BÁO CÁO TASK 1

**Môn học: Mật mã học**

*GVHD: Nguyễn Ngọc Tự*

**THÔNG TIN CHUNG:**

Lớp: NT219.O21.ANTT

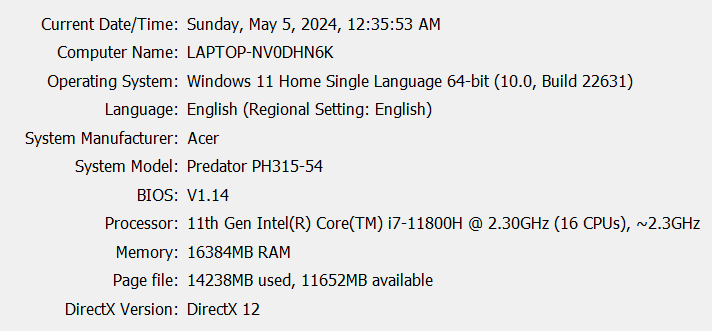
|  |  |  |
| --- | --- | --- |
| **Họ và tên** | **MSSV** | **Email** |
| Phan Quốc Đạt | 22520233 | 22520233@gm.uit.edu.vn |

BÁO CÁO CHI TIẾT

1. **Khái quát**

Mã hóa và giải mã AES, đây là 1 trong các thuật toán mã khóa khối. Mã hóa AES sử dụng khóa đối xứng. Bài task này sử dụng thư viện CryptoPP để mã hóa và giải mã dữ liệu và được thực hiện trên nhiều mode khác nhau, sau đó sử dụng kết quả để so sánh giữa các mode và giữa 2 hệ điều hành là ubuntu và windows.

