REPORT CRYTOGRAPHY – TASK 1-2

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 DES và AES 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 6 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: task1. Hoặc trên link github này.)

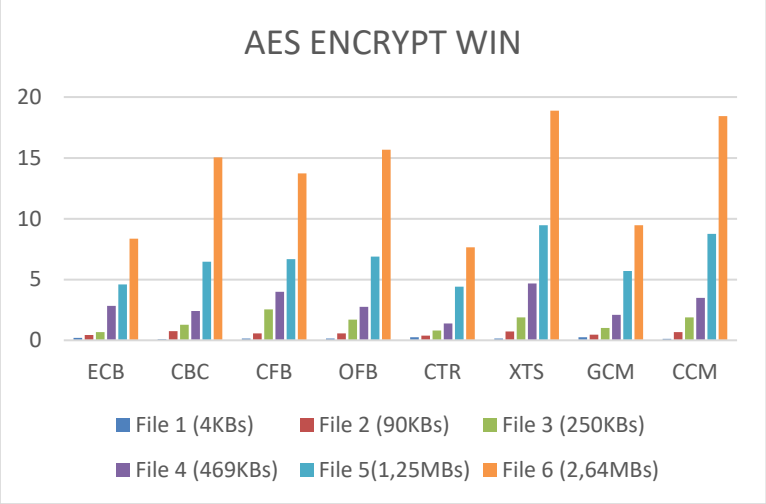
3. Thống kê và biểu đồ.

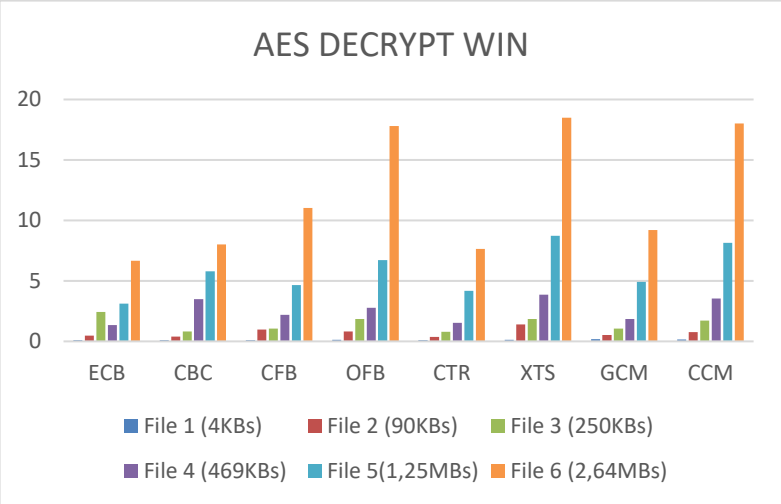
a. Thống kê thời gian.

Em tiến hành encrypt/decrypt 6 file input với 8 mode. Chi tiết thống kê:

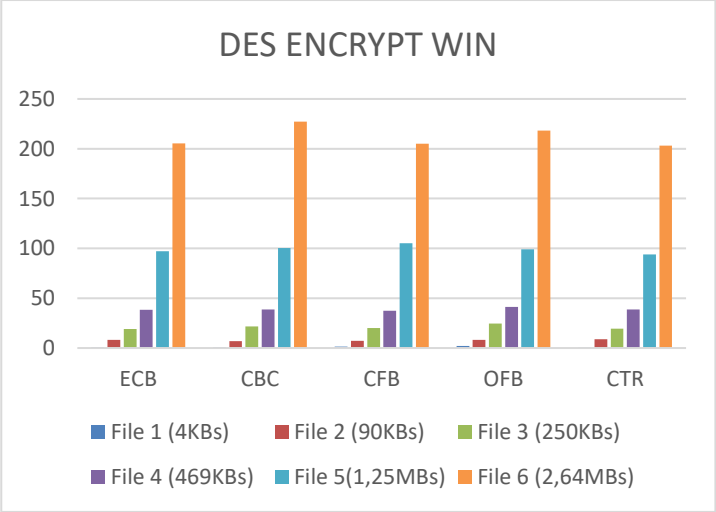
Windows:

