ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

Khoa Công nghệ Thông tin
Học kỳ II, Năm học 2022 - 2023

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. Kerberos (3 điểm)

Xét giao thức xác thực sau đây:

(1) $A \rightarrow B : N_A$

(2) $B \rightarrow A : CA\langle\langle B\rangle\rangle \,||\, N_B \,||\, Sig_B\{N_A \,||\, N_B\}$

(3) $A \rightarrow B: CA\langle\langle A\rangle\rangle \,||\, Sig_A\{N_B \,||\, N_A\}$

Trong đó, N_A và N_B là những số ngẫu nhiên một lần được chọn bởi A và B, Sig_A và Sig_B là các chữ ký số của A và B một cách tương ứng, và $CA\langle\langle A\rangle\rangle$ và $CA\langle\langle B\rangle\rangle$ là các chứng thực khóa công khai của A và B do cơ quan chứng thực CA cấp.

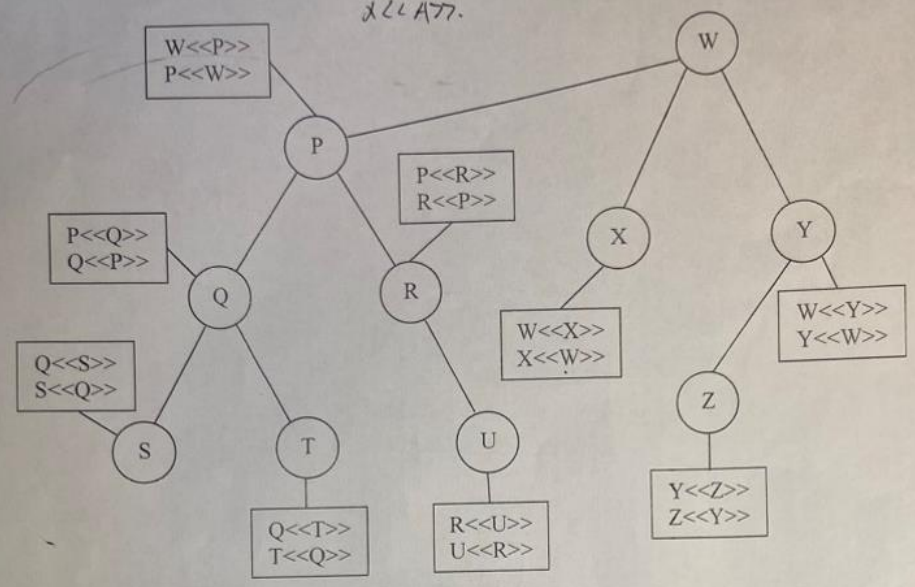
Hãy mô tả một tấn công vào giao thức đã nêu khiến cho một địch thủ C có thể tự xác thực (giả mạo) là A đối với B.

Gợi ý: Có thể tấn công với giả định A đã khởi tạo trước tiên một lần chạy giao thức với

2. Chứng thực X.509 (3 điểm)

Xét dịch vụ xác thực X.509. Cho một mô hình phân cấp các cơ quan chứng thực với các chứng thực lẫn nhau được mô tả như hình vẽ ở trang bên.

Một người dùng A có chứng thực do X cấp. Một người dùng B có chứng thực do U cấp. Hãy cho biết chuỗi các chứng thực lẫn nhau và cách thức cho phép A xác minh tính hợp lệ của khóa công khai của B trong chứng thực do U cấp.



3. An toàn mức giao vận (4 điểm)

Trong một ứng dụng Web, hai bên client và server sử dụng giao thức Handshake trong chuỗi giao thức TLS để xác thực lẫn nhau và thỏa thuận các tham số an ninh (các giải thuật và khóa mật mã). Phương pháp trao đổi khóa được hai bên thống nhất sử dụng là Diffie-Hellman.

a. (1,5 điểm)

Vẽ lược đồ của giao thức TLS Handshake giữa client và server theo cách thức an toàn nhất có thể nhưng chỉ server mới xác thực được client, còn client không xác thực được server.

b. (2,5 điểm)

Với mỗi thông báo tùy chọn (tức những thông báo không phải đối với bất kỳ phương pháp trao đổi khóa nào cũng được gửi) và thông báo *client_key_exchange* trong giao thức ở trên, hãy chỉ ra nó có những tham số cụ thể gì.