REPORT TASK 1

Môn học: Mật mã học

Giảng viên: Nguyễn Ngọc Tự

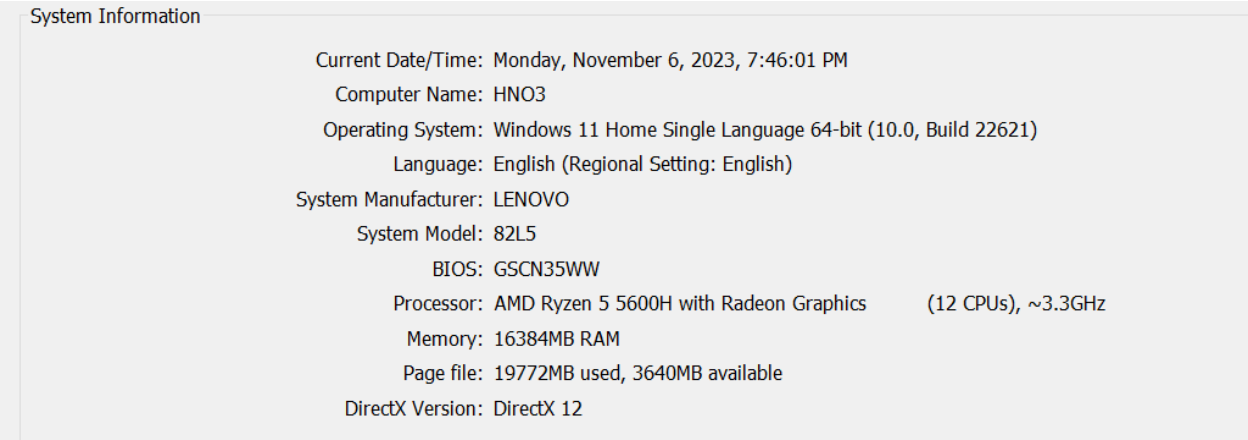
Thái Vĩnh Đạt – 22520235 – ATTN2022

1. Abstract

Đây là bài báo cáo task 1 về mã hóa và giải mã AES (Advance encryption standard). Đây là 1 trong các thuật toán mã hóa khối (block cipher), nó là kiểu mã hóa dữ liệu phổ biến nhất sử dụng khóa đối xứng (Symmetric cipher). Nội dung bài task này là sử dụng thư viện CryptoPP trong C++ để thực hiện mã hóa và giải mã trên nhiều mode khác nhau, sau đó chạy và đo thời gian chạy trên nhiều file input với nhiều kích thước và chạy trên 2 hệ điều hành Window và Ubuntu (linux).

(Toàn bộ file thầy yêu cầu em đều đính kèm đủ trong file rar. Full source code của 2 bài task đều có sẵn trên link github này)