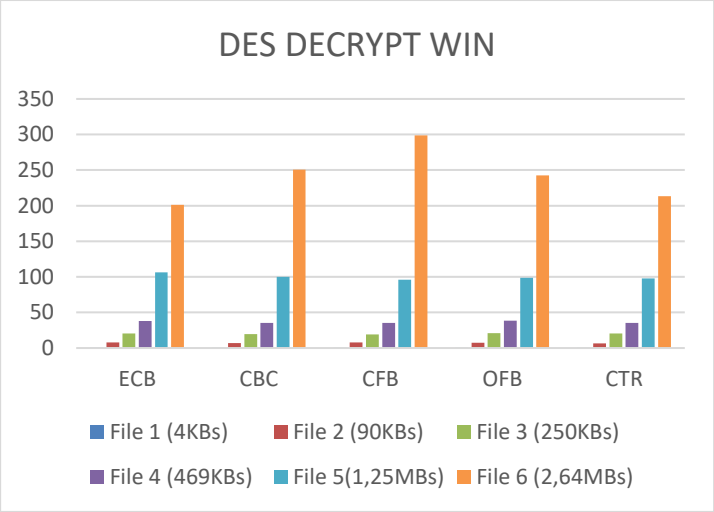
AES Runtime in WINDOWS (ms)								
Encrypt	**ECB**	**CBC**	**CFB**	**OFB**	**CTR**	**XTS**	**GCM**	**CCM**
File 1 (4KBs)	0.2	0.106	0.151	0.143	0.261	0.14	0.244	0.129
File 2 (90KBs)	0.448	0.747	0.568	0.58	0.388	0.739	0.469	0.679
File 3 (250KBs)	0.678	1.292	2.543	1.701	0.809	1.891	1.007	1.883
File 4 (469KBs)	2.841	2.413	3.98	2.753	1.383	4.673	2.091	3.478
File 5(1,25MBs)	4.599	6.463	6.684	6.887	4.403	9.455	5.693	8.748
File 6 (2,64MBs)	8.344	15.052	13.719	15.679	7.638	18.882	9.455	18.427
Decrypt	**ECB**	**CBC**	**CFB**	**OFB**	**CTR**	**XTS**	**GCM**	**CCM**
File 1 (4KBs)	0.11	0.092	0.092	0.12	0.107	0.121	0.186	0.151
File 2 (90KBs)	0.468	0.396	0.987	0.823	0.369	1.411	0.518	0.772
File 3 (250KBs)	2.429	0.806	1.069	1.853	0.784	1.84	1.047	1.712
File 4 (469KBs)	1.344	3.497	2.203	2.771	1.52	3.854	1.851	3.546
File 5(1,25MBs)	3.118	5.792	4.657	6.729	4.179	8.731	4.93	8.144
File 6 (2,64MBs)	6.662	8.014	11.037	17.805	7.632	18.5	9.208	18.029





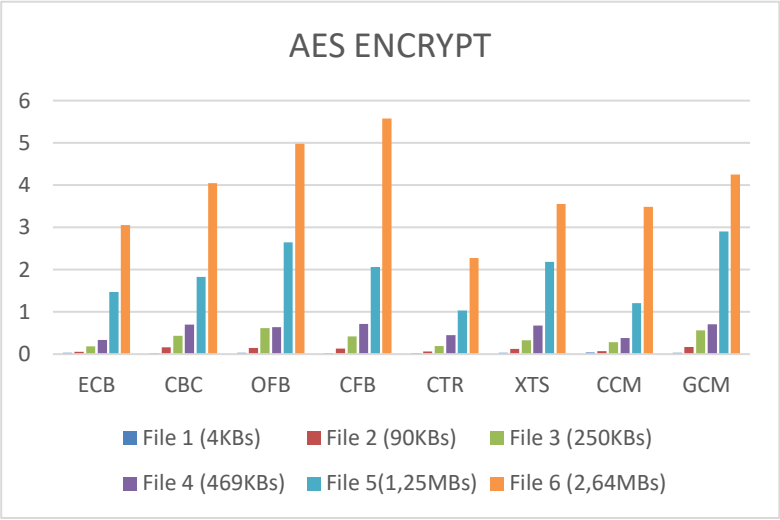
DES Runtime in WINDOWS					
Encrypt	**ECB**	**CBC**	**CFB**	**OFB**	**CTR**
File 1 (4KBs)	0.655	0.836	1.592	2.053	0.532
File 2 (90KBs)	8.235	7.066	7.383	8.28	8.971
File 3 (250KBs)	19.112	21.831	20.024	24.583	19.458
File 4 (469KBs)	38.273	38.728	37.344	41.419	38.75
File 5(1,25MBs)	97.252	100.311	105.22	98.982	93.95
File 6 (2,64MBs)	205.395	227.261	204.937	218.314	203.092
Decrypt	**ECB**	**CBC**	**CFB**	**OFB**	**CTR**
File 1 (4KBs)	0.542	0.319	0.336	0.37	0.349
File 2 (90KBs)	7.698	6.984	7.865	7.645	6.648
File 3 (250KBs)	20.277	19.644	19.088	20.939	20.372
File 4 (469KBs)	38.057	35.338	35.23	38.288	35.1
File 5(1,25MBs)	106.526	100.236	96.037	98.502	97.974
File 6 (2,64MBs)	201.368	250.58	298.604	242.781	213.276

