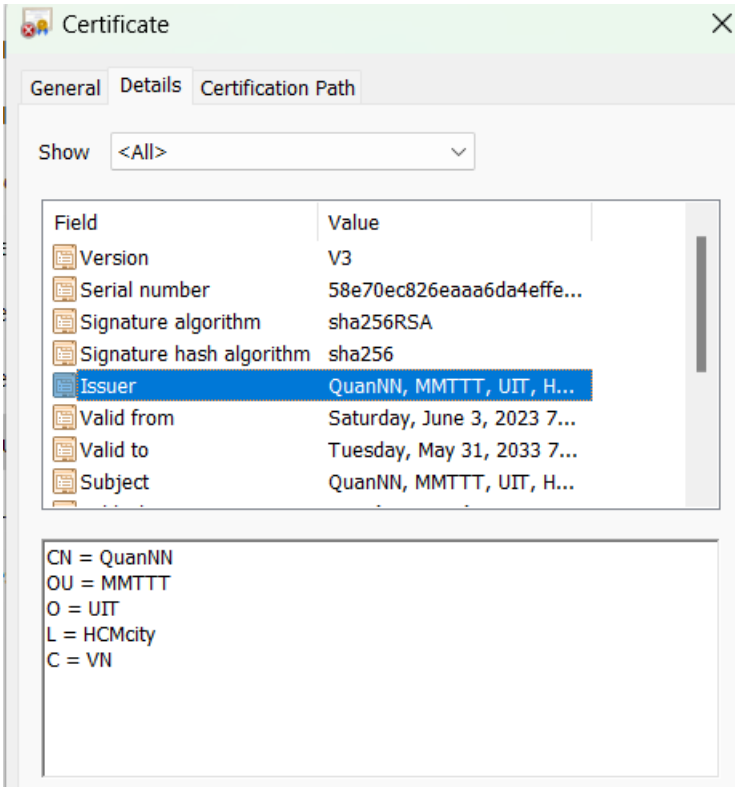
LẬP TRÌNH MẠNG CĂN BẢN

Sơ lược chương trình:

Server: tạo certificate bằng OpenSSL, gửi cert cho client.



certificate của server

Client: nhận cert -> verify cert. Tạo key đối xứng sử dụng thuật toán AES 256 mode CBC, rồi dùng public key của Server để mã hóa key đối xứng rồi gửi server.

Server: nhận được key đối xứng đang bị mã hóa, dùng private key của server để giải mã (thuật toán RSA 4096-bit).

Client: Sử dụng key đối xứng đã tạo để mã hóa thông điệp. Gửi thông điệp mã hóa đến server.

Server: Giải mã thông điệp từ client bằng key đối xứng đã giải mã để

Link demo: https://youtu.be/TQma8E5YbxQ