

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**  
**KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG**

---



**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

<b>PHẦN I: TỔNG QUAN VÀ MÔ TẢ .....</b>	<b>2</b>
<b>1.1. Thông tin cá nhân: .....</b>	<b>2</b>
<b>1.2. Thông tin thiết bị: .....</b>	<b>2</b>
<b>PHẦN II: NỘI DUNG THỰC HÀNH .....</b>	<b>5</b>
<b>AES - Advanced Encryption Standard:.....</b>	<b>5</b>
2.2.1. Bảng thống kê số liệu thực nghiệm: .....	5
2.2.2. Biểu đồ cột so sánh các mode:.....	7
2.2.3. Biểu đồ đường so sánh hai hệ điều hành: .....	9
2.2.4. Phân tích và so sánh:.....	10
<b>2.3. Tổng kết: .....</b>	<b>10</b>

# 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)

## 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](#)

+ [Hỗ trợ Intel® UHD Graphics 617](#)

+ [Apple T2 Security Chip: Security Overview](#)

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

← Settings



Thiên Lai

Thienlai159@gmail.com

Find a setting

System

Bluetooth & devices

Network & internet

Personalization

Apps

Accounts

Time & language

Gaming

Accessibility

Privacy & security

Windows Update

System > About

WanThinnn

MacBookAir8,2

Rename this PC

Device specifications

Copy

Device name

WanThinnn

Processor

Intel(R) Core(TM) i5-8210Y CPU @ 1.60GHz 1.60 GHz

Installed RAM

8.00 GB (7.87 GB usable)

Device ID

4127B833-3A3C-4677-A4EE-0A8BE8357059

Product ID

00331-10000-00001-AA648

System type

64-bit operating system, x64-based processor

Pen and touch

No pen or touch input is available for this display

Related links

Domain or workgroup

System protection

Advanced system settings

Windows specifications

Copy

Edition

Windows 11 Pro

Version

21H2

Installed on

05/05/2024

OS build

22000.2538


Experience

Windows Feature Experience Pack 1000.22001.1000.0

Microsoft Services Agreement

Microsoft Software License Terms

Search



1:16 PM  
17/06/2024

3

### 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 họa 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):

```
else if (action == "encrypt")
{
    if (argc != 8)
    {
        cerr << "Usage: " << argv[0] << " encrypt <KeyFileFormat> <KeyFile> <PlaintextFormat> <PlaintextFile> <CipherFormat> <CipherFile>" << endl;
        return;
    }
    auto start = std::chrono::high_resolution_clock::now();
    for (int i = 0; i < 10000; i++)
    {
        Encryption(argv[2], argv[3], argv[4], argv[5], argv[6], argv[7]);
    }
    auto stop = std::chrono::high_resolution_clock::now();
    auto duration = std::chrono::duration_cast<std::chrono::milliseconds>(stop - start);
    cout << "-----" << endl;
    cout << "Overview AES CBC Manual Encryption Test" << endl;
    cout << "Encryption time: " << duration.count() << " milliseconds" << endl;
    cout << "-----" << endl;
}
else if (action == "decrypt")
{
    if (argc != 8)
    {
        cerr << "Usage: " << argv[0] << " decrypt <KeyFileFormat> <KeyFile> <CipherFormat> <CipherFile> <RecoveredFileFormat> <RecoveredFile>" << endl;
        return;
    }
    auto start = std::chrono::high_resolution_clock::now();
    for (int i = 0; i < 10000; i++)
    {
        Decryption(argv[2], argv[3], argv[4], argv[5], argv[6], argv[7]);
    }
    auto stop = std::chrono::high_resolution_clock::now();
    auto duration = std::chrono::duration_cast<std::chrono::milliseconds>(stop - start);
    cout << "-----" << endl;
    cout << "Overview AES CBC Manual Decryption Test" << endl;
    cout << "Decryption time: " << duration.count() << " milliseconds" << endl;
    cout << "-----" << endl;
}
```

## 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:**

<b>Encrypt</b>	<b>CBC</b>
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:**

