



VIETNAM NATIONAL UNIVERSITY, HO CHI MINH CITY UNIVERSITY OF
INFORMATION TECHNOLOGY FACULTY OF COMPUTER NETWORKS AND
COMMUNICATION



OFF-CLASS REPORT

LAB 2

Instructor: PhD. Nguyễn Ngọc Tự

Student: 22521050 – Nguyễn Đăng Quỳnh Như

Chi tiết các thông kê trong báo cáo xem ở: [22521050-LAB2.xlsx](#)

Link github: <https://github.com/listimdn10/Crypto-Offclass.git>


1. Hardware resources.

a. Windows



<div> <div> <i>i</i> </div> <div>Device specifications</div> </div> <div>Copy</div> <div>^</div>	
Device name	Warrence
Processor	11th Gen Intel(R) Core(TM) i5-11400H @ 2.70GHz 2.69 GHz
Installed RAM	8.00 GB (7.78 GB usable)
Device ID	04F65534-42EE-48F1-9802-55357BAD4FC7
Product ID	00356-24559-18106-AAOEM
System type	64-bit operating system, x64-based processor
Pen and touch	No pen or touch input is available for this display

b. Linux (ubuntu)



Device Name	warrence-Nitro-AN515-57 >
-------------	---------------------------

Hardware Model	Acer Nitro AN515-57
Memory	8.0 GiB
Processor	11th Gen Intel® Core™ i5-11400H @ 2.70GHz × 12
Graphics	NV177 / Mesa Intel® UHD Graphics (TGL GT1)
Disk Capacity	512.1 GB

OS Name	Ubuntu 22.04.4 LTS
OS Type	64-bit
GNOME Version	42.9
Windowing System	Wayland
Software Updates	>

