BÁO CÁO TASK 3

**Môn học: Mật mã học**

*GVHD: Nguyễn Ngọc Tự*

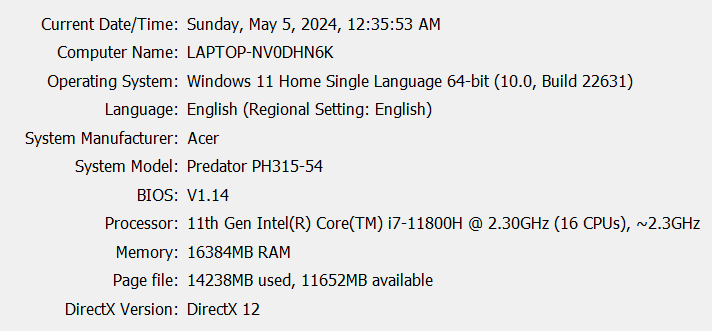
**THÔNG TIN CHUNG:**

Lớp: NT219.O21.ANTT

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

BÁO CÁO CHI TIẾT

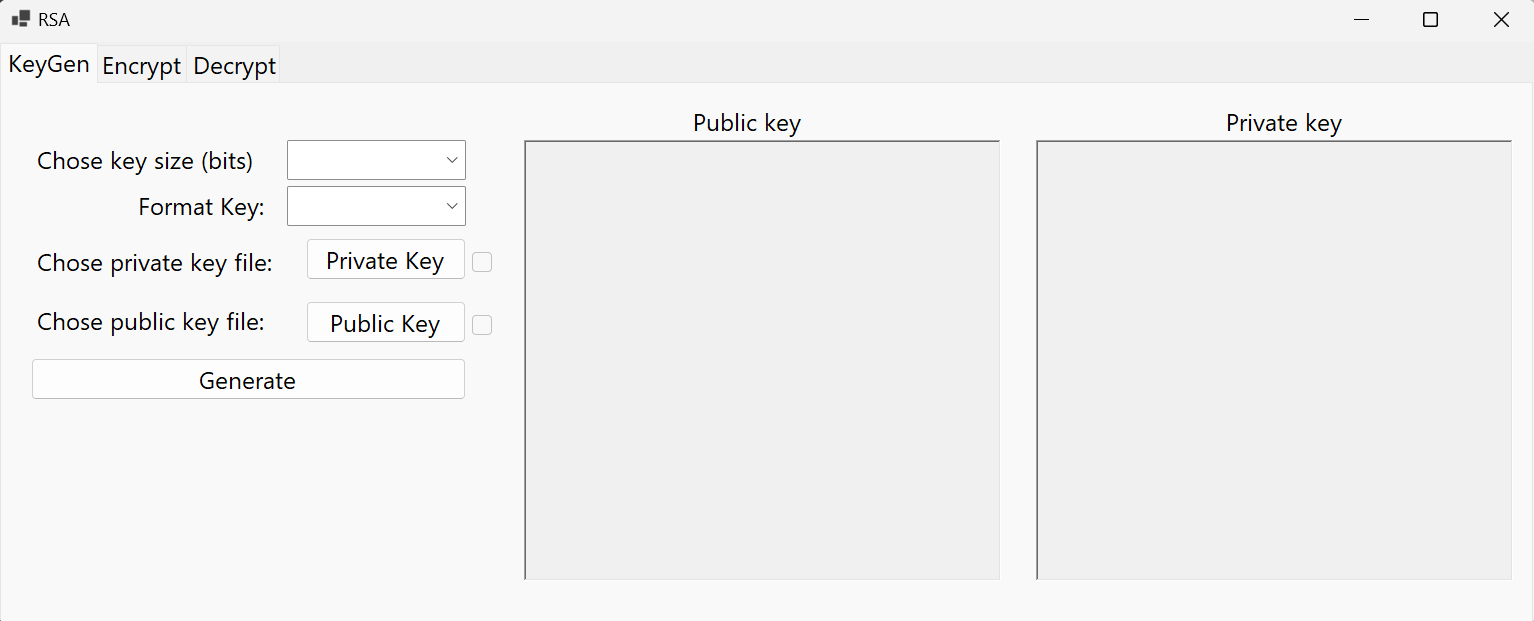
1. **Tài nguyên phần cứng**

