VIETNAM NATIONAL UNIVERSITY, HO CHI MINH CITY UNIVERSITY OF INFORMATION TECHNOLOGY FALCUTY OF COMPUTER NETWORKS AND COMMUNICATION

OFF-CLASS REPORT

LAB 3

Instructor: PhD. Nguyễn Ngọc Tự

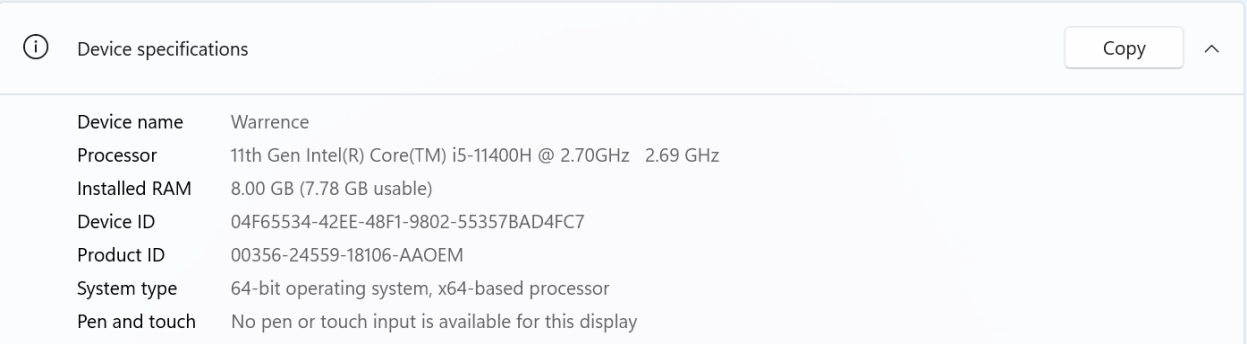
Student: 22521050 – Nguyễn Đặng Quỳnh Như

Chi tiết các thống kê trong báo cáo xem ở: 22521050-Lab3.xlsx

Link github: https://github.com/listimdn10/Crypto-Offclass.git

1. Hardware resources.

a. Windows



b. Linux (ubuntu)

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.

3. Thống kê

a. Thống kê thời gian.

- Tiến hành encrypt/decrypt 3 file input với 3 độ dài key khác nhau.

3.1 Chi tiết thống kê: Windows:

RSA Encryption in Windows (ms)

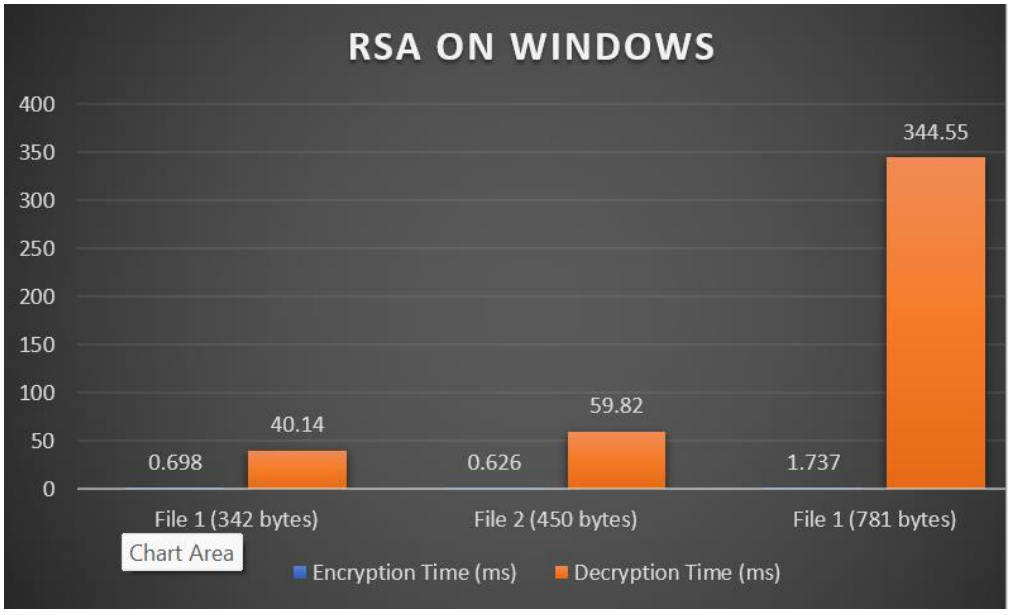
File	3072-bit	4096-bit	7680-bit
File 1 (342 bytes)	0.698		
File 2 (450 bytes)		0.626	
File 3 (781 bytes)			1.737

RSA Decryption in Windows (ms)

