Thời gian : 90 phút
Lớp INT3307 1

Được phép tra cứu tất cả các loại tài liệu
Không được cho người khác mượn tài liệu dưới bất kỳ hình thức nào

Đề thi số 1
An toàn và an ninh mạng

(3 câu, 2 trang, thang điểm 10)

1. Phân phối khóa (3 điểm)

a. (2 điểm)

Giao thức đã cho có những chức năng sau đây:

- Cho phép hai bên chia sẻ một khóa bí mật chung (0,25 điểm): Khóa được bảo mật bằng một giải thuật mật mã khóa công khai có khả năng mã hóa (chẳng hạn RSA) (0,25 điểm)
- Cho phép A xác thực B (0,25 điểm): Thông qua các thông báo số 1 và số 2 (0,25 điểm), vì chỉ B mới có PR_b tương ứng với PU_b đã được A sử dụng để mã hóa N_1 trong thông báo số 1 nên mới có thể tạo ra thông báo số 2 để A giải mã thành công lấy ra đúng N_1 ở thành phần thứ nhất (0,25 điểm)
- Cho phép B xác thực A (0,25 điểm): Thông qua các thông báo số 2 và số 3 (0,25 điểm), vì chỉ A mới có PR_a tương ứng với PU_a đã được B sử dụng để mã hóa N_2 trong thông báo số 2 nên mới có thể tạo ra thông báo số 3 để A giải mã thành công lấy ra đúng N_2 ở thành phần thứ hai (0,25 điểm)

Lưu ý : Trong ý thứ nhất nếu trả lời là khóa được bảo mật bằng một giải thuật mật mã khóa công khai có khả năng trao đổi khóa hoặc trả lời bằng giải thuật RSA cũng được tính điểm ; Trong ý thứ hai nếu trả lời chỉ thông qua thông báo số 1 thì được 0 điểm, nếu trả lời chỉ thông qua thông báo số 2 thì vẫn được 0,25 điểm ; Trong ý thứ ba nếu trả lời chỉ thông qua thông báo số 2 thì được 0 điểm, nếu trả lời chỉ thông qua thông báo số 3 thì vẫn được 0,25 điểm.

b. (1 điểm)

Nếu không có E(PR_a, K_s) thì địch thủ có thể chặn bắt thông báo số 4 mà A gửi cho B và tráo đổi thông báo E(PU_b, K_s) bằng E(PU_b, K'_s) trong đó K'_s là do địch thủ chọn (0,25 điểm) và như vậy khóa bí mật mà B có được lại được chia sẻ với địch thủ chứ không phải với A (0,25 điểm).

Nếu có E(PR_a, K_s) thì vì không biết PR_a, nên địch thủ không thể tạo ra một bản mã của một giá trị khóa chọn trước K'_s (0,25 điểm) để sau khi giải mã bằng PU_a tương ứng sẽ khiến B lấy đúng K'_s thu được làm khóa bí mật chung (0,25 điểm).

2. Chứng thực X.509 (3 điểm)

Chuỗi các chứng thực lẫn nhau là:

S<<Q>>Q<<P>>P<<W>>W<<V>>V<<X>>X<<B>> (1 điểm)

Lưu ý: Mỗi một trong các sai sót sau bị trừ 0,25 điểm: Viết không đúng định dạng chuỗi các chứng thực lẫn nhau (chẳng hạn có dấu phẩy giữa hai chứng thực liên tiếp, mỗi

chứng thực cố ý viết trên một dòng riêng,…); Thiếu Z<<B>>; Cơ quan chứng thực đứng đầu chuỗi không phải là S; Thiếu một chứng thực khóa công khai trong chuỗi,…
Cách thức A xác minh tính hợp lệ của khóa công khai của B trong chứng thực X<<B>>:
A có khóa công khai hợp lệ của S khi xin S cấp S<<A>>.
A sử dụng khóa công khai hợp lệ của S để xác minh S<<Q>>, nếu hợp lệ thì A có khóa công khai hợp lệ của Q.
A sử dụng khóa công khai hợp lệ của Q để xác minh Q<<P>>, nếu hợp lệ thì A có khóa công khai hợp lệ của P.
Cứ như vậy,…
A sử dụng khóa công khai hợp lệ của Z để xác minh X<<B>>, nếu hợp lệ thì A có khóa công khai hợp lệ của B. (2 điểm)

