**Report Lab 3**

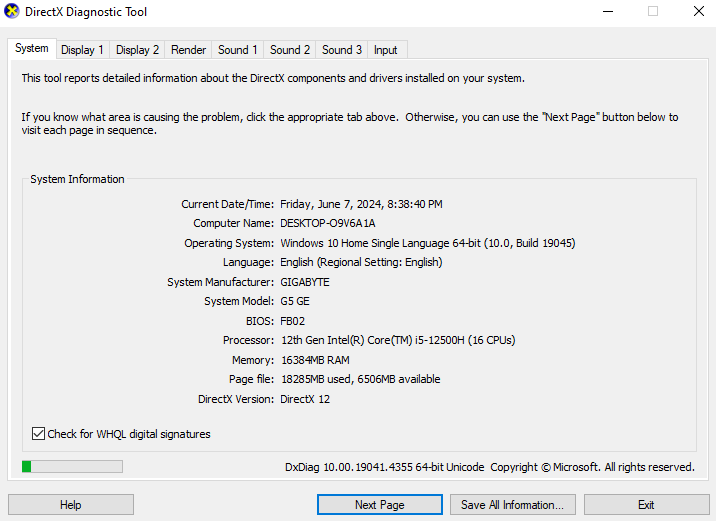
**Student Information**

Full Name: Mai Nguyễn Nam Phương

Student ID Number: 22521164

Class: NT219.O21.ANTT.2

**Device Information**



**RSA-OAEP**

**TEST CASE**

number of iterations: 10000

time counter: mili seconds

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Encrypt (Window)** | | | | **Decrypt (Window)** | | | |
| **Key Size** | **8912** | **10240** | **12288** | **Key size** | **8912** | **10240** | **12288** |
| File 1 (0.4KB) | 0.9587 |  |  | File 1 (0.4KB) | 50.6506 |  |  |
| File 2 (1KB) |  | 0.9965 |  | File 2 (1KB) |  | 56.2361 |  |
| File 3 (1.4KB) |  |  | 1.1201 | File 3 (1.4KB) |  |  | 70.2124 |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Encrypt (Ubuntu)** | | | | **Decrypt (Ubuntu)** | | | |
| **Key Size** | **8912** | **10240** | **12288** | **Key size** | **8912** | **10240** | **12288** |
| File 1 (0.4KB) | 0.7951 |  |  | File 1 (0.4KB) | 47.2643 |  |  |
| File 2 (1KB) |  | 0.7724 |  | File 2 (1KB) |  | 54.6484 |  |
| File 3 (1.4KB) |  |  | 0.8512 | File 3 (1.4KB) |  |  | 68.2124 |

**Comments and Comparison:**

**- Số liệu cho ta thấy việc giải mã RSA tốn thời gian nhiều hơn mã hóa RSA, điều này là do khóa riêng tư lớn hơn rất nhiều so với khóa công khai. Việc giải mã yêu cầu thực hiện nhiều phép toán phức tạp hơn, do khóa công khai thường là một số nhỏ trong khi khóa bí mật là một số lớn. Quá trình mã hóa chỉ cần tính lũy thừa mô-đun với số mũ nhỏ, trong khi giải mã phải tính với số mũ lớn, làm cho các phép toán trở nên phức tạp và tốn thời gian hơn.**

**- Kết quả này còn cho thấy Linux có hiệu suất mã hóa tốt hơn so với Windows. Việc lựa chọn hệ điều hành và chế độ mã hóa phù hợp là yếu tố quan trọng để đạt được hiệu suất tối ưu trong các ứng dụng đòi hỏi mã hóa nhanh chóng.**