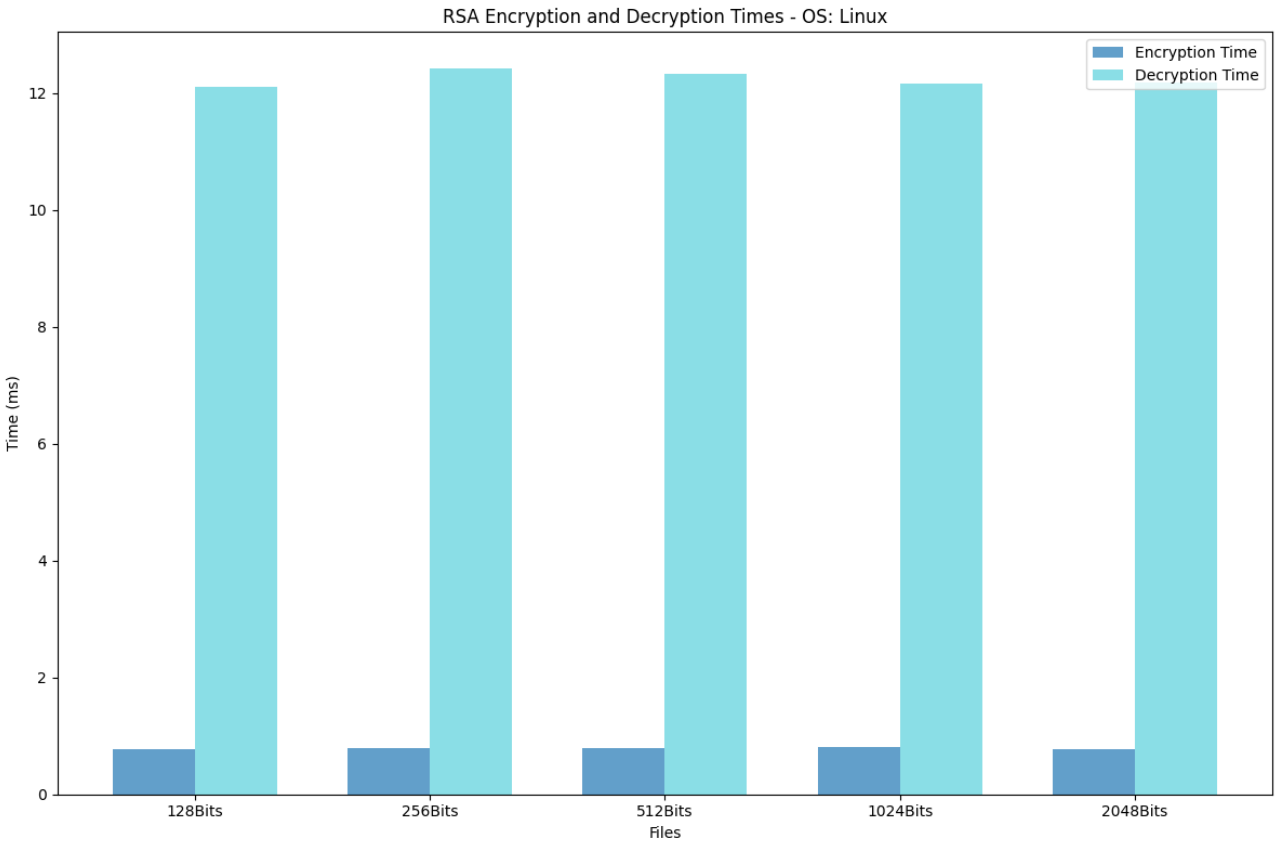
- **RSA on macOS:**



- **RSA on Windows:**



- **RSA on Linux:**



⌥ Phân tích và so sánh

So sánh:

- macOS:
  - Thời gian mã hóa khá ổn định với các kích thước đầu vào khác nhau. Thời gian dao động từ 0.416 ms đến 0.501 ms, cho thấy một sự tăng nhẹ khi kích thước đầu vào lớn hơn nhưng vẫn khá gần nhau.
  - Thời gian giải mã cao hơn một chút so với Linux nhưng cũng cho thấy sự ổn định với các kích thước đầu vào khác nhau. Thời gian dao động từ 14.455 ms đến 14.599 ms, cho thấy sự biến động tối thiểu.
- Windows:
  - Thời gian mã hóa cao hơn đáng kể so với Linux và macOS. Thời gian dao động từ 2.519 ms đến 2.628 ms, cho thấy một sự biến động nhỏ nhưng luôn cao hơn hai hệ điều hành còn lại.
  - Thời gian giải mã nằm giữa thời gian của Linux và macOS. Thời gian dao động từ 13.109 ms đến 13.256 ms, với sự biến động nhỏ tương tự như các hệ điều hành khác.
- Linux:
  - Thời gian mã hóa tương đối ổn định với các kích thước đầu vào khác nhau. Thời gian dao động từ 0.768 ms đến 0.805 ms, không có sự gia tăng đáng kể khi kích thước tệp tăng lên.
  - Thời gian giải mã tương đối ổn định với các kích thước đầu vào khác nhau, giống như thời gian mã hóa. Thời gian dao động từ 12.110 ms đến 12.419 ms, với sự dao động nhỏ.

Tổng quan:

- **Sự ổn định qua các kích thước tệp**: Cả ba hệ điều hành đều thể hiện thời gian mã hóa và giải mã tương đối ổn định qua các kích thước đầu vào khác nhau (từ 128 bits đến 2048 bits).
- Sự khác biệt về hiệu năng:
  - **Linux**: Cho thấy thời gian mã hóa nhanh nhất trong ba hệ điều hành, với thời gian rất ổn định và thấp.
  - **macOS**: Thời gian mã hóa chậm hơn một chút so với Linux nhưng vẫn khá thấp. Thời gian giải mã cao nhất trong ba hệ điều hành.
  - **Windows**: Thời gian mã hóa chậm nhất, cao hơn đáng kể so với Linux và macOS, nhưng thời gian giải mã lại tốt hơn macOS mặc dù vẫn chậm hơn Linux.