Câu 1: D. Between the Transport (TCP) layer and Applicatios layer

Câu 2: A. Digital Certificates

Câu 3: Trong mật mã an ninh mạng, man-in-the-middle attack là cuộc tấn công mà kẻ gian bí mật làm thay đổi thông tin, giao tiếp giữa các bên với nhau mà họ không biết mà vẫn tưởng là thông tin được đến đúng nơi cần đến.

Cách mà SSL chống lại phương thức tấn công man-in-the-middle attack: Client sử dụng CA (**certificate authority)** để xác minh chữ ký của server trước khi thiết lập một kết nối an toàn.

**Câu 4:**

Các bước thực hiện trong SSL Record Protocol:

-Chuẩn bị dữ liệu, cắt nhỏ dữ liệu từ lớp ứng dụng.( Breaking Down the Data from Application layers, with fixed length.)

-Nén dữ liệu(Compress the Data).

-Mã hóa gói thông tin (Encrypt the packets(which was broked down with fixed length).

-Thêm header cho từng thành phần dữ liệu. Mỗi tiêu đề gồm 2 thành phần:length of record and length of block added the original data.

(Add SSL header's in the packets with fixed length)

**Câu 5: Nguồn: https://discovery.csc.ncsu.edu/Courses/csc474-S05/hw/hw4-sol.pdf**

1. Brute-Force Cryptanalytic Attack:SSL sử dụng khóa đối xứng một lần (symmetric one-time session keys) và có khả năng thay đổi trong phiên làm việc.
2. SSL sử dụng các số ngẫu nhiên (của server và client) để tạo ra khóa phiên. Nó giúp tạo ra ngẫu nhiên các bản mã.
3. Các con số ngẫu nhiên sử dụng trong các phiên làm việc có 4 bytes đầu tiên là thời gian đóng dấu, vì vậy nó khác nhau trong mỗi phiên làm việc.
4. Xác thực lẫn nhau bằng chứng chỉ.
5. Password được mã hóa
6. SSL không sử dụng địa chỉ IP để kiểm định client và server.
7. Nếu kẻ tấn công tấn công các kết sau khi xác thực thì vẫn không biết các key mã hóa. Do đó, các phương thức phát hiện sẽ phát hiện nếu kẻ tấn công cố gắng gửi dữ liệu, phương thức này sẽ đóng kết nối. Đồng thời, kẻ tấn công trong quá trình bắt tay sẽ không biết được mật khẩu xác thực.
8. Không thể chống lại