**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**

**KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**

A blue logo with a black background

Description automatically generated

**BÁO CÁO BÀI TẬP THỰC HÀNH**

**LAB 2 OFF CLASS**

**MÔN HỌC: MẬT MÃ HỌC**

**Họ và tên: LẠI QUAN THIÊN**

**Mã số sinh viên: 22521385**

**Lớp: NT219.O21.ANTT**

**TP. HỒ CHÍ MINH, THÁNG 06 NĂM 2024**

**MỤC LỤC**

[PHẦN I: TỔNG QUAN VÀ MÔ TẢ 2](#_Toc169535399)

[1.1. Thông tin cá nhân: 2](#_Toc169535400)

[1.2. Thông tin thiết bị: 2](#_Toc169535401)

[PHẦN II: NỘI DUNG THỰC HÀNH 5](#_Toc169535402)

[AES - Advanced Encryption Standard: 5](#_Toc169535403)

[2.2.1. Bảng thống kê số liệu thực nghiệm: 5](#_Toc169535404)

[2.2.2. Biểu đồ cột so sánh các mode: 7](#_Toc169535405)

[2.2.3. Biểu đồ đường so sánh hai hệ điều hành: 9](#_Toc169535406)

[2.2.4. Phân tích và so sánh: 10](#_Toc169535407)

[2.3. Tổng kết: 10](#_Toc169535408)

# PHẦN I: TỔNG QUAN VÀ MÔ TẢ

## 1.1. Thông tin cá nhân:

Họ và tên: Lại Quan Thiên

Mã số sinh viên: 22521385

Lớp thực hành: NT219.O21.ANTT.1

Link github: [Cryptography-Course/Labs/OffClass/Lab\_2 at main · WanThinnn/Cryptography-Course (github.com)](https://github.com/WanThinnn/Cryptography-Course/tree/main/Labs/OffClass/Lab_2)

## 1.2. Thông tin thiết bị:

**- Thiết bị:** Macbook Air 2019 – RAM 8GB (LPDDR3 2133MHz) – SSD 128GB

**- Hệ điều hành:**

+ Windows 11 Pro (cài đặt thông qua Bootcamp của Apple)

+ Ubuntu 22.04 Jammy Jellyfish (cài đặt thông qua [t2linux.org](https://t2linux.org/))

**- Bộ xử lý:**

+ Intel Core i5 8210Y – 1.60GHz – Turbo Boost 3.60Ghz

+ Intel UHD Graphics 617

+ Apple T2 Security Chip

**- Thông tin về bộ xử lý:**

+ [Intel Core i58210Y Processor 4M Cache up to 3.60 GHz Thông số kỹ thuật sản phẩm](https://ark.intel.com/content/www/vn/vi/ark/products/189912/intel-core-i5-8210y-processor-4m-cache-up-to-3-60-ghz.html)

+ [Hỗ trợ Intel® UHD Graphics 617](https://www.intel.vn/content/www/vn/vi/support/products/189913/graphics/processor-graphics/intel-uhd-graphics-family/intel-uhd-graphics-617.html)

+ [Apple T2 Security Chip: Security Overview](https://www.apple.com/jp/mac/docs/Apple_T2_Security_Chip_Overview.pdf)

- Các thực nghiệm được thực thi trong quá trình laptop cắm điện, nhiệt độ phòng

A screenshot of a computer

Description automatically generated

**1.3. Tổng quan:**

Bài báo cáo bao gồm: Báo cáo code thuật toán AES-CBC bằng ngôn ngữ C++ và không sử dụng thư viện CryptoPP. Sau khi xây dựng code thì tiến hành tạo sáu file test case với kích thước khác nhau, thực hiện đo thời gian 10 000 lần mã hóa/giải mã trên cả hai Hệ điều hành Windows và Linux. Viết bảng thống kê số liệu và vẽ biểu đồ phân tích và so sánh.