<b>Decrypt</b>	<b>CBC</b>
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

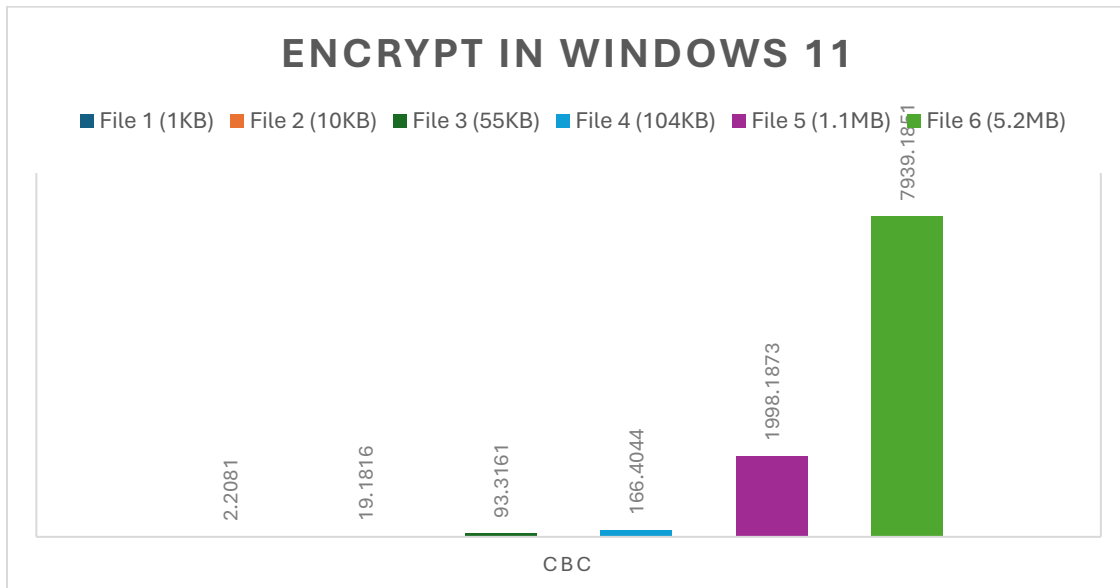


### 2.2.2. Biểu đồ cột so sánh các mode:

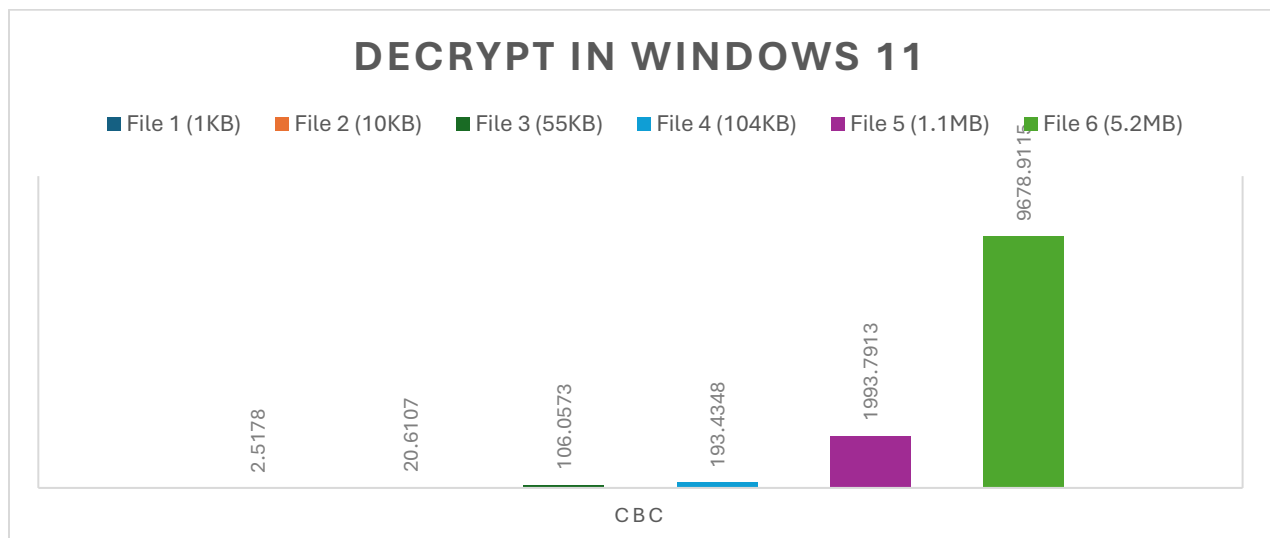
Dựa theo số liệu từ các bảng ở trên, vẽ biểu đồ để dễ dàng so sánh một cách trực quan:

