BÁO CÁO TASK 2

**Môn học: Mật mã học**

*GVHD: Nguyễn Ngọc Tự*

**THÔNG TIN CHUNG:**

Lớp: NT219.O21.ANTT

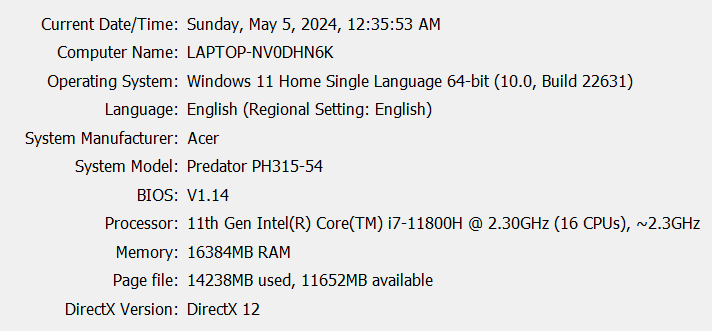
|  |  |  |
| --- | --- | --- |
| **Họ và tên** | **MSSV** | **Email** |
| Phan Quốc Đạt | 22520233 | 22520233@gm.uit.edu.vn |

BÁO CÁO CHI TIẾT

1. **Khái quát**

Mã hóa và giải mã AES mode CBC, đây là 1 trong các thuật toán mã khóa khối. Mã hóa AES sử dụng khóa đối xứng. Bài task này không được sử dụng thư viện hỗ trợ nào để mã hóa và giải mã dữ liệu, sau đó sử dụng kết quả để so sánh với khi dùng thư viện hỗ trợ và giữa 2 hệ điều hành là ubuntu và windows.

