REPORT CRYTOGRAPHY –TASK 5

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 5 bao gồm việc triển khai mã nguồn để thực hiện các thuật toán chữ ký số ECDSA, RSASS-PSS bằng ngôn ngữ C++, sử dụng thư viện OpenSSL để hỗ trợ.

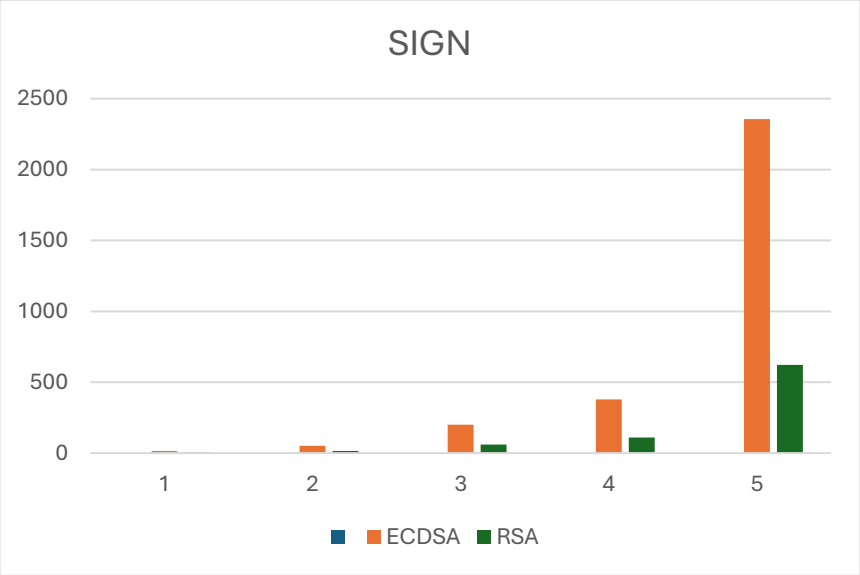
3. Thống kê, báo cáo

a. Thống kê thời gian.

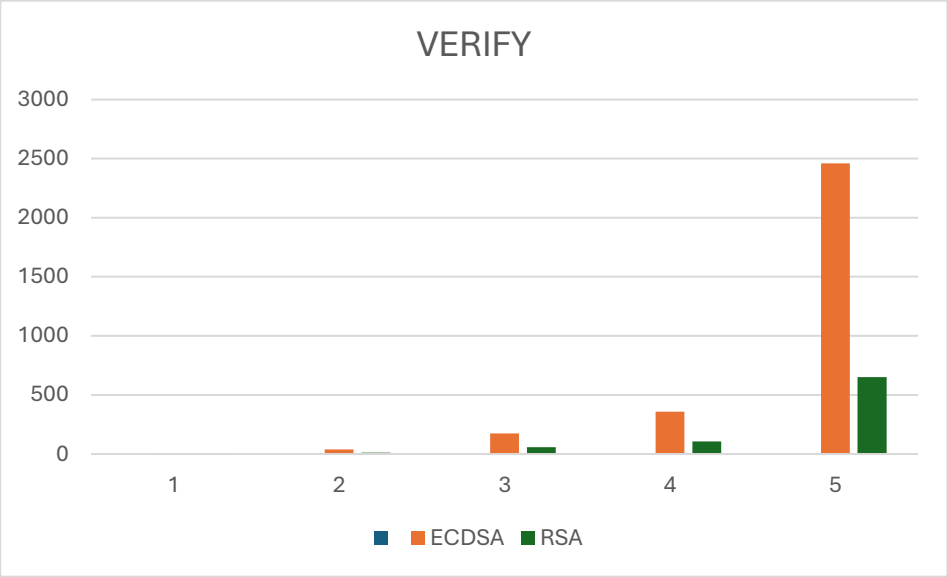
Em tiến hành kí và xác thực các file input theo 5 size khác nhau (milliseconds). Thời gian có tính thêm thời gian đọc file.