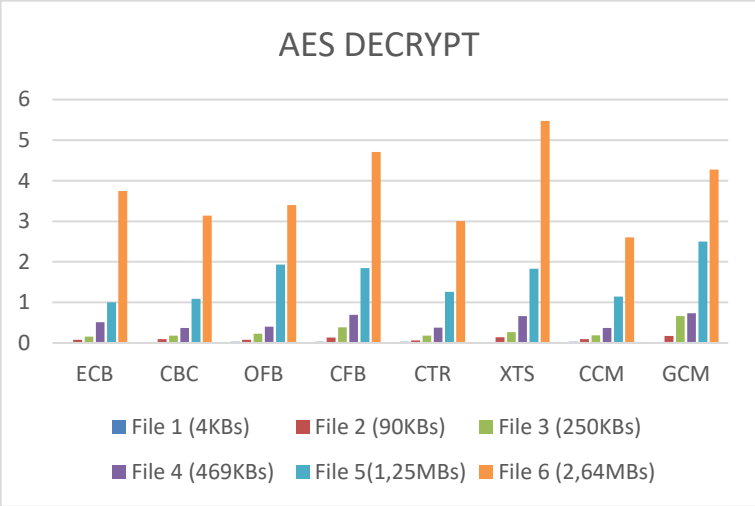




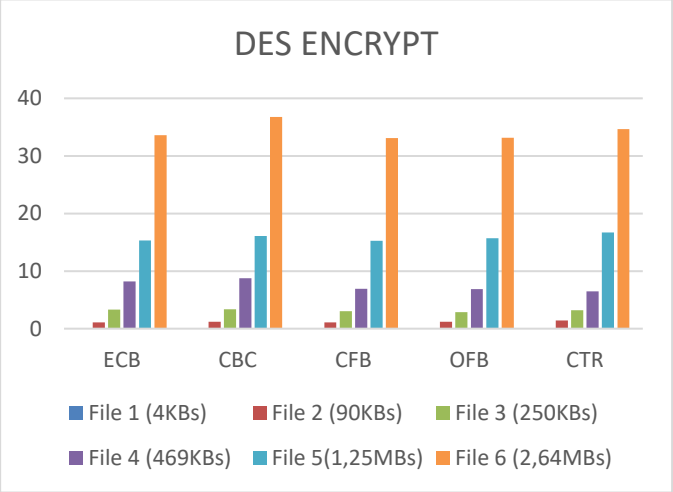
Linux:

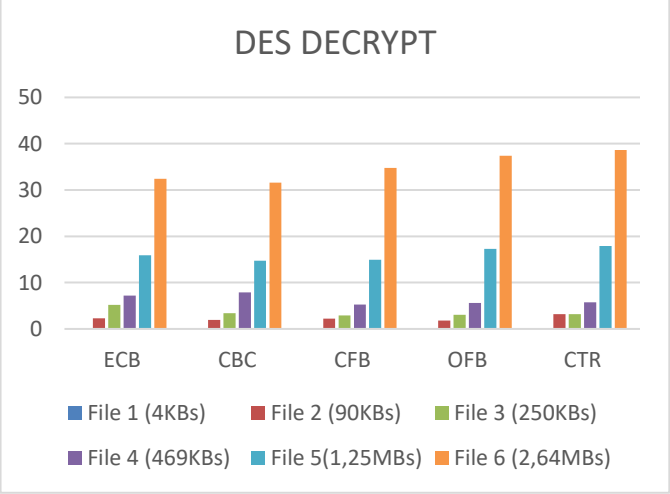
AES Runtime in LINUX (ms)								
Encrypt	**ECB**	**CBC**	**OFB**	**CFB**	**CTR**	**XTS**	**CCM**	**GCM**
File 1 (4KBs)	0.029	0.022	0.03	0.023	0.028	0.029	0.043	0.029
File 2 (90KBs)	0.059	0.159	0.146	0.13	0.063	0.122	0.073	0.166
File 3 (250KBs)	0.181	0.435	0.615	0.417	0.195	0.33	0.285	0.565
File 4 (469KBs)	0.339	0.697	0.636	0.712	0.449	0.674	0.381	0.706
File 5(1,25MBs)	1.475	1.829	2.648	2.064	1.036	2.187	1.205	2.905
File 6 (2,64MBs)	3.052	4.046	4.978	5.58	2.272	3.554	3.486	4.251
Decrypt	**ECB**	**CBC**	**OFB**	**CFB**	**CTR**	**XTS**	**CCM**	**GCM**
File 1 (4KBs)	0.019	0.025	0.028	0.03	0.031	0.025	0.033	0.025
File 2 (90KBs)	0.077	0.091	0.078	0.129	0.059	0.137	0.094	0.17
File 3 (250KBs)	0.16	0.178	0.226	0.387	0.183	0.267	0.186	0.662
File 4 (469KBs)	0.508	0.367	0.398	0.693	0.38	0.664	0.368	0.736
File 5(1,25MBs)	0.999	1.088	1.934	1.845	1.262	1.83	1.143	2.499
File 6 (2,64MBs)	3.748	3.139	3.398	4.71	3.006	5.476	2.602	4.274





