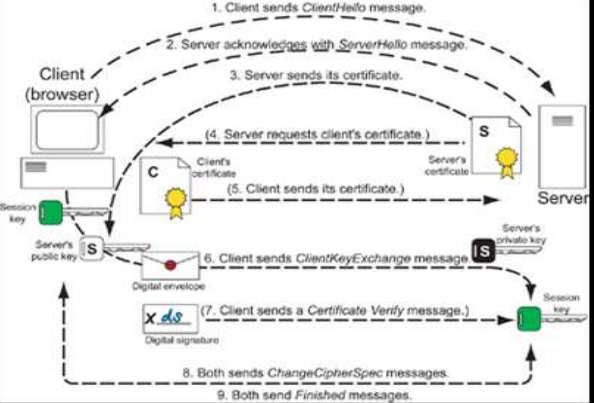
Bài tập: Mô tả quá trình thiết lập kết nối SSL



1. Client gửi gói tin Client/Hello yêu cầu kết nối
2. Server xác nhận với gói tin Server/Hello
3. Server gửi chứng chỉ số của nó
4. Server yêu cầu chứng chỉ số của Client
5. Client gửi chứng chỉ số của nó
6. Client tạo khoá xanh truy cập được một lần (khoá phiên), sử dụng để mã hoá thông điệp là khoá trao đổi. Sau khi mã hoá khoá xanh, thông điệp tiếp tục được mã hoá bởi khoá công khai của server tạo thành Digital envelope. Và client gửi Digital envelope cho server.

Server giải mã thông điệp bằng khoá bí mật của server và sau đó là khoá phiên (session key).

1. Client băm thông điệp Digital Envelope bằng hàm băm, sau đó mã hoá bằng khoá bí mật của Client tạo chữ kí số. Client gửi gói này cho server. Server sẽ mã hoá và so sánh với Digital envelope để xác minh tính toàn vẹn của gói tin.
2. Cả hai bên gửi gói ChangeCipherSpec cho nhau.
3. Cả hai bên gửi gói Finished cho nhau.