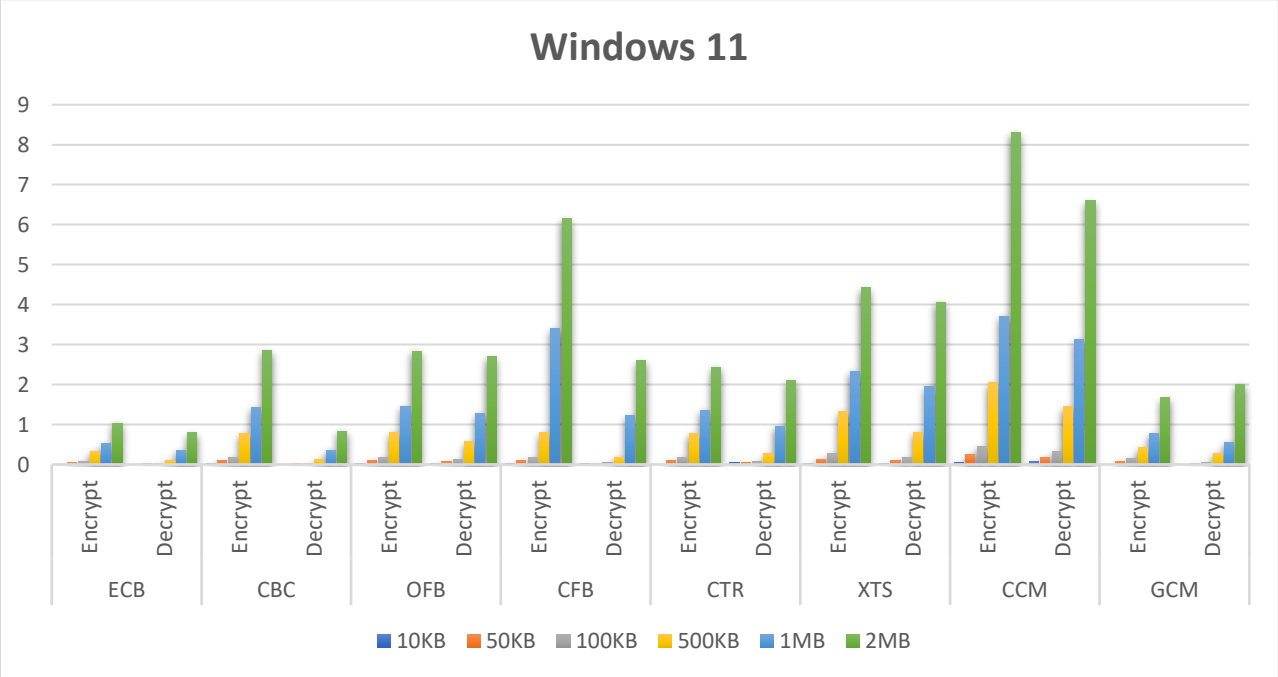
2. Hardware resource



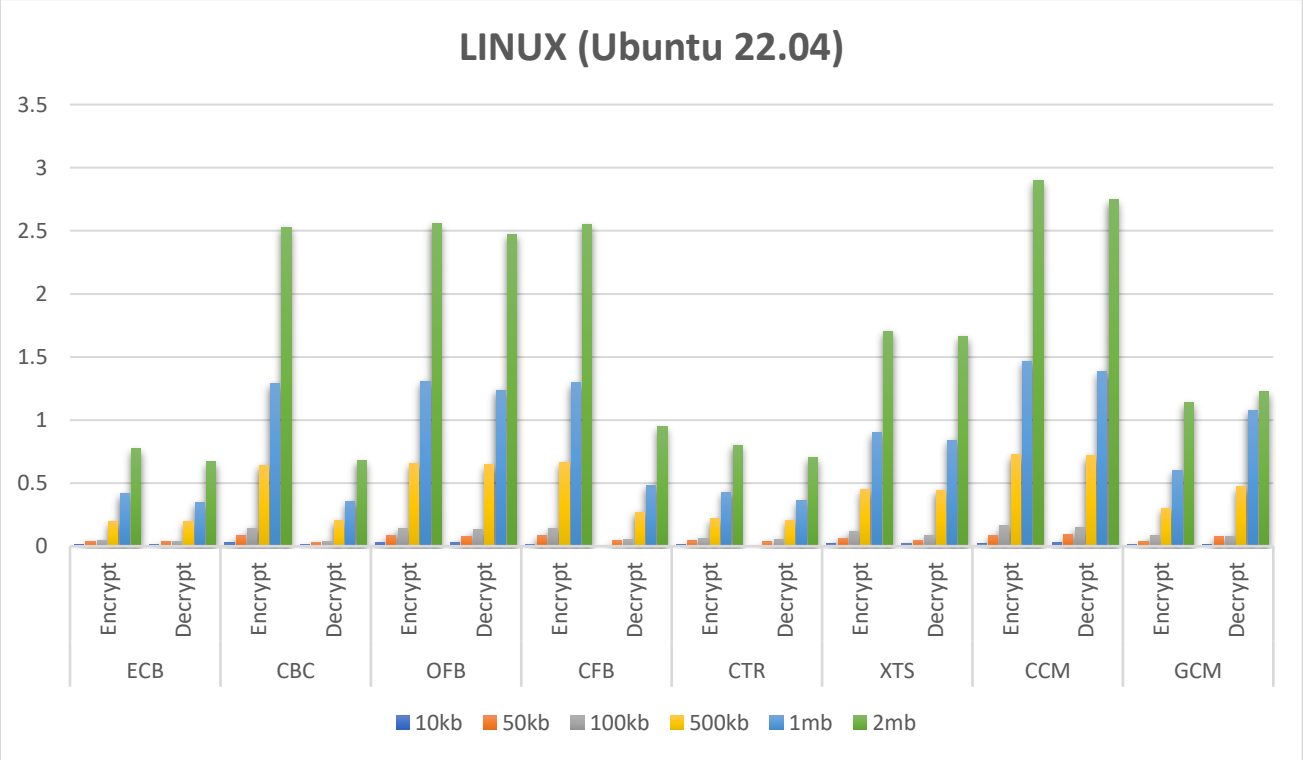
3. Thống kê và biểu đồ:

Sau đây là bảng số liệu em thu thập được sau khi encrypt và decrypt lần lượt 8 mode trên 6 file có kích thước khác nhau, mỗi lần chạy em cho encrypt/decrypt 1000 lần và lấy thời gian trung bình mỗi lần.