Dưới đây là hình ảnh minh hoạ phần code chạy 10 000 lần của AES-CBC (bao gồm toàn bộ quá trình load file, check format, thực hiện mã hoá/giải mã và lưu/xuất file):

A computer screen shot of text

Description automatically generated

# PHẦN II: NỘI DUNG THỰC HÀNH

## 2.1. AES - Advanced Encryption Standard:

### 2.2.1. Bảng thống kê số liệu thực nghiệm:

Dưới đây là bảng thống kê chi tiết thời gian encrypt/decrypt của từng mode (đơn vị thời gian: ms):

#### 2.2.1.1. Hệ điều hành Windows 11:

* **Bảng thời gian trung bình 10 000 lần Encrypt:**

|  |  |
| --- | --- |
| **Encrypt** | **CBC** |
| File 1 (1KB) | 2.2081 |
| File 2 (10KB) | 19.1816 |
| File 3 (55KB) | 93.3161 |
| File 4 (104KB) | 166.4044 |
| File 5 (1.1MB) | 1998.1873 |
| File 6 (5.2MB) | 7939.1851 |

* **Bảng thời gian trung bình 10 000 lần Decrypt:**

|  |  |
| --- | --- |
| **Decrypt** | **CBC** |
| File 1 (1KB) | 2.5178 |
| File 2 (10KB) | 20.6107 |
| File 3 (55KB) | 106.0573 |
| File 4 (104KB) | 193.4348 |
| File 5 (1.1MB) | 1993.7913 |
| File 6 (5.2MB) | 9678.9115 |

#### 2.2.1.2. Hệ điều hành Ubuntu 22.04 (Linux):

* **Bảng thời gian trung bình 10 000 lần Encrypt:**

|  |  |
| --- | --- |
| **Encrypt** | **CBC** |
| File 1 (1KB) | 1.8011 |
| File 2 (10KB) | 14.5623 |
| File 3 (55KB) | 82.21 |
| File 4 (104KB) | 153.08 |
| File 5 (1.1MB) | 2074.5829 |
| File 6 (5.2MB) | 7785.3945 |

* **Bảng thời gian trung bình 10 000 lần Decrypt:**

|  |  |
| --- | --- |
| **Decrypt** | **CBC** |
| File 1 (1KB) | 2.3193 |
| File 2 (10KB) | 18.6518 |
| File 3 (55KB) | 124.01 |
| File 4 (104KB) | 232.05 |
| File 5 (1.1MB) | 2227.6503 |
| File 6 (5.2MB) | 9669.6195 |

### 2.2.2. Biểu đồ cột so sánh các mode:

Dựa theo số liệu từ các bảng ở trên, vẽ biểu đồ để dễ dàng so sánh một cách trực quang:

#### 2.2.2.1. Hệ điều hành Windows 11:

* **Biểu đồ thời gian trung bình 10 000 lần Encrypt:**
* **Biểu đồ thời gian trung bình 10 000 lần Decrypt:**

#### 2.2.2.1. Hệ điều hành Ubuntu 22.04 (Linux):

* **Biểu đồ thời gian trung bình 10 000 lần Encrypt:**
* **Biểu đồ thời gian trung bình 10 000 lần Decrypt:**

### 2.2.3. Biểu đồ cột so sánh hai hệ điều hành:

Dưới đây là biểu đồ so sánh thời gian mã hoá và giải mã file 5.2 MB trên 2 hệ điều hành:

### 2.2.4. Phân tích và so sánh:

- Thời gian thực thi sẽ tăng dần theo kích thước file đầu vào, file càng lớn thì thời gian càng lâu.

- Thời gian mã hoá và giải mã sẽ chậm hơn đáng kể so với thuật toán sử dụng thư viện CryptoPP

- Tương tự như Lab 1 Offclass, thì thời gian thực thi trên Linux vẫn nhanh hơn so với Windows. Linux thường được tối ưu hóa cho hiệu suất và quản lý tài nguyên hiệu quả. Các phiên bản Linux có thể được cấu hình đặc biệt để giảm thiểu overhead của hệ điều hành, giúp các tác vụ tính toán nặng như mã hóa và giải mã chạy nhanh hơn. Windows có nhiều dịch vụ chạy nền và các yếu tố khác có thể tiêu tốn tài nguyên hệ thống, làm giảm hiệu suất tổng thể. Ngoài ra còn có các yếu tố khác như: Kiến trúc hệ điều hành, Quản lý bộ nhớ, Hệ thống tập tin, Sự tối ưu trên cả hệ điều hành, Sự tối ưu của nhà sản xuất cho thiết bị của mình.

## 2.3. Tổng kết:

Sau bài lab này, từ việc code tay AES-CBC mà không sử dụng thư viện CryptoPP thì em đã hiểu được cách mà thuật toán AES-CBC thực thi và có cái nhìn tổng quát về thời gian thực thi của thuật toán như thế nào đối với từng kích thước file, và cũng nhận thấy sự khác biệt giữa thực thi trên Linux và trên Windows.