LAB 7 – MÃ HÓA RSA

Author: Trần Quý Nam

Date: 05/4/2025

Bài 1. Xây dựng ứng dụng mã hóa và giải mã tin nhắn sử dụng RSA (không sử dụng thư viện) có các chức năng:

- Có menu: tạo khóa, gửi tin nhắn (mã hóa), nhận tin nhắn (giải mã), thoát
- Tạo cặp khóa RSA (public, private)
- Mã hóa tin nhắn sử dụng khóa công khai
- Giải mã tin nhắn sử dụng khóa riêng
- Hiển thị rõ quá trình mã hóa và giải mã

Bài 2. Xây dựng ứng dụng sử dụng mã hóa RSA (có sử dụng thư viện, ví dụ Python có thư viện cryptography hoặc PyCryptodome hoặc C++ có thư viện Crypto++) với các chức năng chính:

- Tạo cặp khóa RSA (public, private) và lưu khóa vào file
- Mã hóa và giải mã tin nhắn (messages)
- Mã hóa và giải mã thông tin ghi trong file. Ghi bản mã vào file và đọc, giải mã bản mã từ file.
- Mã hóa các file nhỏ (PDF, TXT, hình ảnh)
- Cho phép gửi nhận tin nhắn qua mạng LAN (socket)
