ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ
Thời gian : 90 phút
Lớp INT3307

Khoa Công nghệ Thông tin
Học kỳ II, Năm học 2022 - 2023
Được phép tra cứu tất cả các loại tài liệu
Không được cho người khác mượn tài liệu dưới bất kỳ hình thức nào

Lời giải Đề thi số 1
An toàn và an ninh mạng

(3 câu, 2 trang, thang điểm 10)

1. Kerberos (3 điểm)

(1) A-> C: N_A **0.25 điểm**

(1') C->B: N_A **0.5 điểm**

(2') B->C: CA<<B>>|| N_B || $Sig_B\{N_A \| N_B\}$ **0.5 điểm** **Time**

(2)C->A: CA<<C>> || N_B || $Sig_c\{N_A \| N_B\}$ **0.75 điểm**

(3) A->C: CA<<A>> || $Sig_A\{N_B \| N_A\}$ **0.5 điểm**

(3') C->B: CA<<A>> || $Sig_A\{N_B \| N_A\}$ **0.5 điểm**

Lưu ý:

- Giao thức thực hiện hai lần (giữa A với C và giữa B với C) chứ không phải C xen vào giữa kết nối giữa A và B sau đó sửa và chuyển tiếp các thông báo
- Cần viết đúng thứ tự và định dạng các thông báo

Bước (1'), bước (2) cần chỉ rõ các giá trị N_A, N_B lấy từ bước (1) và (2'), nếu ko sẽ bị trừ **0.25 điểm**

Bước (3') cần nói gửi lại thông báo số (3) hoặc thành phần $Sig_A\{N_B \| N_A\}$ được lấy từ bước (3) (C không thể tự tạo ra chữ ký do không biết khoá riêng của A) nếu không sẽ bị trừ **0.25 điểm**

2. Chứng thực X.509 (3 điểm)

X<<W>>W<<P>>P<<R>>R<<U>>U<<B>> (1.5 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 U<<B>>; Cơ quan chứng thực đứng đầu chuỗi không phải là X; 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 U<<B>>:
Vì A có chứng thực khóa công khai do X cấp nên A có khóa công khai hợp lệ của X.
A sử dụng khóa công khai hợp lệ của X để xác minh X<<W>>, nếu hợp lệ thì A có khóa công khai hợp lệ của W.

A sử dụng khóa công khai hợp lệ của W để xác minh W<<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 U để xác minh U<<B>>, nếu hợp lệ thì A có khóa công khai hợp lệ của B. (1.5 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 X khi xin X cấp X<<A>>"); Chỉ viết câu "A sử dụng khóa công khai hợp lệ của X…" rồi đến luôn "Cứ như vậy" (vì không thể hiện được tính lặp lại trong giải thích),…

3. An toàn mức giao vận (4 điểm)

a. (2 điểm)

Vẽ đầy đủ tất cả các thông báo trừ server_key_exchange (**2 điểm**)

Lưu ý : Mỗi thông báo bị thừa hay thiếu bị trừ 0,25 điểm, nhưng cho sinh viên 0,25 điểm nếu viết đủ bộ khung. 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 DH của server (Có thể viết tắt là CA<<S>>^{DH} hay CA<<S>>$_{DH}$) (**0,25 điểm**)

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 (**0.25 điểm**) và chế độ sử dụng là chữ ký số (**0.25 điểm**) (cũng có thể viết là xác thực), không cần nói rõ về certificate_authorities

Thông báo certificate ở giai đoạn 3 chứa chứng thực khóa công khai RSA của client (Có thể viết tắt là CA<<C>>^{RSA} hay CA<<C>>$_{RSA}$) (**0,25 điểm**)

Thông báo client_key_exchange chứa khóa công khai Diffie-Hellman của client và các tham số tổng thể (**0,25 điểm**) được ký với khóa riêng RSA của client (**0,25 điểm**) (Có thể viết tắt là C$\{PU_c^{DH} \| q \| \alpha\}^{RSA}$)

Thông báo certificate_verify chứa chữ ký của client trên các thông báo client và server trước đó trao đổi với nhau và master_secret (**0.25 điểm**) sử dụng khóa riêng RSA của client (**0,25 điểm**)

Lưu ý : Giải thuật RSA trong lời giải trên có thể thay thế bằng giải thuật DSS