Lab 9: Chữ ký số và Trao đổi khóa

Author: Trần Quý Nam

Date: 05/4/2025

Bài 1: Xây dựng chương trình C++ thực hiện ký và xác minh chữ ký số cho file văn bản sử dụng RSA hoặc ElGamal và hàm băm SHA-256

- Ký và xác minh chữ ký số cho file văn bản sử dụng RSA/ElGamal và hàm băm SHA-256
- Sinh khóa (RSA hoặc ElGamal)
- Băm nội dung file văn bản bằng SHA-256
- Ký giá trị băm bằng khóa riêng
- Lưu chữ ký vào file
- Xác minh chữ ký bằng khóa công khai

Sử dụng thư viện gợi ý: OpenSSL, Crypto++ hoặc Botan.

Bài 2: Mô phỏng trao đổi khóa Diffie-Hellman giữa hai bên trong C++ (dùng thư viện)

Viết chương trình C++ mô phỏng quá trình trao đổi khóa Diffie-Hellman giữa hai bên (Alice và Bob), từ đó tạo ra một khóa bí mật chung.

Yêu cầu chức năng:

- Khởi tạo tham số chung: Một số nguyên tố lớn p và một phần tử sinh g. In ra p, g để kiểm tra.

- Tạo khóa riêng và công khai: Mỗi bên (Alice và Bob) sinh một khóa riêng (số ngẫu nhiên nhỏ hơn p)

- Tính khóa công khai tương ứng $A = g^a \bmod p$, $B = g^b \bmod p$

- Trao đổi và tính khóa chung: Alice nhận B từ Bob và tính $K = B^a \bmod p$. Bob nhận A từ Alice và tính $K = A^b \bmod p$. Kiểm tra xem hai khóa tính ra có giống nhau không.

Thư viện có thể sử dụng: OpenSSL, Crypto++ có hỗ trợ đầy đủ Diffie-Hellman trong dh.h hoặc dùng thư viện Botan.