Windows:

		SIGN			
	1MB	10MB	50MB	100MB	1GB
ECDSA	15.664	51.2889	201.23	379.089	2356.1
RSA	5.229	15.637	59.548	110.691	622.375

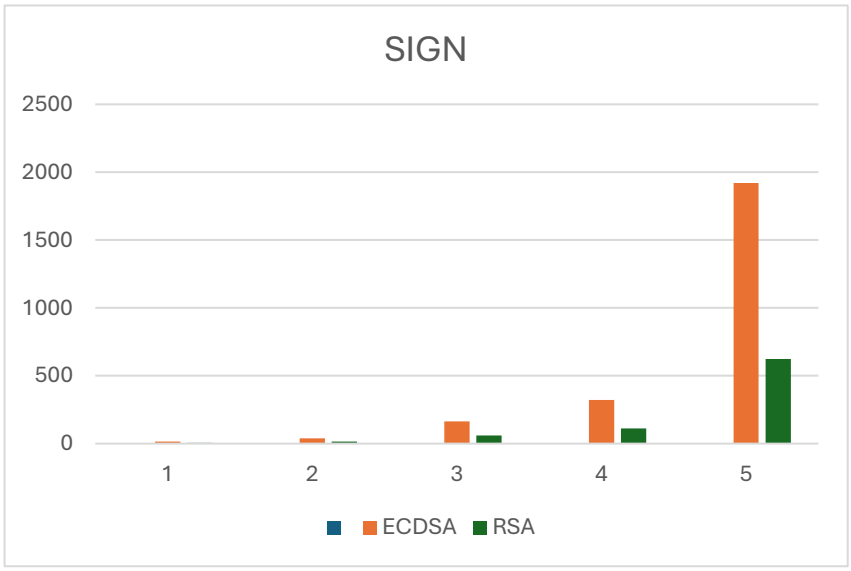


	VERIFY				
	1MB	10MB	50MB	100MB	1GB
ECDSA	6.0043	38.1268	174.232	357.261	2459.85
RSA	2.998	12.519	58.806	107.634	650.998

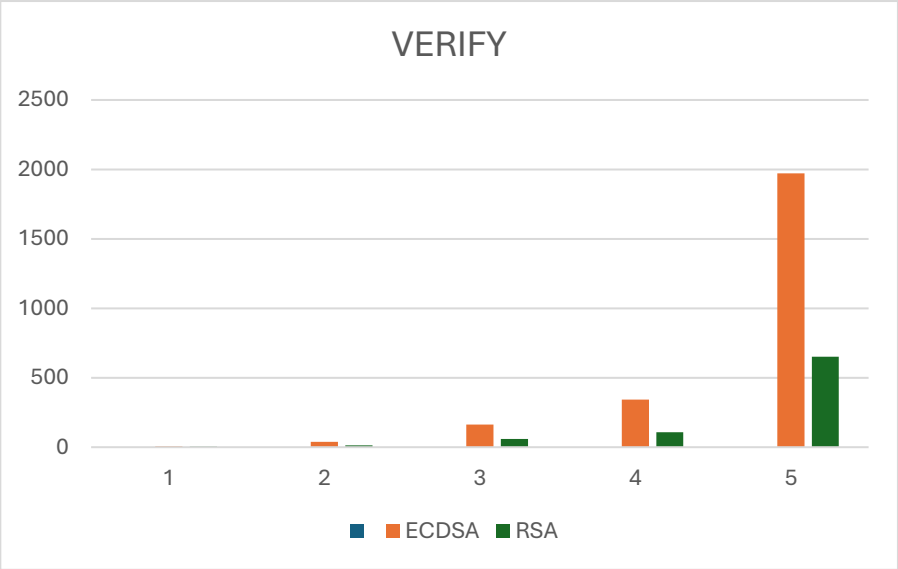


Linux:

	SIGN				
	1MB	10MB	50MB	100MB	1GB
ECDSA	14.958	38.817	162.676	321.572	1920.65
RSA	11.135	15.147	56.042	120.097	658.51



	VERIFY				
	1MB	10MB	50MB	100MB	1GB
ECDSA	5.796	38.232	163.364	342.628	1970.53
RSA	1.703	9.982	42.13	82.008	452.218



b. So sánh ECDSA giữa linux và windows

⇨ Tổng thời gian kí và xác thực giữa linux và windows có sự chênh lệch
⇨ Linux chạy nhanh hơn windows

	1MB	10MB	50MB	100MB	1GB
WINDOWS	21.6683	89.4157	375.462	736.35	4815.95
LINUX	20.754	77.049	326.04	664.2	3891.18