# **REPORT CRYTOGRAPHY – TASK 1**

Student: Nguyễn Thị Quỳnh Anh

ID: 22520064

Lecturer: Nguyễn Ngọc Tự

1. **Hardware resources.**
   1. **Windows**

**A screenshot of a computer

Description automatically generated**

* 1. **Linux (ubuntu)**

A screenshot of a computer

Description automatically generated

1. **Giới thiệu.**

Bài báo cáo task 1 bao gồm báo cáo code implement thuật toán AES bằng ngôn ngữ C++ và sử dụng thư viện CryptoPP hỗ trợ việc mã hóa và giải mã. Sau khi xây dựng code thì tiến hành tạo 6 file với kích thước khác nhau, thực hiện đo thời gian 1000 lần mã hóa/giải mã trên cả OS Windows và Linux. Cuối cùng thống kê, vẽ biểu đồ phân tích và so sánh. Chi tiết hơn em xin trình bày ở các mục sau.

*(Code: cùng folder với file report, folder name: task1. Hoặc trên link github* [*này*](https://github.com/ik-nown/Cryptography)*.)*

1. **Thống kê và biểu đồ.**
   1. **Thống kê thời gian.**

Em tiến hành encrypt/decrypt 6 file input với 8 mode. Sau đây là bảng thống kê chi tiết.

**Windows:**

A table of numbers and letters

Description automatically generated

**Linux:**

**A table of numbers and letters

Description automatically generated with medium confidence**

*(Bảng thống kê chi tiết tại file statistical.xlsx)*

Bởi vì thời gian giữa 4 file đầu tiên không có sự chênh lệch lớn, nên em sẽ vẽ biểu đồ thời gian xử lí của 6 với kích thước là 2.64MBs để dễ dàng so sánh giữa hai hệ điều hành khác nhau.

* 1. **Biểu đồ so sánh.**
     1. **Biểu đồ hóa hai bảng thống kê.**

Figure Encryption in Windows

Figure Decryption in Windows

Figure Encryption in Linux

Figure Decryption in Linux

* + 1. **Biểu đồ giữa linux và windows.**

Figure Encryption

1. **So sánh và phân tích.**

Theo thống kê thì thời gian giữa quá trình decrypt và encrypt giữa của các mode không chênh lệch lớn về thời gian, nằm trong khoảng ( ~0.1 đến 1.0 ms). Do đó em chọn một trong hai quá trình này so sánh giữa linux và windows (Figure 5) và chọn file lớn nhất trong các testcase của em để dễ dàng nhận thấy sự khác biệt.

Giữa hai OS thì thời gian chạy của Linux (Ubuntu) nhanh hơn hẳn so với

Windows, thời gian nhanh hơn gấp nhiều lần. Đặc biệt là dùng ECB mode, Linux nhanh hơn Windows khoảng 10 lần. Sự khác biệt này liên quan tới nhiều vấn đề của cài đặt hệ thống, việc quản lí tài nguyên, v.v.... của hai hệ điều hành này.

Giữa các mode với nhau, thời gian của mode ECB là nhanh nhất, bởi vì ECB mã hóa từng block riêng lẽ với nhau và không có các thao tác phức tạp (ví dụ XOR với IV) như các mode khác, và vì ECB mã hóa và giải mã theo từng khối độc lập nên khối sau không phụ thuộc vào khối trước, do đó các khối được xử lí đồng thời (song song) nên hiệu suất cao hơn. CCM mode là mode có thời gian xử lí lâu nhất, bởi vì CCM ( Counter with CBC-MAC) là mode khá phức tạp, kết hợp giữa CTR và CBC-MAC đóng vai trò đảm bảo độ xác thực. Ngoài ra, thời gian của các mode còn lại khá tương đồng nhau, file nhỏ hơn 1MBs thì càng chênh lệch rất ít – không đáng kể.

Trong từng mode, input size càng lớn thì thời gian mã hóa và thời gian giải mã càng lâu.

1. **Tổng kết.**

Sau bài lab này, em đã biết cách sử dụng thư viện CryptoPP, code implement mã hóa và giải mã AES bằng thư viện này, build task, dual boot 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.