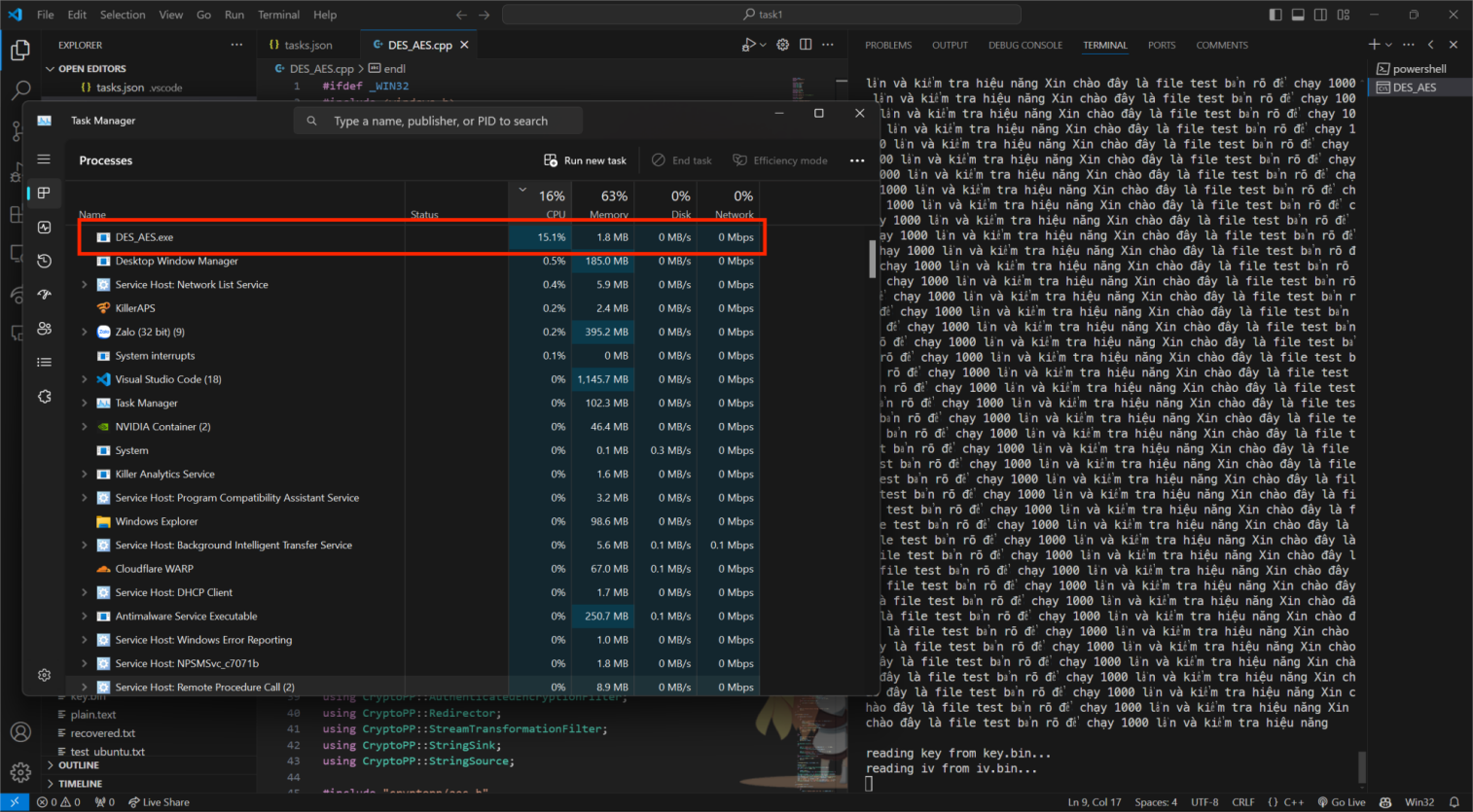
1. **Tài nguyên phần cứng**





1. **Hiệu xuất**

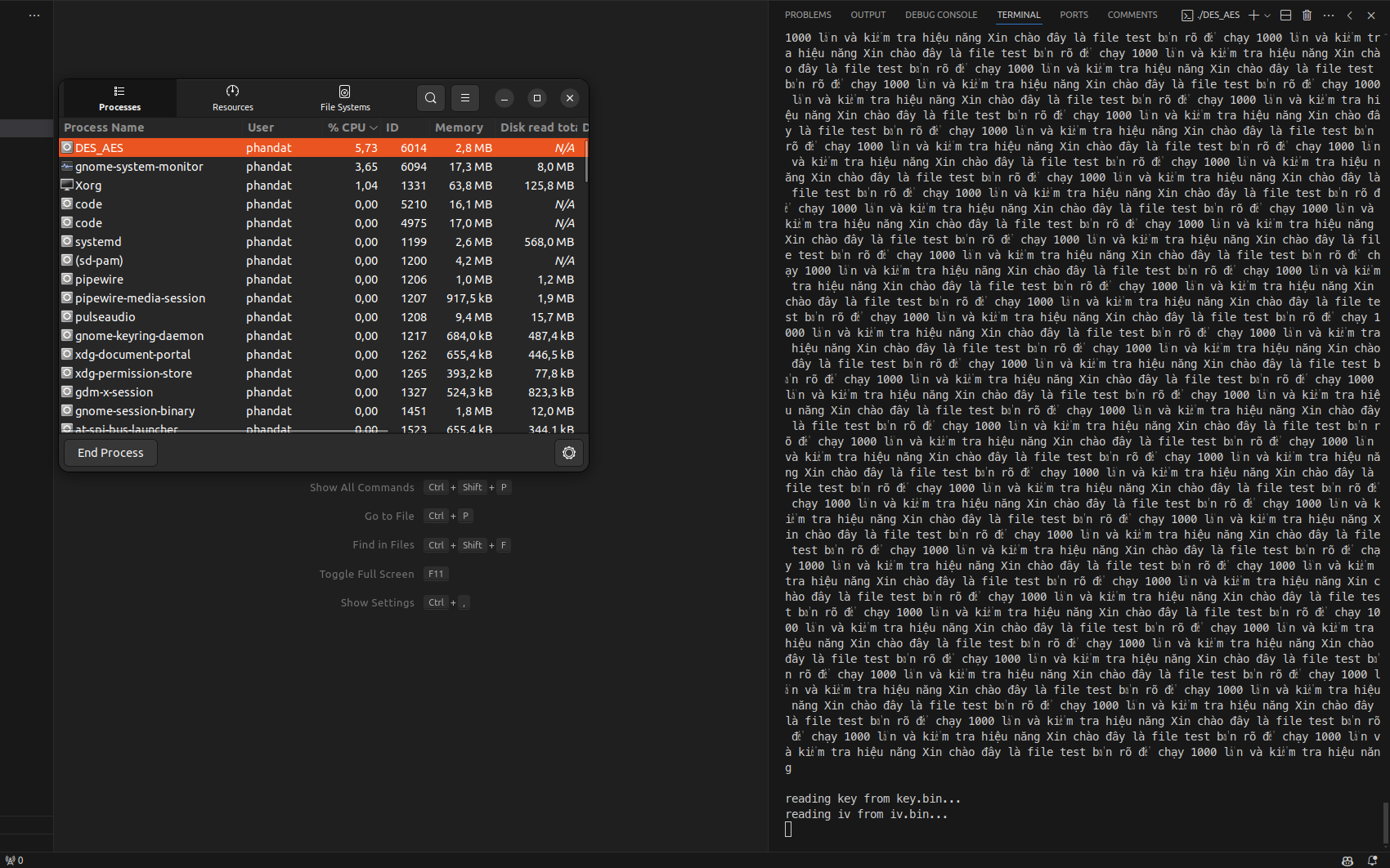
**Windows:**



Hiệu xuất xử lý trung bình 15% 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 các mode khác nhau và kích thước dữ liệu khác nhau. 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.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Windows 11 AES** | | | | | | | |
| **AES Modes** | | **10KB** | **50KB** | **200KB** | **600KB** | **2MB** | **7MB** |
| **ECB** | **Encrypt** | **0.054** | **0.258** | **1.025** | **3.096** | **10.754** | **37.082** |
| **Decrypt** | **0.056** | **0.264** | **1.055** | **3.171** | **10.906** | **37.104** |
| **CBC** | **Encrypt** | **0.057** | **0.272** | **1.085** | **3.288** | **11.151** | **41.262** |
| **Decrypt** | **0.056** | **0.264** | **1.059** | **3.231** | **10.709** | **39.971** |
| **OFB** | **Encrypt** | **0.055** | **0.264** | **1.052** | **3.417** | **10.949** | **40.085** |
| **Decrypt** | **0.055** | **0.262** | **1.056** | **3.162** | **10.512** | **37.397** |
| **CFB** | **Encrypt** | **0.056** | **0.264** | **1.043** | **3.130** | **10.701** | **36.213** |
| **Decrypt** | **0.055** | **0.260** | **1.033** | **3.144** | **10.296** | **37.211** |
| **CTR** | **Encrypt** | **0.055** | **0.267** | **1.046** | **3.189** | **10.513** | **37.202** |
| **Decrypt** | **0.055** | **0.264** | **1.047** | **3.155** | **10.896** | **36.992** |
| **XTS** | **Encrypt** | **0.049** | **0.238** | **0.948** | **2.869** | **9.647** | **34.555** |