Window 11							
Modes		10KB	50KB	100KB	500KB	1MB	2MB
ECB	Encrypt	0.005(ms)	0.058	0.083	0.335	0.527	1.031
	Decrypt	0.01	0.017	0.027	0.109	0.354	0.791
CBC	Encrypt	0.015	0.099	0.165	0.784	1.424	2.852
	Decrypt	0.01	0.017	0.029	0.115	0.36	0.837
OFB	Encrypt	0.015	0.095	0.17	0.803	1.45	2.832
	Decrypt	0.026	0.066	0.123	0.575	1.276	2.696
CFB	Encrypt	0.015	0.094	0.165	0.792	3.404	6.155
	Decrypt	0.016	0.023	0.043	0.185	1.215	2.6
CTR	Encrypt	0.01	0.095	0.171	0.775	1.359	2.431
	Decrypt	0.037	0.038	0.068	0.271	0.952	2.106
XTS	Encrypt	0.02	0.133	0.266	1.327	2.337	4.42
	Decrypt	0.02	0.094	0.165	0.808	1.956	4.055
CCM	Encrypt	0.038	0.239	0.447	2.041	3.713	8.311
	Decrypt	0.074	0.167	0.318	1.442	3.128	6.603
GCM	Encrypt	0.007	0.084	0.151	0.423	0.779	1.667
	Decrypt	0.008	0.0269	0.0512	0.2858	0.5542	2.0058



LINUX (Ubuntu 22.04)							
Mode		10kb	50kb	100kb	500kb	1mb	2mb
ECB	Encrypt	0.011(ms)	0.036	0.049	0.194	0.417	0.772
	Decrypt	0.014	0.036	0.041	0.197	0.344	0.668
CBC	Encrypt	0.028	0.083	0.144	0.64	1.288	2.529
	Decrypt	0.014	0.033	0.041	0.202	0.356	0.679
OFB	Encrypt	0.032	0.086	0.14	0.658	1.307	2.554
	Decrypt	0.028	0.08	0.132	0.645	1.237	2.471
CFB	Encrypt	0.016	0.082	0.142	0.665	1.295	2.549
	Decrypt	0.007	0.043	0.052	0.27	0.485	0.946
CTR	Encrypt	0.013	0.042	0.065	0.217	0.429	0.8
	Decrypt	0.008	0.034	0.056	0.205	0.36	0.7
XTS	Encrypt	0.02	0.065	0.117	0.449	0.899	1.703
	Decrypt	0.025	0.049	0.083	0.445	0.841	1.661
CCM	Encrypt	0.019	0.088	0.163	0.727	1.466	2.899
	Decrypt	0.03	0.092	0.145	0.716	1.382	2.745
GCM	Encrypt	0.014	0.038	0.082	0.3	0.601	1.137
	Decrypt	0.011	0.076	0.081	0.473	1.076	1.225



4. So sánh và nhận xét:

- Theo số liệu và biểu đồ ở trên, có thể thấy kích thước input càng lớn thì thời gian mã hóa và giải mã cũng càng lớn (điều này khá hiển nhiên).
- Đối với các mode với nhau, có thể thấy thời gian encrypt và decrypt của ECB nhanh hơn hẳn so với các mode còn lại nếu làm việc trên cùng input cùng kích thước. Điều này đến là vì mode ECB là một mode làm việc đơn giản nhất (mã hóa từng block riêng biệt), và hiển nhiên nó cũng dễ bị tấn công nhất. Ngược lại, mode CCM là mode có thời gian mã hóa/giải mã lâu nhất, lý do khiến AES mode CCM có thời gian mã hóa/giải mã lâu nhất là do nó kết hợp hai phương pháp mã hóa khác nhau: chế độ đếm (counter mode) và CBC-MAC (Cipher Block Chaining Message Authentication Code), mỗi phương pháp đều yêu cầu những bước tính toán phức tạp, tuy nhiên đánh đổi cho thời gian mã hóa là tính bảo mật mà nó mang lại được cho là rất an toàn.
- So sánh giữa 2 hệ điều hành thì ta thấy hầu hết Ubuntu chạy nhanh hơn hẳn Windows, điều này đến từ nhiều vấn đề của cài đặt hệ thống, việc quản lí tài nguyên, v.v.... của hai hệ điều hành này.