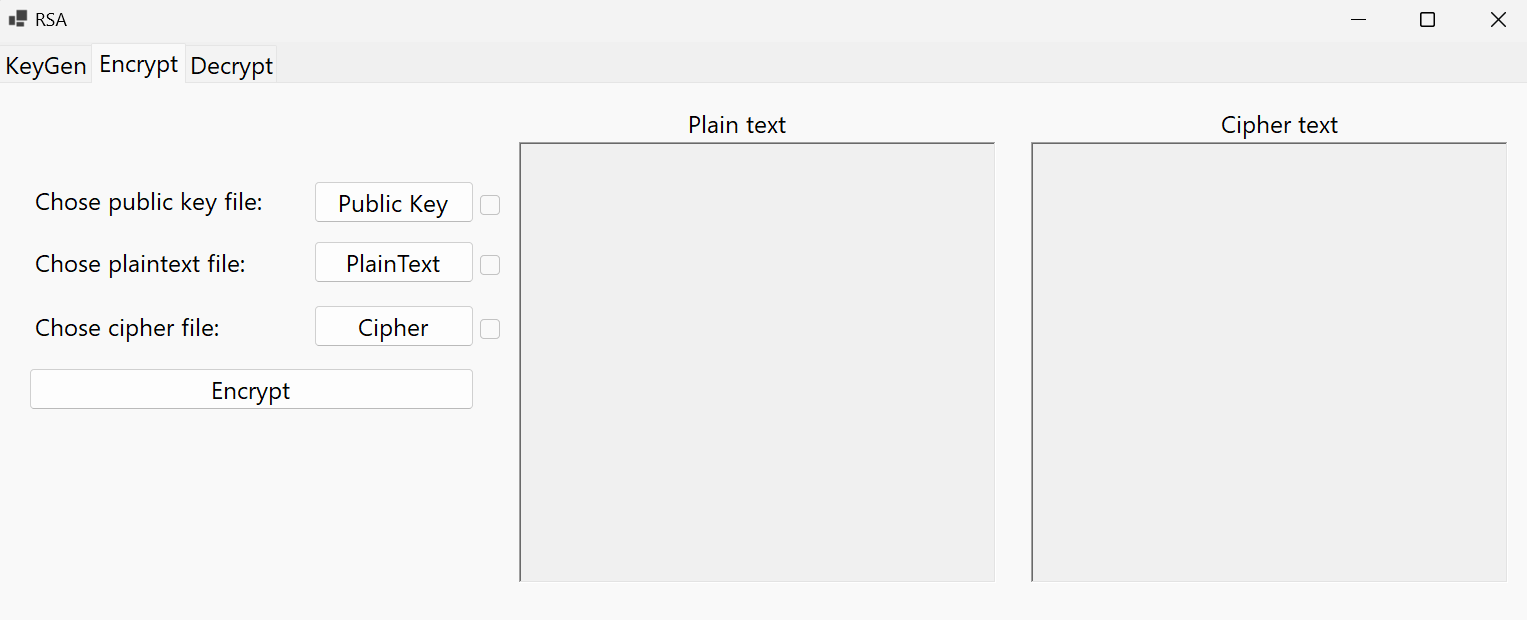


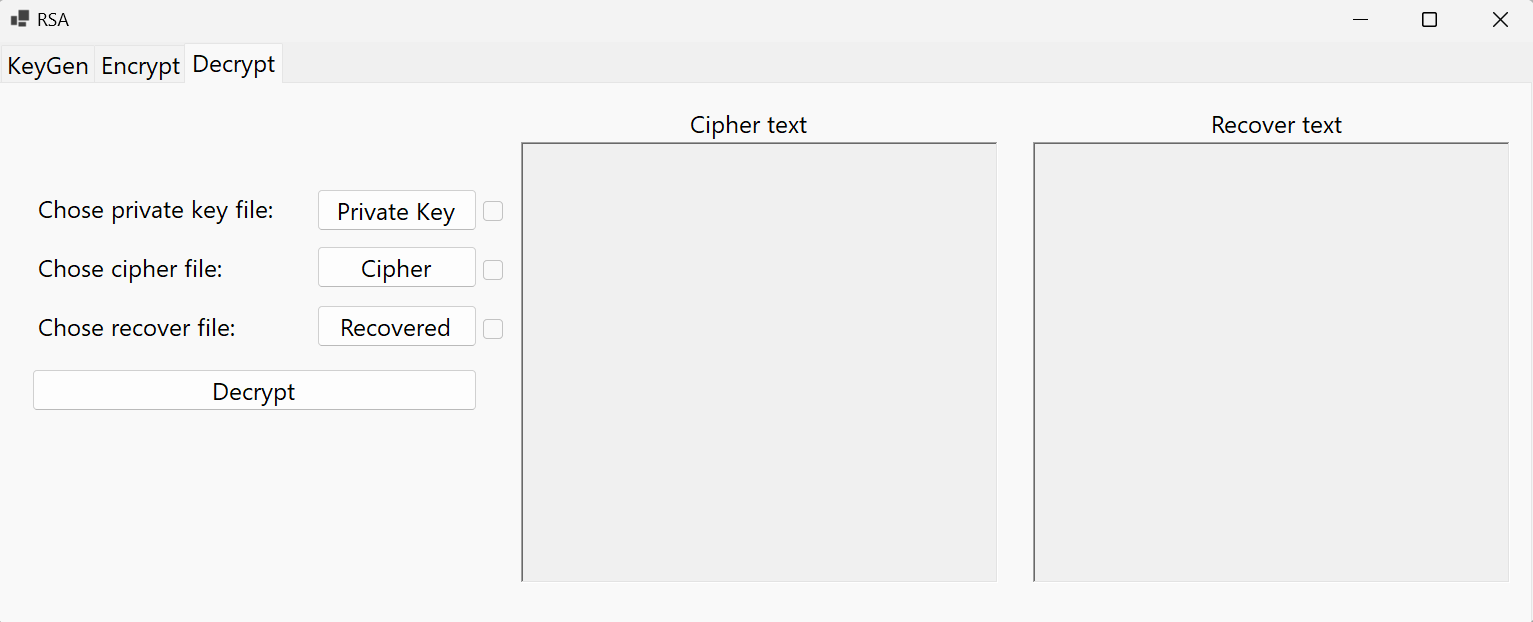


1. **Làm GUI cho chương trình**

Tạo giao diện bằng C# để tạo