ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

Khoa Công nghệ Thông tin
Năm học 2020 - 2021

Thời gian : 120 phút
Lớp INT3307

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

(4 câu, 3 trang, thang điểm 10)

1. Hệ thống phân phối khóa và xác thực người dùng Kerberos (2,5 điểm)

Viết một hội thoại xác thực người dùng phân tán với cùng các mục tiêu và theo đúng trình tự 5 bước như hội thoại sau đây

- **Một lần mỗi phiên người dùng đăng nhập**

  (1) C → AS: $ID_c \parallel ID_{tgs}$

  (2) AS → C: $E(K_c, Thẻ_{tgs})$

- **Một lần với mỗi kiểu dịch vụ**

  (3) C → TGS: $ID_c \parallel ID_v \parallel Thẻ_{tgs}$

  (4) TGS → C: $Thẻ_v$

- **Một lần với mỗi phiên dịch vụ**

  (5) C → V: $ID_c \parallel Thẻ_v$

$Thẻ_{tgs} = E(K_{tgs}, [ID_c \parallel AD_c \parallel ID_{tgs} \parallel TS_1 \parallel Hạn_1])$

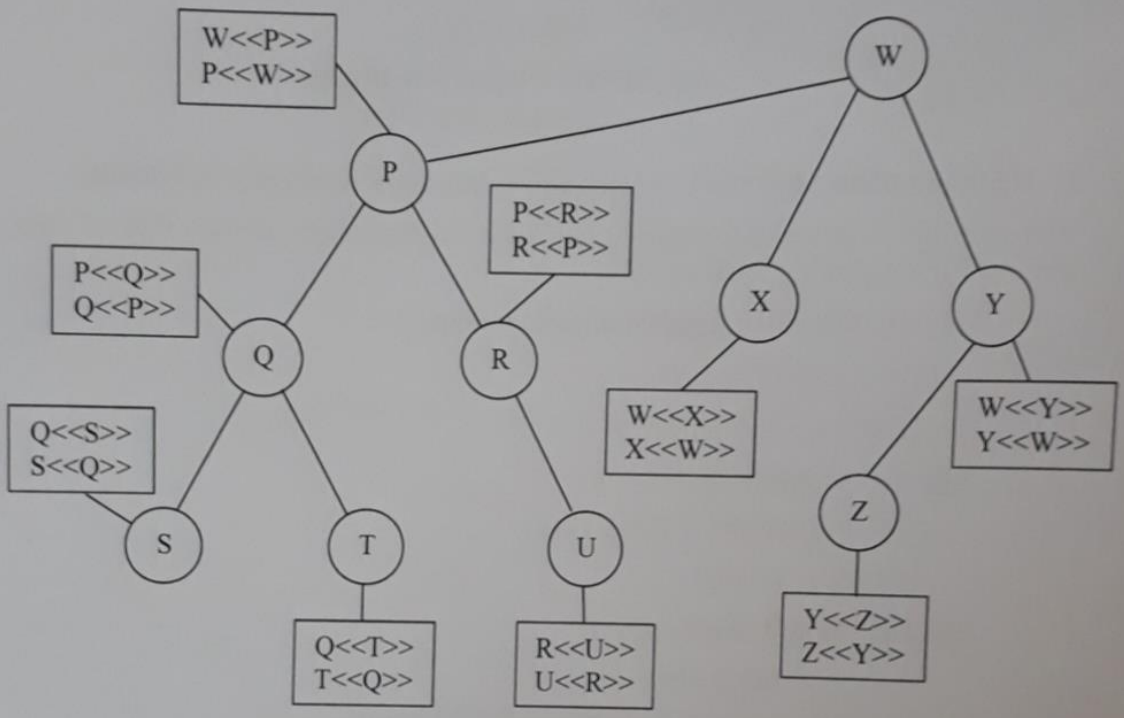
$Thẻ_v = E(K_v, [ID_c \parallel AD_c \parallel ID_v \parallel TS_2 \parallel Hạn_2])$

