BÁO CÁO TASK 5

**Môn học: Mật mã học**

*GVHD: Nguyễn Ngọc Tự*

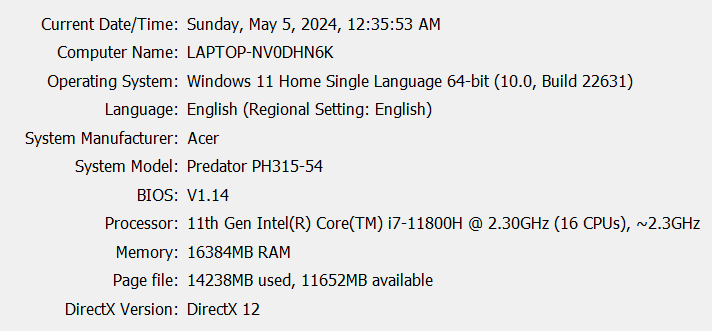
**THÔNG TIN CHUNG:**

Lớp: NT219.O21.ANTT

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

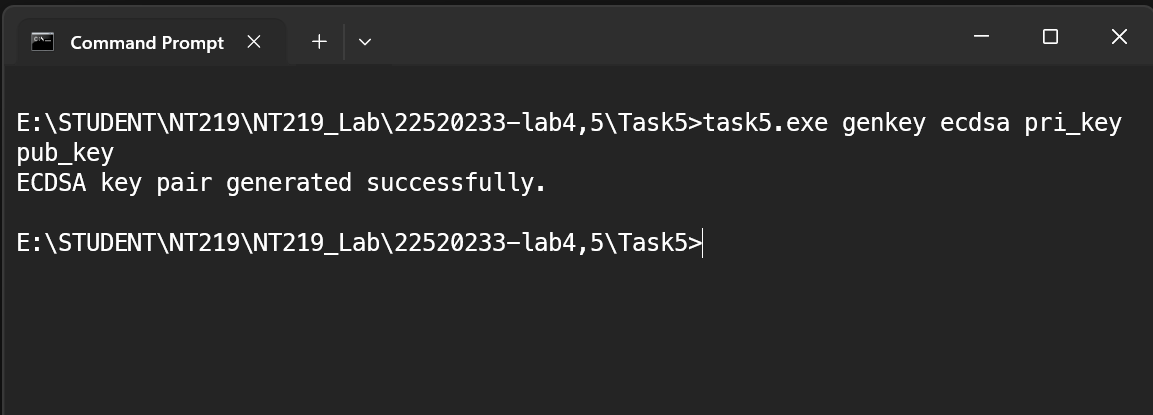
BÁO CÁO CHI TIẾT

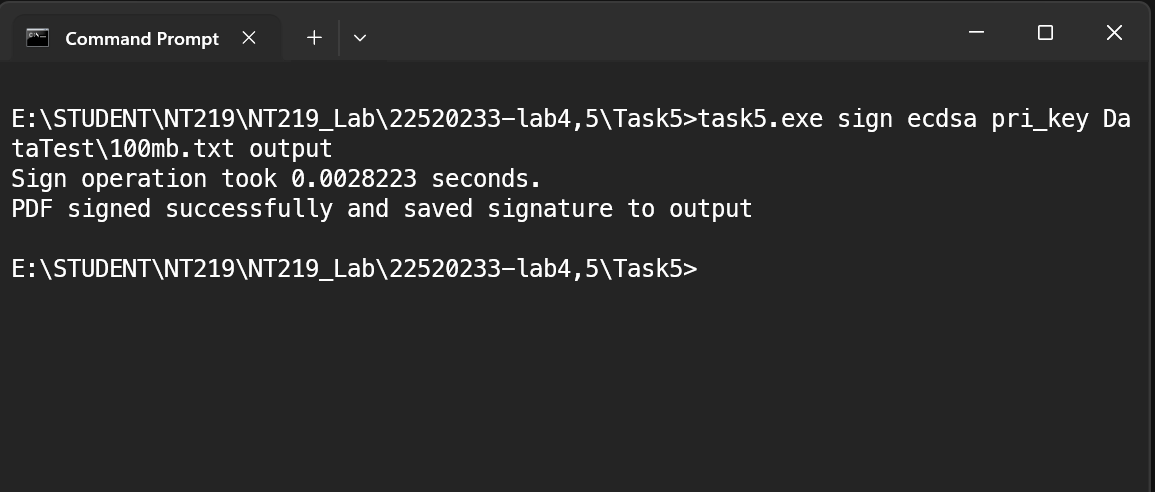
1. **Tài nguyên phần cứng**

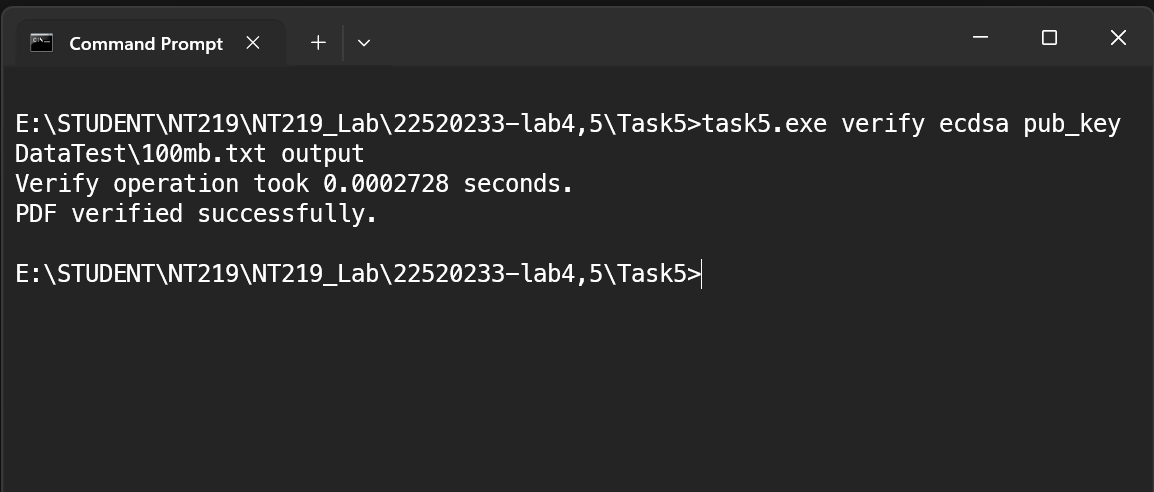




1. **Demo**







1. **Thống kê kết quả**

Dưới đây là kết quả thống kế được từ Windows 11 và Ubuntu, 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 sign/verify được tính theo ms (mili giây). Kết quả ở đây được tính toán từ thời gian bắt đầu sign/verify 1000 lần cho đến khi kết thúc.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Windows 11** | | | | | |
| **Size** | | **2mb** | **10mb** | **50mb** | **100mb** |
| **ECDSA** | **Sign** | **2.039** | **2.213** | **2.289** | **2.442** |
| **Verify** | **0.215** | **0.254** | **0.266** | **0.269** |
| **RSAPSS** | **Sign** | **2.772** | **2.807** | **2.934** | **2.923** |
| **Verify** | **0.153** | **0.158** | **0.183** | **0.176** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ubuntu** | | | | | |
| **Size** | | **2mb** | **10mb** | **50mb** | **100mb** |
| **ECDSA** | **Sign** | **0.420** | **0.407** | **0.425** | **0.449** |
| **Verify** | **0.100** | **0.105** | **0.111** | **0.106** |
| **RSAPSS** | **Sign** | **0.861** | **0.891** | **0.872** | **0.885** |
| **Verify** | **0.234** | **0.251** | **0.246** | **0.248** |

1. **Nhận xét**

- Xét về thời gian thì thuật toán ECDSA nhanh hơn thuật toán RSAPSS. Với file số liệu lớn dần thì thời gian chênh nhau không đáng kể.

- Hệ điều hành Ubuntu nhanh hơn hệ điều hành windows ở mọi điểm