key, mã hóa và giải mã

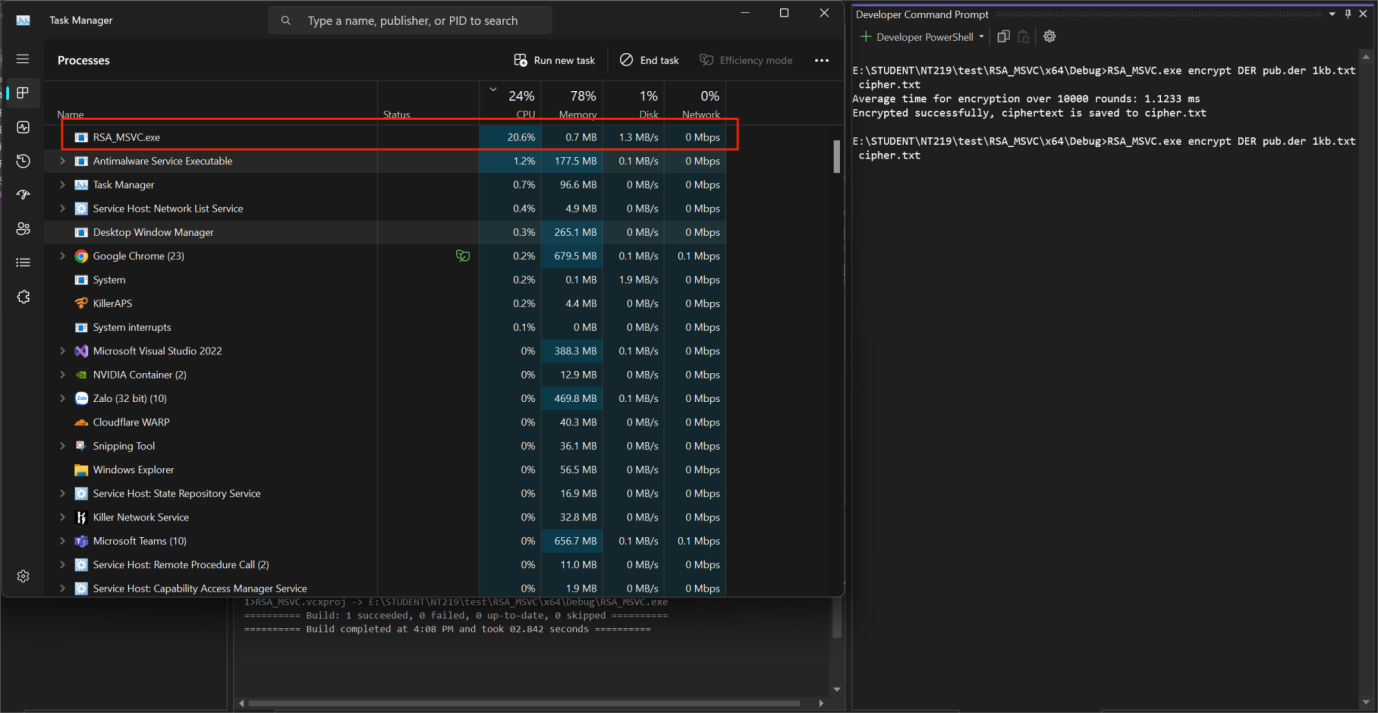






1. **Hiệu xuất**

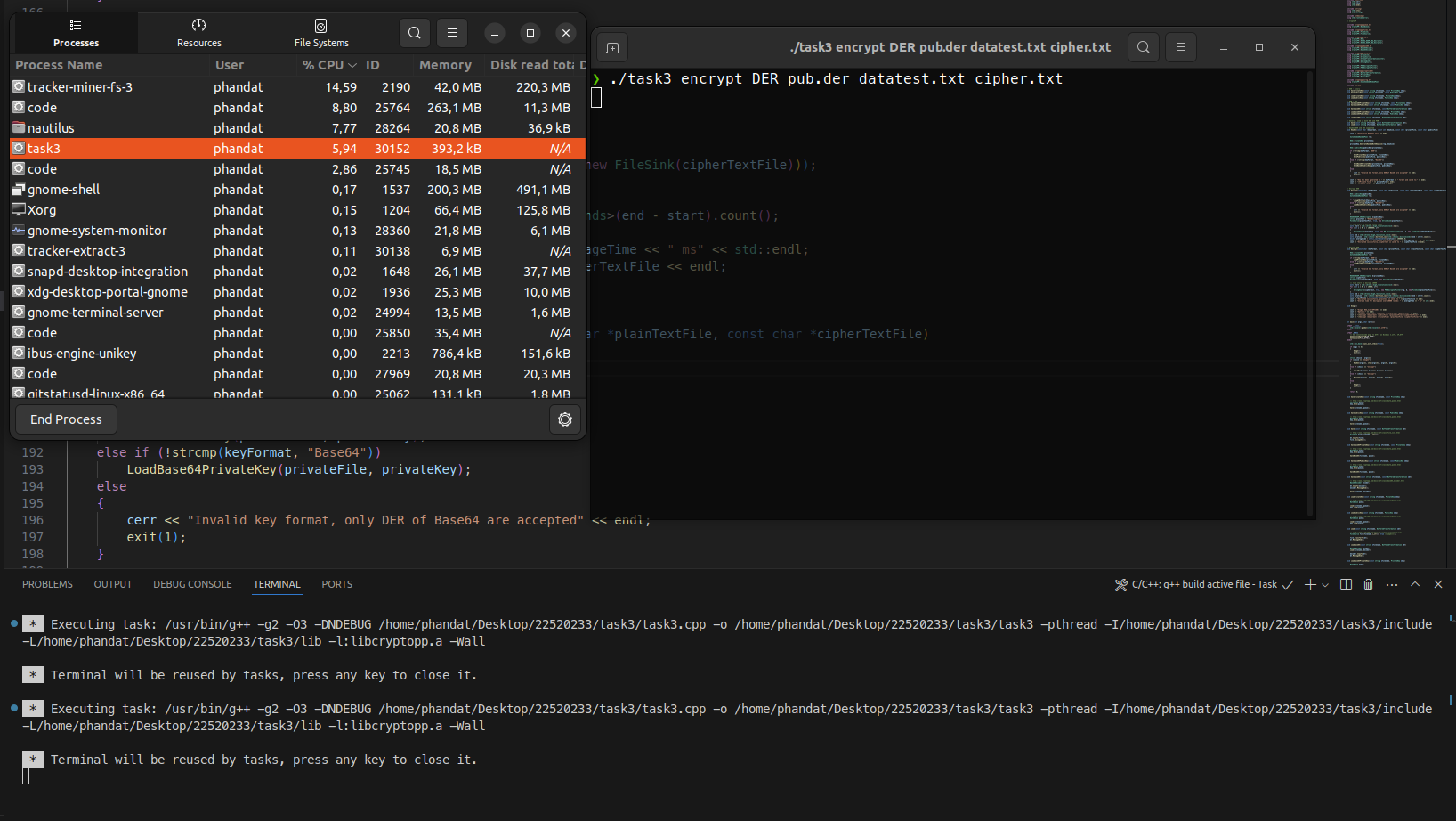
**Windows**:



Hiệu xuất sử dụng khoảng 20% CPU khi mã hóa 10000 lần

(Để xem hiệu xuất em đã chỉnh sửa lại code để thực hiện lặp lại 10000 lần và tính thời gian, em sử dụng cmd để lấy thông tin, còn giao diện cho người dùng thì không cần hiển thị thời gian)

**Ubuntu**:



Hiệu xuất sử dụng khoảng 6% CPU khi mã hóa 10000 lần

(Để xem hiệu xuất em đã chỉnh sửa lại code để thực hiện lặp lại 10000 lần và tính thời gian, em sử dụng cmd để lấy thông tin, còn giao diện cho người dùng thì không cần hiển thị thời gian)

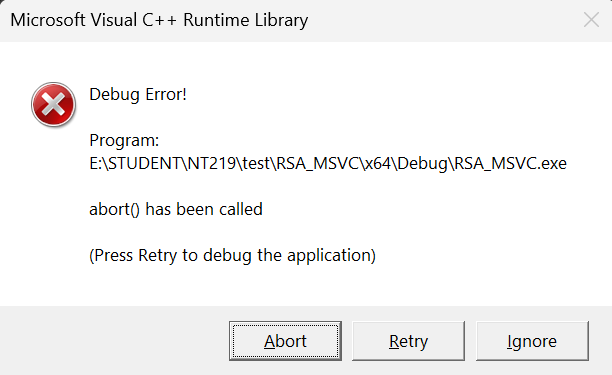
1. **Thống kê kết quả**

Dưới đây là kết quả thống kế được từ Windows 11 và Ubuntu. Kết quả được thực hiện dựa trên cùng dữ liệu đầu vào và khóa 3072 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.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test** | | **File 8 bytes** | **File 150 bytes** | **File 300 bytes** |
| **Windows** | **Encrypt** | **1.077 ms** | **1.066 ms** | **1.113 ms** |
| **Decrypt** | **87.063 ms** | **88.779 ms** | **86.944 ms** |
| **Ubuntu** | **Encrypt** | **0.082 ms** | **0.081 ms** | **0.081 ms** |
| **Decrypt** | **3.794 ms** | **3.777 ms** | **3.838 ms** |

**Lưy ý:**

Khi thực hiện mã hóa file có kích lớn sẽ báo lỗi **abort() has been called**. Lỗi này sảy ra khi input vào lớn hơn modul n = p . q, Input sẽ phụ thuộc theo key key phải lớn thì mới có thể mã hóa được input lớn. Ở đây do em dùng key 3072 bits nên chỉ có thể mã hóa khoảng 300 ký tự.



1. **Nhận xét**

- Theo số liệu đã được thu thập ở trên có thể thấy được với kích thước dữ liệu khác nhau nhưng thời gian cũng tương đương nhau. Là vì RSA dựa trên các phép toán số học với các số nguyên tố lớn, không phụ thuộc vào kích thước của dữ liệu đầu vào

- 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.

- Có thể thấy là mã hóa RSA rất lâu hơn so với các mode của AES. Bởi vì RSA sử dụng 2 khóa bất đối xứng còn AES sử dụng khóa đối xứng, độ dài của khóa RSA thường lớn hơn 2048 bit còn khóa của AEES thường 128 tới 256 bit. Nhưng RSA lại có độ an toàn cao hơn AES