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

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

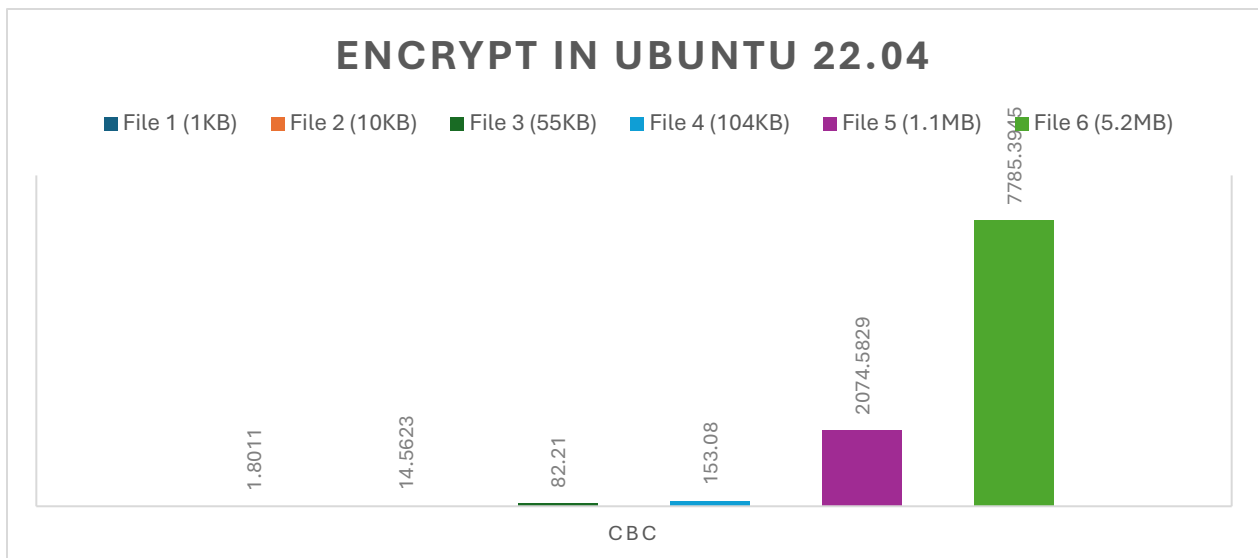


- **Biểu đồ thời gian trung bình 10 000 lần Decrypt:**

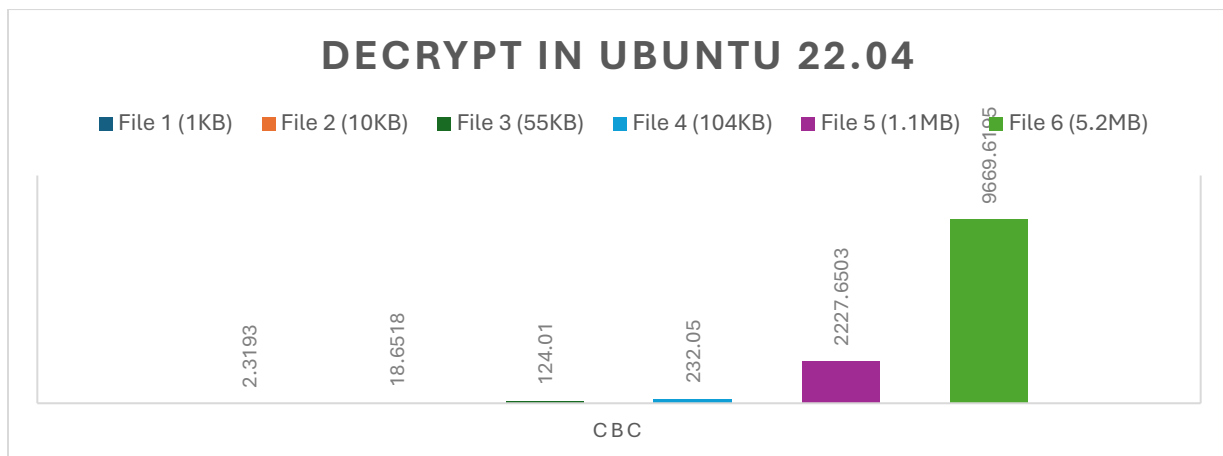