Lưu ý: Mỗi một trong các sai sót sau bị trừ 0,25 điểm: Nói "sử dụng khóa công khai" mà không nói chính xác là "sử dụng khóa công khai hợp lệ"; Viết thiếu điều kiện "nếu hợp lệ"; Viết thiếu câu mở đầu "Vì A có chứng thực…" (câu mở đầu cũng được coi là đúng không bị trừ điểm nếu viết là "A lấy khóa công khai hợp lệ trực tiếp từ S khi xin S cấp S<<A>>"); Chỉ viết câu "A sử dụng khóa công khai hợp lệ của S…" rồi đến luôn "Cứ như vậy" (vì không thể hiện được tính lặp lại trong giải thích),…

3. An ninh mức giao vận (4 điểm)

a. (1 điểm)

Vẽ đầy đủ tất cả các thông báo (không thiếu bất kỳ thông báo tùy chọn nào) (1 điểm)

Lưu ý : Mỗi thông báo bị thừa hay thiếu bị trừ 0,25 điểm, nhưng cho sinh viên 0,25 điểm thay vì 0 điểm nếu vẽ được cơ bản bộ khung của giao thức SSL Handshake. Tên gọi của các thông báo nếu sai về chính tả thì không bị trừ điểm, nhưng nếu sai về ngữ nghĩa thì cũng bị trừ 0,25 điểm.

b. (2 điểm)

Thông báo certificate ở giai đoạn 2 chứa chứng thực khóa công khai RSA có chức năng ký (hay DSS) của server (Có thể viết tắt là $CA\langle\langle S\rangle\rangle^{RSA,signatrue}$ hay $CA\langle\langle S\rangle\rangle_{RSA,signature}$ hay $CA\langle\langle S\rangle\rangle^{DSS}$) (0,25 điểm)

Thông báo server_key_exchange chứa khóa công khai RSA có chức năng mã hóa của server (0,25 điểm) được ký với khóa riêng RSA có chức năng ký của server (0,25 điểm) (Có thể viết tắt là $S\{PU_s^{RSA,encryption}\}^{RSA,signature}$)

Thông báo certificate_request bao gồm certificate_type và certificate_authorities trong đó certificate_type chỉ ra kiểu giải thuật mật mã khóa công khai là RSA và chế độ sử dụng là chữ ký số (cũng có thể viết là xác thực), không cần nói rõ về certificate_authorities (0,25 điểm)

Thông báo certificate ở giai đoạn 3 chứa chứng thực khóa công khai RSA có chức năng ký của client (Có thể viết tắt là $CA\langle\langle C\rangle\rangle^{RSA,signature}$ hay $CA\langle\langle C\rangle\rangle^{RSA}$) (0,25 điểm)

Thông báo client_key_exchange chứa khóa bí mật pre_master_secret được sinh ra bởi client (0,25 điểm) và được mã hóa với khóa công khai RSA có chức năng mã hóa của server (0,25 điểm) (Có thể viết tắt là $E(PU_s^{RSA,encryption}$, pre_master_secret))

Thông báo certificate_verify chứa chữ ký của client trên các thông báo client và server trước đó trao đổi với nhau sử dụng khóa riêng RSA có chức năng ký của client (0,25 điểm)

Lưu ý : Nếu sinh viên nói thông báo certificate_verify chứa cả master_secret như trong giao thức SSL thì không bị trừ điểm

c. (1 điểm)

Những khoảng thời gian nào sau đây có sự thay đổi trong bảng giá trị các thông số (1 điểm):

- Tại server sau khi nhận thông báo `client_hello` và trước khi nhận thông báo `change_cipher_spec` từ client
- Tại client sau khi nhận thông báo `server_hello` và trước khi gửi thông báo `change_cipher_spec`
- Tại server sau khi gửi thông báo `server_hello` và trước khi nhận thông báo `change_cipher_spec`
- Tại client sau khi gửi thông báo `change_cipher_spec` và trước khi gửi thông báo `finished` tới server
- Tại server sau khi nhận thông báo `change_cipher_spec` và trước khi nhận thông báo `finished` từ client
- Tại client sau khi nhận thông báo `change_cipher_spec` và trước khi nhận thông báo `finished` từ server
- Tại server sau khi gửi thông báo `change_cipher_spec` và trước khi gửi thông báo `finished` đến client

Lưu ý : Cứ mỗi hai thông báo đúng được 0,25 điểm ; Nếu lẻ một thông báo đúng thì được thêm 0,25 điểm ; Nếu thừa một thông báo sai thì bị trừ 0,25 điểm.