| **Decrypt** | **0.051** | **0.244** | **0.957** | **2.899** | **9.655** | **34.578** |
| **CCM** | **Encrypt** | **0.110** | **0.531** | **2.153** | **6.406** | **22.284** | **75.314** |
| **Decrypt** | **0.111** | **0.534** | **2.132** | **6.382** | **21.349** | **78.025** |
| **GCM** | **Encrypt** | **0.072** | **0.341** | **1.379** | **4.084** | **14.557** | **48.235** |
| **Decrypt** | **0.074** | **0.347** | **1.383** | **4.112** | **13.733** | **48.587** |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Windows 11 DES** | | | | | | | |
| **DES Modes** | | **10KB** | **50KB** | **200KB** | **600KB** | **2MB** | **7MB** |
| **ECB** | **Encrypt** | **0.116** | **0.572** | **2.273** | **6.874** | **23.251** | **80.240** |
| **Decrypt** | **0.117** | **0.567** | **2.281** | **6.847** | **23.159** | **81.691** |
| **CBC** | **Encrypt** | **0.131** | **0.637** | **2.537** | **7.668** | **25.621** | **90.480** |
| **Decrypt** | **0.121** | **0.568** | **2.391** | **6.845** | **23.412** | **82.001** |
| **OFB** | **Encrypt** | **0.128** | **0.622** | **2.488** | **7.550** | **25.296** | **89.541** |
| **Decrypt** | **0.127** | **0.620** | **2.477** | **7.444** | **25.004** | **89.909** |
| **CFB** | **Encrypt** | **0.130** | **0.625** | **2.505** | **7.596** | **25.126** | **89.812** |
| **Decrypt** | **0.120** | **0.572** | **2.277** | **6.910** | **23.227** | **82.013** |
| **CTR** | **Encrypt** | **0.134** | **0.655** | **2.612** | **7.872** | **27.147** | **93.519** |
| **Decrypt** | **0.133** | **0.654** | **2.640** | **7.851** | **27.187** | **92.393** |