### 2.2.2.1. Hệ điều hành Ubuntu 22.04 (Linux):

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

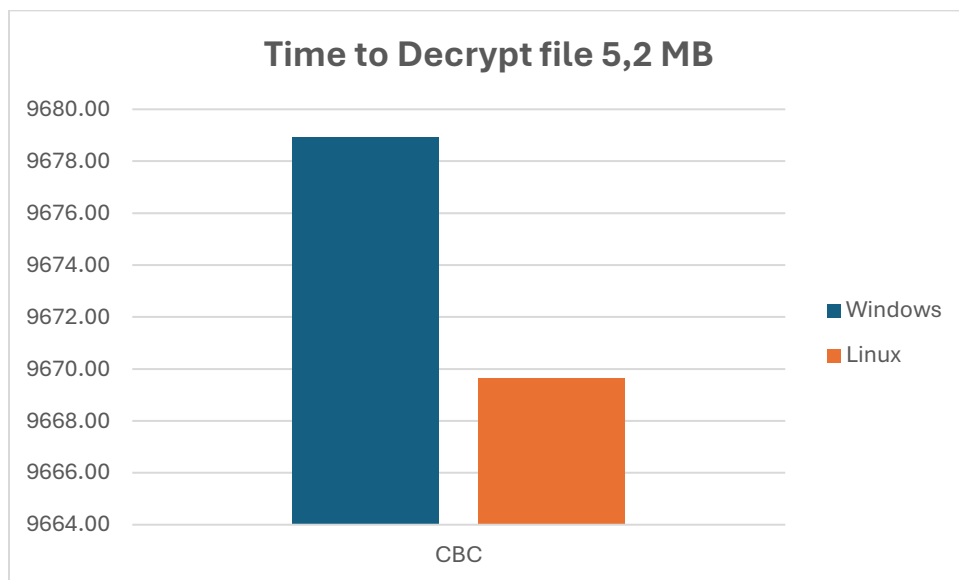
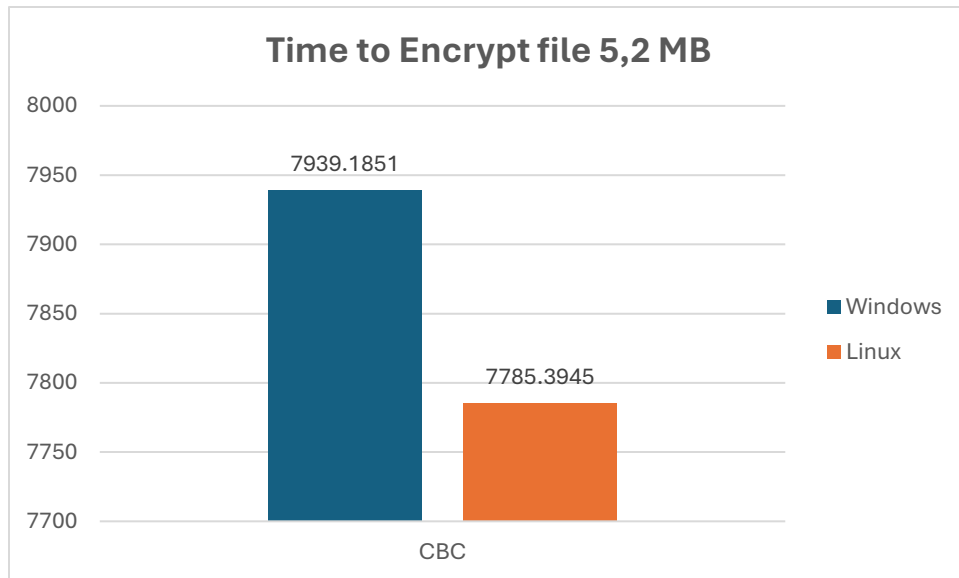


- **Biểu đồ thời gian trung bình 10 000 lần Decrypt:**



### 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.