File	3072-bit	4096-bit	7680-bit
File 1 (342 bytes)	40.14		
File 2 (450 bytes)		59.82	
File 3 (781 bytes)			344.55

Ta se co:

File Size	RSA Key Size	Encryption Time (ms)	Decryption Time (ms)
File 1 (342 bytes)	3072-bit	0.698	40.14
File 2 (450 bytes)	4096-bit	0.626	59.82
File 1 (781 bytes)	7680-bit	1.737	344.55



3.2 Chi tiết thống kê: linux

RSA Encryption in Linux (ms)

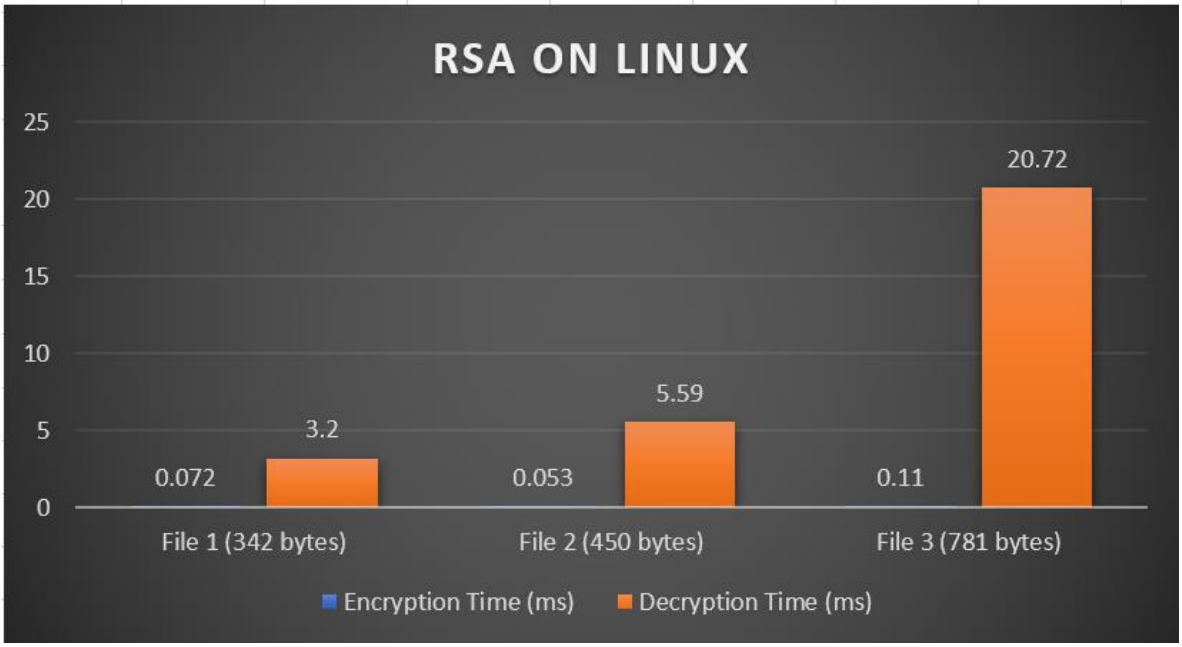
File	3072-bit	4096-bit	7680-bit
File 1 (342 bytes)	0.072		
File 2 (450 bytes)		0.053	
File 3 (781 bytes)			0.110

RSA Decryption in Linux (ms)

File	3072-bit	4096-bit	7680-bit
File 1 (342 bytes)	3.20		
File 2 (450 bytes)		5.59	
File 3 (781 bytes)			20.72