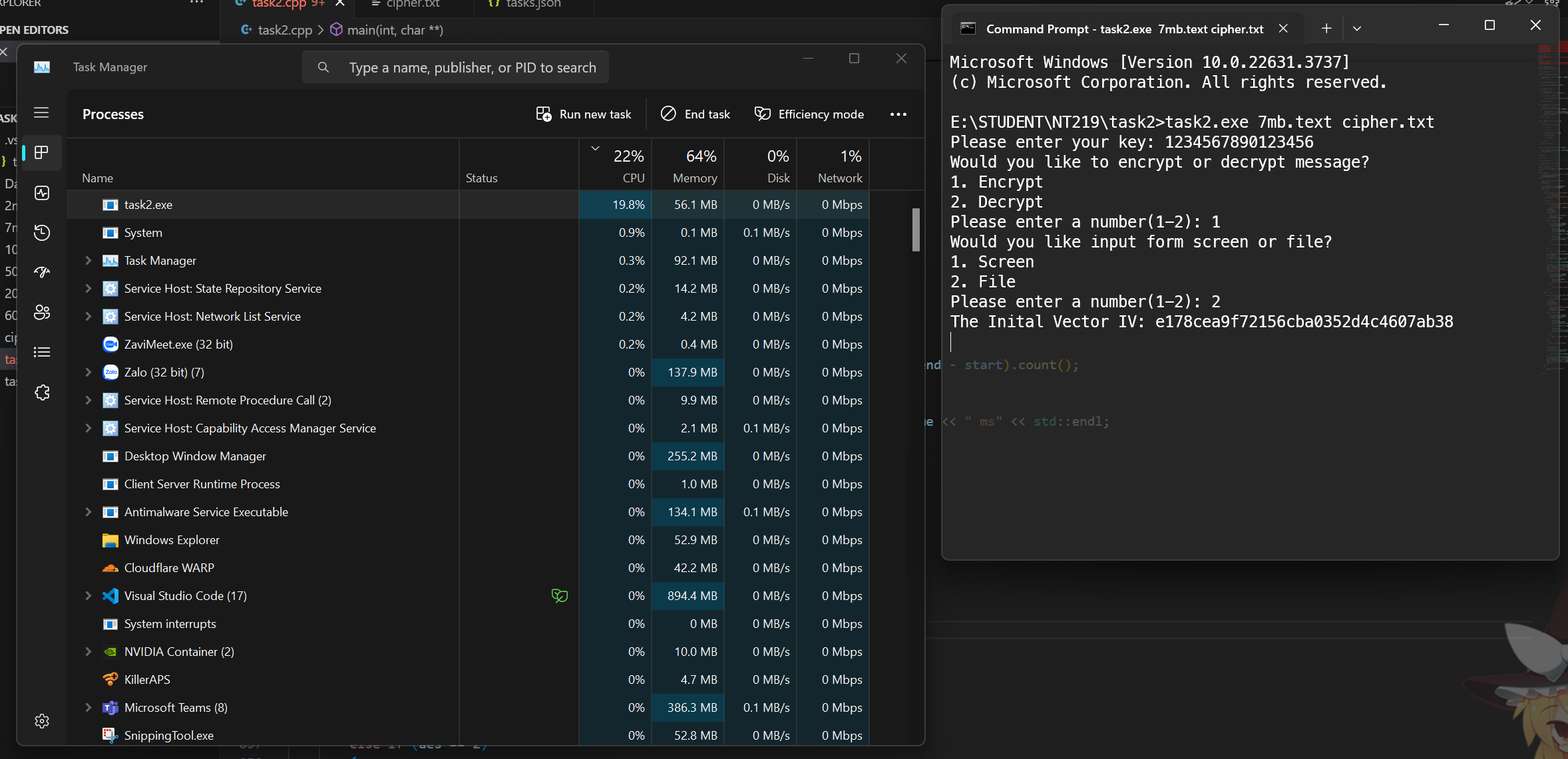
1. **Tài nguyên phần cứng**





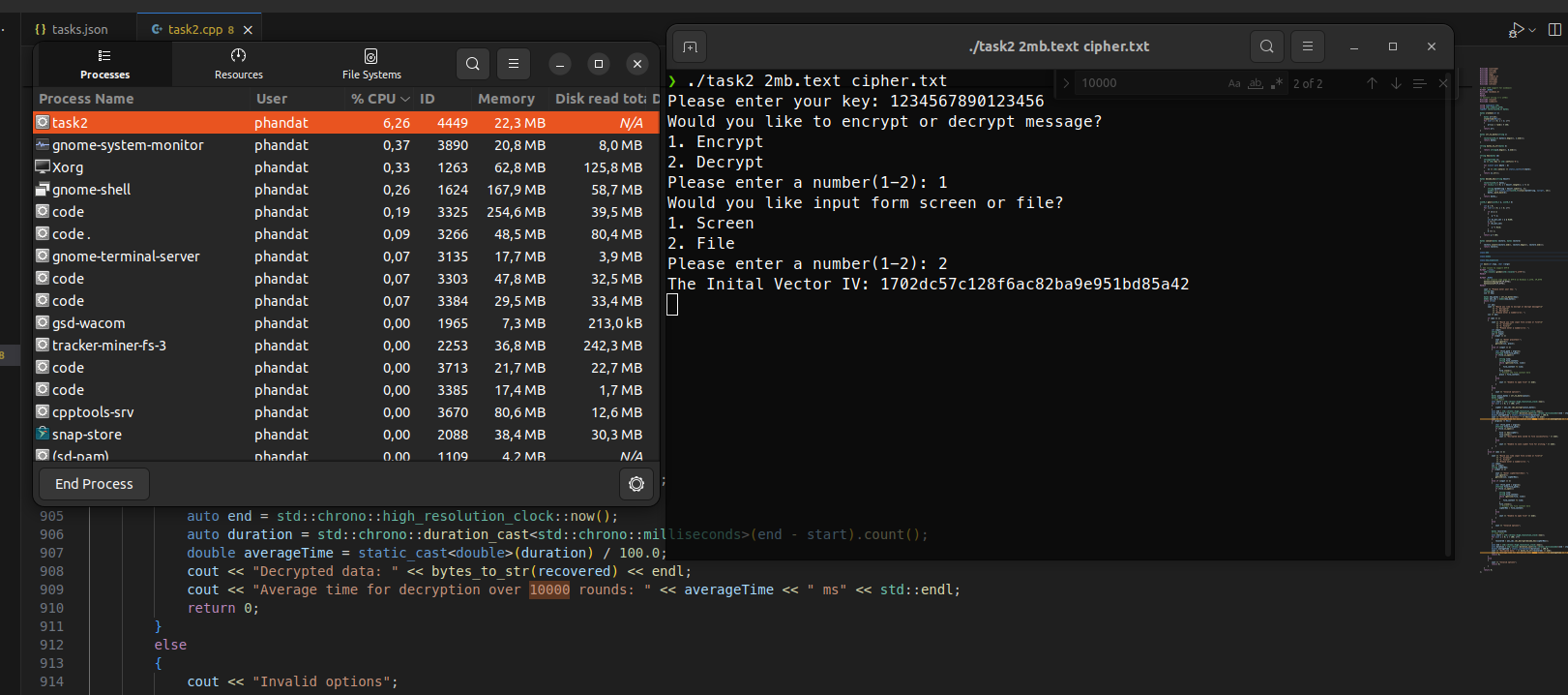
1. **Hiệu xuất**

**Windows:**



Hiệu xuất xử lý trung bình 20% CPU cho việc mã hóa tập tin

(Thông số này được em lấy từ lúc chương trình encrypt, trong đó đoạn code dã được em đã chỉnh sửa code để tạo 1 vòng lặp mã hóa 10000 sau đó tính thời gian vào ghi lại)

**Ubuntu**:

Hiệu xuất xử lý trung bình 6% CPU cho việc mã hóa tập tin

(Thông số này được em lấy từ lúc chương trình encrypt, trong đó đoạn code dã được em đã chỉnh sửa code để tạo 1 vòng lặp mã hóa 10000 sau đó tính thời gian vào ghi lại)

1. **Thống kê kết quả**

Dưới đây là kết quả thống kế được từ Windows 11, kết quả thu lại được từ việc sử dụng mode CBC và kích thước dữ liệu khác nhau với key 128 bits. Số liệu ở dưới là thời gian mã hóa và giải mã được tính theo ms (mili giây). Kết quả ở đây được tính toán từ thời gian bắt đầu mã hóa/giải mã 10000 lần cho đến khi kết thúc.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **CBC Mode** | | | | | | | |
| **File Size** | | **10KB** | **50KB** | **100KB** | **200KB** | **600KB** | **2MB** |
