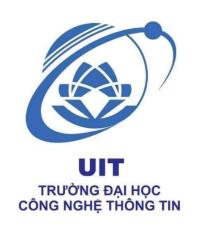
UNIVERSITY OF INFORMATION TECHNOLOGY FACULTY OF COMPUTER NETWORK AND COMMUNICATION



CRYPTOGRAPHY

Report Lab 2 Coding AES using only C++ without other cryptographic external libraries

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 SonomaWindows 11 Pro Version 23H2Ubuntu 22.04.4 LTS

2. Computation performance on macOS, Windows and Linux

0.0		Input Size						
O	OS		256KB	512KB	1MB	8MB	16MB	
macOS	Encrypt	0.295	0.878	1.452	2.574	19.228	38.772	
	Decrypt	0.291	0.689	0.964	1.781	11.857	23.824	
	Encrypt	5.258	8.679	9.454	12.542	60.852	122.947	
Windows	Decrypt	5.319	9.042	9.071	10.864	48.754	98.614	
Linux	Encrypt	2.808	8.069	13.714	25.302	172.820	331.254	
	Decrypt	2.823	7.581	13.190	24.859	164.950	315.734	
300 - 250 - 200 -	Comparison o	f AES CBC Encryption and I	Decryption Times Across Op	erating Systems and Input	Files	AES	CBC Encryption - 1KB.txt CBC Decryption - 1KB.txt CBC Decryption - 256KB.txt CBC Decryption - 256KB.txt CBC Decryption - 512KB.txt CBC Decryption - 512KB.txt CBC Decryption - 512KB.txt CBC Decryption - 1MB.txt CBC Decryption - 1MB.txt CBC Decryption - 8MB.txt CBC Decryption - 8MB.txt CBC Decryption - 1MB.txt CBC Decryption - 1MB.txt CBC Decryption - 1MB.txt	

N Phân tích và so sánh

Nhận xét chung:

- Windows có thời gian thực hiện cao hơn so với macOS và Linux trên hầu hết các kích thước tập tin đầu vào.
- macOS thường có thời gian thực hiện tốt hơn Linux đối với các tập tin lớn, trong khi Linux thường tốt hơn cho các tập tin nhỏ.
- Linux có thể có thời gian thực hiện lớn nhất, đặc biệt là với các tập tin lớn, có thể do sự khác biệt trong triển khai mã hóa/giải mã trên các nền tảng.

So sánh chi tiết:

- Windows:

- O Thời gian mã hóa và giải mã trung bình của Windows cao hơn so với macOS và Linux đối với tất cả các kích thước tập tin đầu vào.
- Windows có thời gian mã hóa và giải mã lớn nhất đối với các tập tin lớn, như 8MB và 16MB.

- macOS:

- Thời gian thực hiện của macOS tương đối nhỏ hơn so với Windows và Linux, đặc biệt là đối với các tập tin lớn.
- O Thời gian mã hóa và giải mã của macOS tăng dần theo kích thước tập tin đầu vào.

- Linux:

- Linux thường có thời gian thực hiện cao nhất đối với cả mã hóa và giải mã, đặc biệt là với các tập tin lớn như 8MB và 16MB.
- Đối với các tập tin nhỏ hơn, thời gian thực hiện của Linux cũng tương đối cao so với macOS.