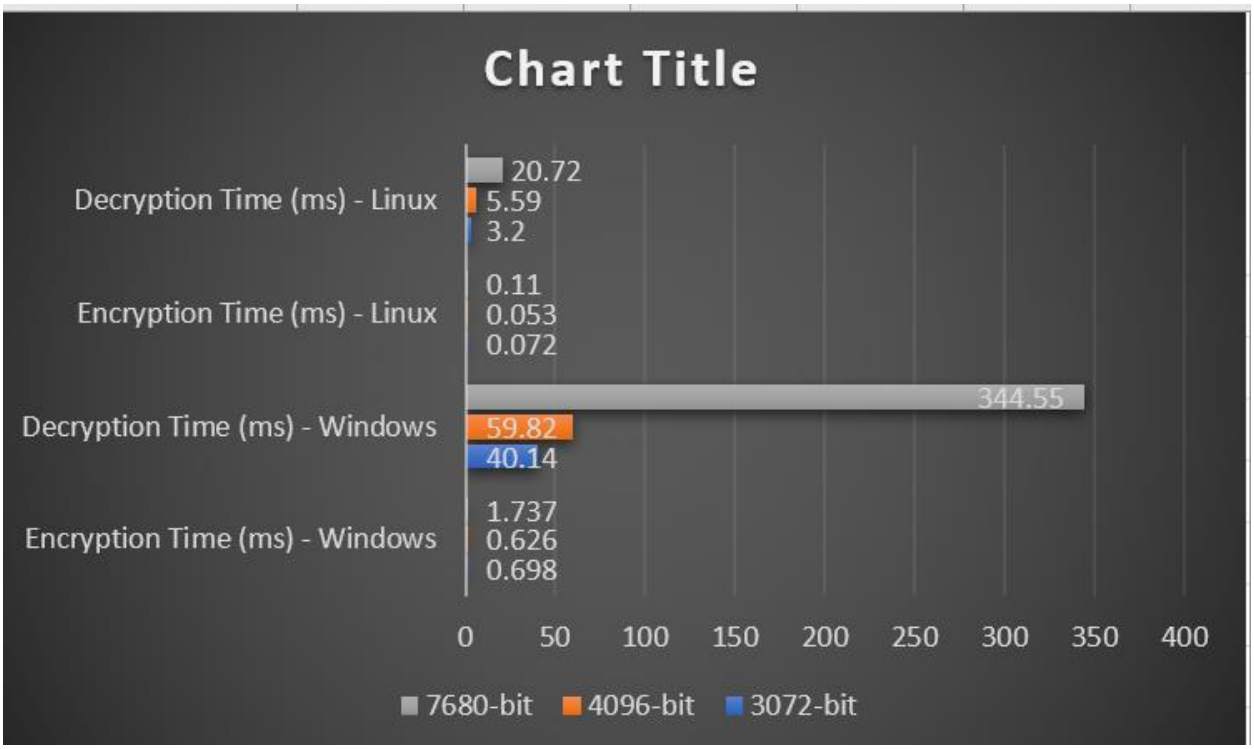
Ta sẽ có:

File Size	RSA Key Size	Encryption Time (ms)	Decryption Time (ms)
File 1 (342 bytes)	3072-bit	0.072	3.2
File 2 (450 bytes)	4096-bit	0.053	5.59
File 3 (781 bytes)	7680-bit	0.11	20.72



Kết luận:

RSA Key Size	Encryption Time (ms) - Windows	Decryption Time (ms) - Windows	Encryption Time (ms) - Linux	Decryption Time (ms) - Linux
3072-bit	0.698	40.14	0.072	3.2
4096-bit	0.626	59.82	0.053	5.59
7680-bit	1.737	344.55	0.11	20.72



Dựa vào bảng so sánh thời gian mã hóa và giải mã RSA trên hai hệ điều hành Windows và Linux, chúng ta có thể thấy một số điểm khác biệt chính:

1. **Tốc độ mã hóa**:
   - Trên cả ba kích thước tệp, Linux mã hóa nhanh hơn Windows một cách đáng kể.
   - Với khóa 3072-bit, thời gian mã hóa trên Linux là 0.072 ms, nhanh hơn khoảng 10 lần so với 0.698 ms trên Windows.
   - Với khóa 4096-bit, thời gian mã hóa trên Linux là 0.053 ms, nhanh hơn khoảng 12 lần so với 0.626 ms trên Windows.
   - Với khóa 7680-bit, thời gian mã hóa trên Linux là 0.110 ms, nhanh hơn khoảng 16 lần so với 1.737 ms trên Windows.
2. **Tốc độ giải mã**:
   - Linux cũng giải mã nhanh hơn Windows một cách đáng kể.
   - Với khóa 3072-bit, thời gian giải mã trên Linux là 3.2 ms, nhanh hơn khoảng 12.5 lần so với 40.14 ms trên Windows.

- Với khóa 4096-bit, thời gian giải mã trên Linux là 5.59 ms, nhanh hơn khoảng 10.7 lần so với 59.82 ms trên Windows.
- Với khóa 7680-bit, thời gian giải mã trên Linux là 20.72 ms, nhanh hơn khoảng 16.6 lần so với 344.55 ms trên Windows.

3. **Hiệu quả xử lý**:
   - Linux cho thấy hiệu suất vượt trội hơn nhiều so với Windows trong cả mã hóa và giải mã RSA. Điều này có thể là do cách Linux quản lý tài nguyên hệ thống và tối ưu hóa các tác vụ tính toán mã hóa tốt hơn so với Windows.

Tóm lại, Linux vượt trội hơn Windows trong cả hai khía cạnh mã hóa và giải mã RSA, cho thấy sự ưu việt trong hiệu suất của Linux đối với các tác vụ mã hóa đòi hỏi nhiều tính toán.