REPORT CRYTOGRAPHY –TASK 3

Student: Trịnh Thị Bích Thảo

ID: 22521376

Lecturer: Nguyễn Ngọc Tự

---

1. Hardware resources.

a. Windows

Current Date/Time:	Friday, June 14, 2024, 9:38:15 AM
Computer Name:	SEIPIEH
Operating System:	Windows 11 Home Single Language 64-bit (10.0, Build 22631)
Language:	English (Regional Setting: English)
System Manufacturer:	ASUSTeK COMPUTER INC.
System Model:	VivoBook_ASUSLaptop X421EAY_A415EA
BIOS:	X421EAY.308
Processor:	11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz (8 CPUs), ~2.4GHz
Memory:	8192MB RAM
Page file:	11903MB used, 11341MB available
DirectX Version:	DirectX 12

b. Linux (ubuntu)

```
sei@TrinhThiBichThao-22521376:~$ lscpu
Architecture:                    x86_64
CPU op-mode(s):                  32-bit, 64-bit
Byte Order:                      Little Endian
Address sizes:                   39 bits physical, 48 bits virtual
CPU(s):                          8
On-line CPU(s) list:             0-7
Thread(s) per core:              2
Core(s) per socket:              4
Socket(s):                       1
NUMA node(s):                    1
Vendor ID:                       GenuineIntel
CPU family:                      6
Model:                           140
Model name:                      11th Gen Intel(R) Core(TM) i5-1135G7 @ 2.40GHz
Stepping:                        1
CPU MHz:                         2400.000
CPU max MHz:                     4200,0000
CPU min MHz:                     400,0000
BogoMIPS:                        4838.40
Virtualization:                  VT-x
L1d cache:                       192 KiB
L1i cache:                       128 KiB
L2 cache:                        5 MiB
L3 cache:                        8 MiB
NUMA node0 CPU(s):               0-7
```

2. Giới thiệu.

Bài báo cáo task 1 bao gồm việc triển khai mã nguồn để thực hiện thuật toán RSA bằng ngôn ngữ C++, sử dụng thư viện CryptoPP để hỗ trợ mã hóa và giải mã. Sau khi xây dựng mã nguồn, em đã tạo 3 tệp tin với các kích thước khác nhau và tiến hành đo thời gian thực hiện 10000 lần mã hóa/giải mã trên cả hai hệ điều hành Windows và Linux. Cuối cùng, kết quả được thống kê và biểu diễn dưới dạng biểu đồ để phân tích và so sánh. Chi tiết cụ thể sẽ được trình bày trong các mục sau.

(Code: cùng folder với file report, folder name: task3. Hoặc trên link github này.)

3. Thống kê và biểu đồ.

a. Thống kê thời gian.

Em tiến hành encrypt/decrypt 3 file input với 3 độ dài key khác nhau. Chi tiết thống kê:

Windows:

RSA ENCRYPT IN WINDOWS			
	3072	4096	7680
File 1 (342 bytes)	1.178		
File 2 (450bytes)		1.057	
File 3 (781 bytes)			2.93

RSA DECRYPT IN WINDOWS			
	3072	4096	7680
File 1 (342 bytes)	67.741		
File 2 (450bytes)		100.966	
File 3 (781 bytes)			581.271

Linux:

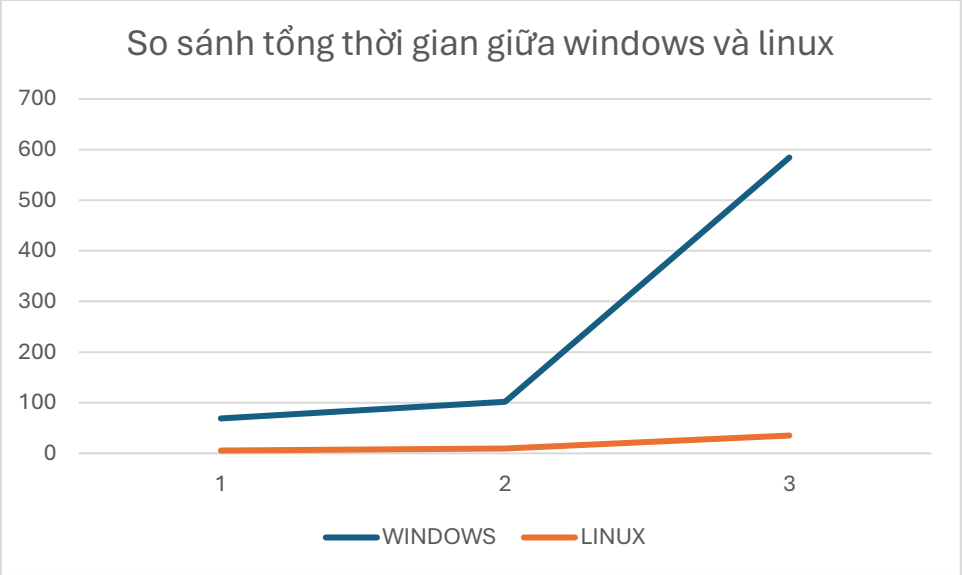
RSA ENCRYPT IN LINUX			
	3072	4096	7680
File 1 (342 bytes)	0.122		
File 2 (450bytes)		0.089	
File 3 (781 bytes)			0.186

RSA DECRYPT IN LINUX			
	3072	4096	7680
File 1 (342 bytes)	5.398		
File 2 (450bytes)		9.435	
File 3 (781 bytes)			34.961

b. So sánh

⇨ Tổng thời gian encrypt và decrypt giữa windows và linux có sự chênh lệnh rõ rệt
⇨ Linux chạy nhanh hơn windows nhiều lần

Tổng time	File 1	File 2	File 3
WINDOWS	68.919	102.023	584.201
LINUX	5.52	9.524	35.147



4. So sánh và phân tích.

- Số liệu cho ta thấy việc giải mã RSA tốn thời gian hơn mã hóa RSA nhiều lần. Bởi vì do khóa riêng tư lớn hơn nhiều so với khóa công khai, dẫn đến số lượng phép toán cần thiết để giải mã lớn hơn đáng kể. Mã hóa sử dụng khóa công khai thường là một số nhỏ (thường là 65537), trong khi giải mã sử dụng khóa riêng tư là một số lớn. Do đó, các phép toán liên quan đến giải mã (lũy thừa mô-đun với số mũ lớn) phức tạp và tốn thời gian hơn so với mã hóa.

- Kết quả này 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 quan trọng để đạt hiệu suất tối ưu trong các ứng dụng yêu cầu mã hóa nhanh chóng.

5. Tổng kết.

Sau bài lab này, em đã biết cách sử dụng thư viện CryptoPP, code implement mã hóa và giải mã RSA bằng thư viện này và có cái nhìn tổng quát về thời gian thực thi của từng loại, nhận thấy sự khác biệt giữa thực thi trên Linux và trên Windows.