| **Windows** | **Encrypt** | **16.5203** | **82.2** | **186.7** | **399.8** | **4621.2** | **76589.8** |
| **Decrypt** | **18.2174** | **87.4** | **196.0** | **409.7** | **4625.5** | **75314.3** |
| **Unbuntu** | **Encrypt** | **3.5521** | **19.86** | **46.95** | **125.4** | **684.35** | **11903.0** |
| **Decrypt** | **4.468** | **24.47** | **52.87** | **135.7** | **741.21** | **12810.9** |

1. **Nhận xét**

- Theo số liệu đã được thu thập ở trên có thể thấy được với kích thước dữ liệu tăng lên bao nhiêu lần thì thời gian mã hóa và giải mã cũng tăng lên bấy nhiêu lần.

- Có thể vì mode AES CBC này không sử dụng thư viện đã được tối lưu nên quá trình giải mã và mã hóa rất tốn thời gian

- Với 2 hệ điều hành Windows và Ubuntu thì có thể thấy được hệ điều hành Ubuntu thực hiện công việc mã hóa và giải mã đều nhanh hơn Windows. Thời gian thực hiện công việc này có thể thay đổi bởi các phiên bản khác nhau và tài nguyên xử lý tại thời điểm khác nhau. Sự chênh lệnh thời gian có thể vì windows cần chạy nhiều tác vụ hơn ubuntu, nên windows chưa được tối lưu cho việc này.