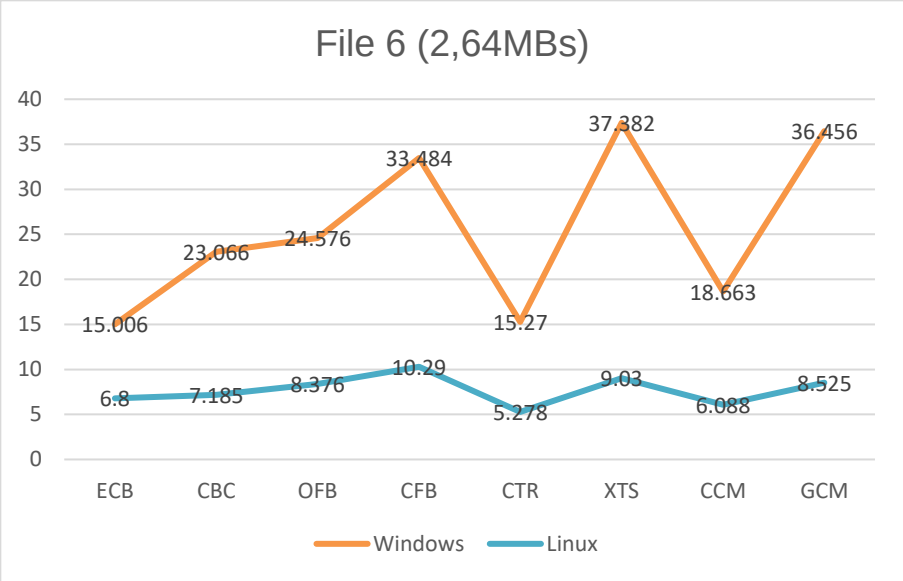
DES Runtime in LINUX					
Encrypt	**ECB**	**CBC**	**CFB**	**OFB**	**CTR**
File 1 (4KBs)	0.055	0.049	0.04	0.05	0.043
File 2 (90KBs)	1.067	1.171	1.071	1.221	1.426
File 3 (250KBs)	3.312	3.39	3.044	2.887	3.176
File 4 (469KBs)	8.215	8.751	6.943	6.891	6.503
File 5(1,25MBs)	15.321	16.098	15.243	15.694	16.703
File 6 (2,64MBs)	33.623	36.785	33.083	33.137	34.643
Decrypt	**ECB**	**CBC**	**CFB**	**OFB**	**CTR**
File 1 (4KBs)	0.041	0.029	0.03	0.036	0.031
File 2 (90KBs)	2.269	1.939	2.248	1.823	3.19
File 3 (250KBs)	5.214	3.389	2.908	3.067	3.165
File 4 (469KBs)	7.183	7.889	5.288	5.585	5.761
File 5(1,25MBs)	15.88	14.763	14.939	17.304	17.909
File 6 (2,64MBs)	32.442	31.584	34.796	37.398	38.661





⇨ Tổng thời gian encrypt và decrypt giữa windows và linux có sự chênh lệnh rõ rệt, biểu hiện rõ ràng nhất ở File 6 (2,64Mbs) (AES)

⇨ Linux chạy nhanh hơn windows



4. So sánh và phân tích.

- Biểu đồ cho thấy thời gian mã hóa của một file 2.64MB trên các chế độ mã hóa khác nhau trên Windows và Linux. Linux mã hóa nhanh hơn Windows đáng kể. Điều này có thể do Linux quản lý tài nguyên và tối ưu hệ thống tốt hơn.

- CTR là chế độ nhanh nhất vì mã hóa và giải mã từng block song song và không yêu cầu xử lý phức tạp. Chế độ ECB cũng có thời gian mã hóa ngắn do mã hóa từng block riêng lẻ mà không có sự phụ thuộc giữa các block. Ngược lại, các chế độ như XTS và GCM chậm hơn trên Windows do các bước xử lý phức tạp. Thời gian mã hóa của các chế độ còn lại như CBC, OFB, và CFB trên Linux cũng nhanh hơn Windows rõ rệt.

- 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.

- Trong từng mode, kích thước đầu vào càng lớn thì thời gian mã hóa và giải mã càng lâu.

5. Tổng kết.

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