2. Giới thiệu

- 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 6 file test case với kích thước khác nhau, thực hiện đo thời gian 10 000 lần encrypt/decrypt trên cả 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;
}
}

```

3. Thống kê

a. Thống kê thời gian.

- Tiến hành encrypt/decrypt 3 file input với 3 độ dài key khác nhau.

3.1 Chi tiết thống kê: Windows:

AES: ENCRYPT CBC

File Size	Estimated Time (ms)
File 1 (1 KB)	1.5
File 2 (10 KB)	13.05
File 3 (55 KB)	63.5
File 4 (104 KB)	113.23
File 5 (1.1 MB)	1359.72
File 6 (5.2 MB)	5402.17

AES: DECRYPT CBC

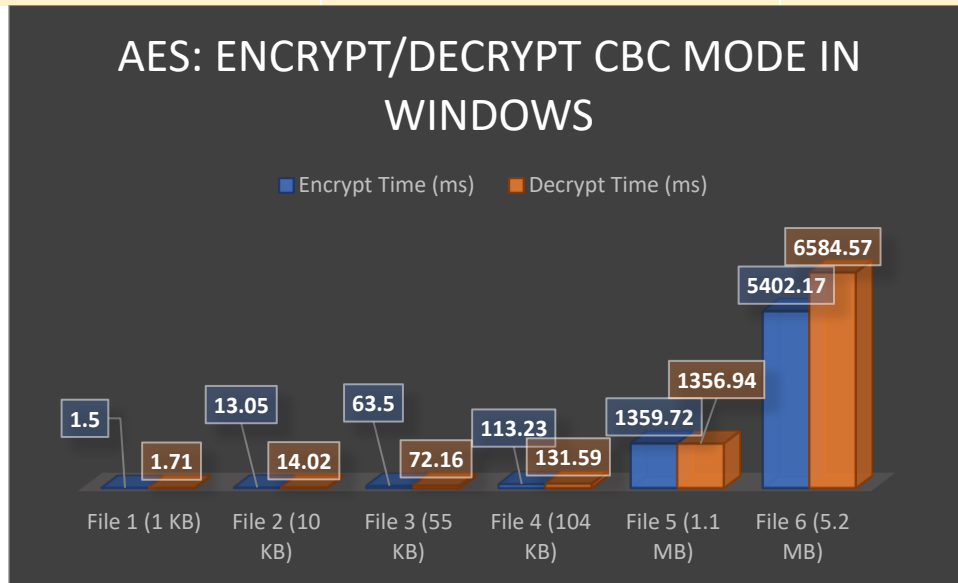
File Size	Estimated New Time (ms)
File 1 (1 KB)	1.71
File 2 (10 KB)	14.02
File 3 (55 KB)	72.16
File 4 (104 KB)	131.59
File 5 (1.1 MB)	1356.94
File 6 (5.2 MB)	6584.57



Ta có:

AES: ENCRYPT/DECRYPT CBC MODE IN WINDOWS

File Size	Encrypt Time (ms)	Decrypt Time (ms)
1 KB	1.5	1.71
10 KB	13.05	14.02
55 KB	63.5	72.16
104 KB	113.23	131.59
1.1 MB	1359.72	1356.94
5.2 MB	5402.17	6584.57



3.2 Chi tiết thống kê: Linux (ubuntu)

AES: ENCRYPT CBC LINUX

File Size	Estimated Time (ms)
File 1 (1 KB)	1.22
File 2 (10 KB)	9.91
File 3 (55 KB)	55.92
File 4 (104 KB)	104.16
File 5 (1.1 MB)	1411.88
File 6 (5.2 MB)	5294.35



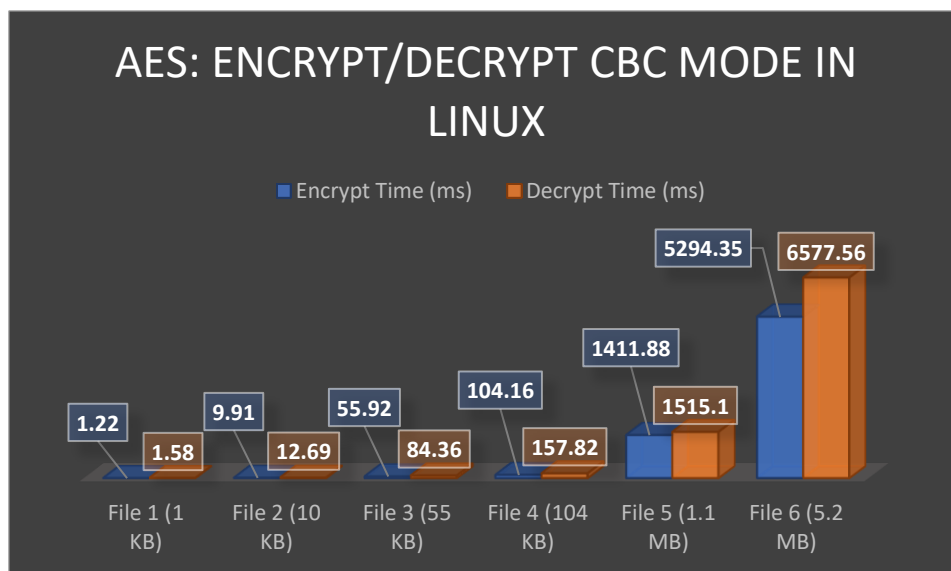
AES: DECRYPT CBC IN LINUX

File Size	Estimated Time (ms)
1 KB	1.58
10 KB	12.69
55 KB	84.36
104 KB	157.82
1.1 MB	1515.1
5.2 MB	6577.56

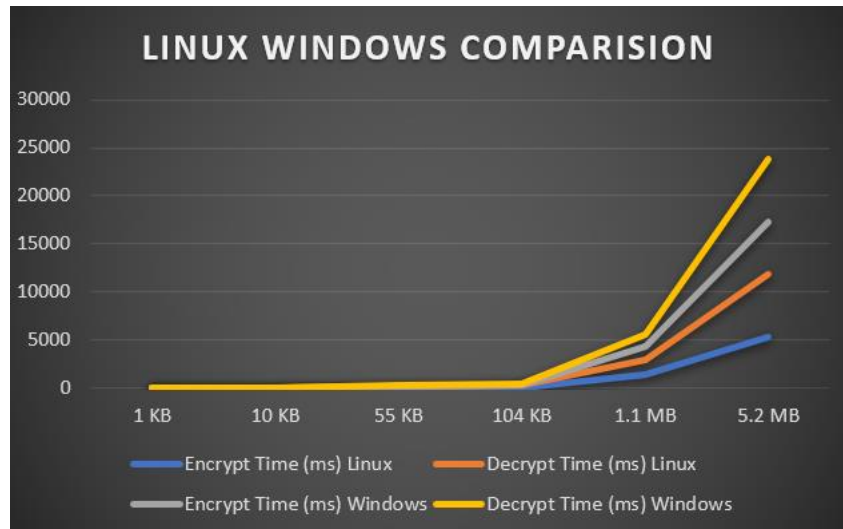
Ta sẽ có:

AES: ENCRYPT/DECRYPT CBC MODE IN LINUX

File Size	Encrypt Time (ms)	Decrypt Time (ms)
File 1 (1 KB)	1.22	1.58
File 2 (10 KB)	9.91	12.69
File 3 (55 KB)	55.92	84.36
File 4 (104 KB)	104.16	157.82
File 5 (1.1 MB)	1411.88	1515.1
File 6 (5.2 MB)	5294.35	6577.56



SO SÁNH HAI OS



