LAB 5 – THUẬT TOÁN MÃ HÓA TIÊN TIẾN AES

Author: Trần Quý Nam

Date: 24/3/2025

Sinh viên cài đặt thực thi các chương trình sau dùng C++:

Bài 1. Mã hóa AES. Cài đặt chương trình C++ thực hiện mã hóa AES. Trong bài tập này, sinh viên cần cài đặt thuật toán AES trong C++ để thực hiện mã hóa và giải mã dữ liệu văn bản:

- Mã hóa dữ liệu văn bản đầu vào bằng AES.
- Giải mã văn bản đã được mã hóa để khôi phục nội dung gốc.
- Hỗ trợ AES-128 (Khóa 128-bit).

Sinh viên có thể tham khảo codes trên các links (nhưng cần hiểu và giải thích được codes):

- https://github.com/ceceww/aes
- https://github.com/SergeyBel/AES

Bài 2. Xây dựng chương trình thực hiện thuật toán AES với ứng dụng nhắn tin. Có thể sử dụng một trong các cách sau:

- Sử dụng lập trình Socket Programming dựa trên giao thức TCP/IP dùng ngôn ngữ C++/Java hay Python.
- Sử dụng lập trình Web, dùng các framework với ngôn ngữ JavaScript hay Python.
- Sử dụng các giao diện đồ họa GUI trên bất cứ ngôn ngữ lập trình và thư viện đồ họa nào sinh viên yêu thích.

Bài 3: Xây dựng chương trình thực hiện thuật toán AES với file dữ liệu với nội dung file liên quan đến "Dai Nam University"

- Sử dụng lập trình C++ vào ra với tệp dữ liệu.
- Mã hóa AES dữ liệu trong file và ghi vào file khác.
- Đọc file mã hóa, giải mã AES và chuyển thành file dữ liệu ban đầu.