Dưới đây là kết quả thống kế được từ Ubuntu, kết quả thu lại được từ việc sử dụng các mode khác nhau và kích thước dữ liệu tương tự Windows. 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.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Ubuntu** | | | | | | | |
| **Modes** | | **10KB** | **50KB** | **200KB** | **600KB** | **2MB** | **7MB** |
| **ECB** | **Encrypt** | **0.002** | **0.008** | **0.032** | **0.093** | **0.313** | **1.089** |
| **Decrypt** | **0.002** | **0.009** | **0.035** | **0.097** | **0.325** | **1.125** |
| **CBC** | **Encrypt** | **0.007** | **0.037** | **0.144** | **0.434** | **1.445** | **5.064** |
| **Decrypt** | **0.002** | **0.010** | **0.037** | **0.110** | **0.367** | **1.262** |
| **OFB** | **Encrypt** | **0.008** | **0.038** | **0.149** | **0.445** | **1.497** | **5.247** |
| **Decrypt** | **0.008** | **0.037** | **0.148** | **0.443** | **1.482** | **5.229** |
| **CFB** | **Encrypt** | **0.008** | **0.038** | **0.149** | **0.454** | **1.533** | **5.406** |
| **Decrypt** | **0.003** | **0.014** | **0.058** | **0.178** | **0.658** | **2.302** |
| **CTR** | **Encrypt** | **0.002** | **0.010** | **0.036** | **0.108** | **0.373** | **1.475** |
| **Decrypt** | **0.002** | **0.008** | **0.039** | **0.106** | **0.354** | **1.252** |
| **XTS** | **Encrypt** | **0.005** | **0.026** | **0.114** | **0.356** | **1.317** | **4.456** |
| **Decrypt** | **0.005** | **0.024** | **0.112** | **0.348** | **1.232** | **4.429** |
| **CCM** | **Encrypt** | **0.009** | **0.044** | **0.174** | **0.519** | **1.732** | **6.088** |
| **Decrypt** | **0.001** | **0.045** | **0.173** | **0.524** | **1.752** | **6.143** |
| **GCM** | **Encrypt** | **0.003** | **0.013** | **0.050** | **0.162** | **0.529** | **1.809** |
| **Decrypt** | **0.003** | **0.014** | **0.050** | **0.156** | **0.513** | **1.805** |

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.

- 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.

- Giữa 2 thuật toán mã hóa AES và DES thì có thể thấy AES nhanh hơn hẳn DES mặc dù DES có khóa nhỏ hơn AES. Có thể vì DES đã quá cũ không còn được tối ưu cho phầm cứng và phầm mềm, còn AES thì mới hơn nên được tối ưu cho phần cứng và phầm mềm và độ bao mật cũng cao hơn.

- Trong các mode thì trong đó có thể thấy được ECB là mode có thời gian thực thi công việc nhanh nhất vì thuật toán của ECB có cơ chế đơn giản nhất, ECB làm việc trên từng Block độc lập với các khối khác. Do đó nó có thể thực hiện song song với các khối khác mà không cần đợi dữ liệu từ khối trước đó, tuy nhiên nó dễ gặp vấn đề bảo mật hơn các khối khác.

- Ngược lại trong các mode thì thấy được CCM là chế độ cần nhiều thời gian để thực hiện công việc nhất. CCM tốn nhiều thời gian vì CCM kết hợp cả việc mã hóa và xác thực trong cùng một quá trình, nó sử dụng phương pháp kết hợp bộ đếm và CBC-MAC. Tuy việc thực hiện công việc có vẻ tốn thời gian nhưng nó có độ an toàn cao hơn những mode khác