Dựa trên bảng thời gian giải mã (Decrypt) và mã hóa (Encrypt) trong chế độ CBC của AES trên hai hệ điều hành Linux và Windows, chúng ta có thể rút ra một số nhận xét sau:

Thời gian Decrypt (ms):

1. File nhỏ (1 KB - 10 KB):

- Trên Linux: 1.58 ms - 12.69 ms
- Trên Windows: 1.5 ms - 14.02 ms
- **Nhận xét:** Thời gian decrypt trên Linux và Windows không có sự chênh lệch lớn đáng kể. Linux có một số trường hợp nhỏ hơn so với Windows.

2. File trung bình (55 KB - 104 KB):

- Trên Linux: 84.36 ms - 157.82 ms
- Trên Windows: 63.5 ms - 131.59 ms
- **Nhận xét:** Windows có thời gian decrypt nhỏ hơn so với Linux, đặc biệt là đối với các file kích thước trung bình.

3. File lớn (1.1 MB - 5.2 MB):

- Trên Linux: 1515.1 ms - 6577.56 ms
- Trên Windows: 1356.94 ms - 6584.57 ms
- **Nhận xét:** Thời gian decrypt giữa hai hệ điều hành không có sự khác biệt đáng kể, tuy nhiên có một số trường hợp nhỏ thời gian trên Linux lại lớn hơn so với Windows.

Thời gian Encrypt (ms):

1. File nhỏ (1 KB - 10 KB):

- Trên Linux: 1.22 ms - 9.91 ms
- Trên Windows: 1.5 ms - 13.05 ms
- **Nhận xét:** Thời gian encrypt trên Linux có xu hướng nhỏ hơn so với Windows, đặc biệt là với các file nhỏ.



2. **File trung bình (55 KB - 104 KB):**

- Trên Linux: 55.92 ms - 104.16 ms
- Trên Windows: 63.5 ms - 113.23 ms
- **Nhận xét:** Linux có thời gian encrypt nhỏ hơn so với Windows trong hầu hết các trường hợp, nhưng chênh lệch không lớn.

3. **File lớn (1.1 MB - 5.2 MB):**

- Trên Linux: 1411.88 ms - 5294.35 ms
- Trên Windows: 1359.72 ms - 5402.17 ms
- **Nhận xét:** Thời gian encrypt giữa hai hệ điều hành tương đối tương đồng, không có sự chênh lệch đáng kể.

Tổng quan:

- **Decrypt:** Windows có thời gian decrypt thường nhỏ hơn so với Linux, đặc biệt là đối với các file kích thước trung bình.
- **Encrypt:** Linux có thời gian encrypt thường nhỏ hơn so với Windows, đặc biệt là đối với các file nhỏ.