Tuy nhiên, phiên bản mới chỉ sử dụng mật mã khóa công khai, không sử dụng mã hóa đối xứng phải, tức là phải thỏa mãn các điều kiện sau:

- Server xác thực AS, server cấp thẻ TGS, mỗi người dùng ID_c và mỗi server dịch vụ V đều có một khóa công khai RSA vừa có chức năng ký vừa có chức năng mã hóa được chứng thực từ trước bởi một cơ quan chứng thực chung CA
- Ngay từ đầu AS đã có chứng thực khóa công khai CA<<ID_c>> của mỗi người dùng ID_c, AS đã có chứng thực khóa công khai CA<<TGS>> của TGS, TGS đã có các chứng thực khóa công khai CA<<AS>> của AS và CA<<V>> của mỗi server dịch vụ V, mỗi server dịch vụ V đều có chứng thực khóa công khai CA<<TGS>> của TGS
- Người dùng ID_C không có mật khẩu P_C được lưu giữ dưới dạng giá trị băm K_c trên server xác thực AS như trong hội thoại trên
- Server xác thực AS không có khóa bí mật chung K_{tgs} với server cấp thẻ TGS như trong hội thoại trên
- Server cấp thẻ TGS không có khóa bí mật chung K_v với mỗi server dịch vụ V như trong hội thoại trên

2. Chứng thực X.509 (2,5 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 dưới đây.



Một người dùng A có chứng thực do Q cấp. Một người dùng B có chứng thực do Y 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 Y cấp.

3. An toàn mức giao vận (2,5 điểm)

Trong một ứng dụng Web, hai bên client và server sử dụng giao thức Handshake trong chuỗi giao thức SSL để xác thực lẫn nhau và thỏa thuận các tham số an ninh (các giải thuật và khóa mật mã). Giả sử client và server đều có từ trước các cặp khóa riêng và khóa công khai theo giải thuật RSA. Các cặp khóa RSA chỉ có thể sử dụng cho chức năng ký, không phù hợp với chức năng mã hóa. Phương pháp trao đổi khóa được hai bên thống nhất sử dụng là RSA.

a. (1 điểm)

Vẽ sơ đồ trao đổi thông báo 4 giai đoạn giữa client và server trong giao thức SSL Handshake theo phương pháp trao đổi khóa đã cho sao cho cả hai bên client và server đều có thể xác thực lẫn nhau.

b. (1,5 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*, hãy chỉ ra nó có những tham số cụ thể gì.

4. An toàn thư điện tử (2,5 điểm)

ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

Khoa Công nghệ Thông tin
Năm học 2020 - 2021

Chương trình PGP của một người dùng A lưu giữ vòng khóa công khai có các trường **Public Key**, **User ID**, **Owner Trust**, và **Signatures** như sau:

Public Key	PU_A	PU_B	PU_C	PU_D	PU_E	PU_F	PU_G	PU_H	PU_I
User ID	A	B	C	D	E	F	G	H	I
Owner Trust	*Tột bậc*	*Hoàn toàn*	*Hoàn toàn*	*Hoàn toàn*	*Một phần*	*Một phần*	*Một phần*	*Không tin cậy*	*Không biết*
Signatures	-	A, K	E, F	E, J	B, F	A, B	D, E	C, D	D, H

Tính hợp lệ của khóa công khai (**Key Legitimacy**) được PGP tính theo các quy tắc sau:

- Khóa công khai của bản thân người dùng A là *hợp lệ*.
- Nếu một khóa công khai có ít nhất một chữ ký có độ tin cậy (**Signature Trust**) là *tột bậc* thì nó *hợp lệ*.
- Nếu không, tính hợp lệ của khóa công khai được tính bằng tổng trọng số độ tin cậy của các chữ ký. Trọng số 1 được gán cho các chữ ký có độ tin cậy *hoàn toàn*. Trọng số 1/2 được gán cho các chữ ký có độ tin cậy *một phần*. Nếu tổng trọng số đạt tới hoặc vượt ngưỡng là 1 thì khóa công khai được xác định là *hợp lệ*.
- Trong tất cả những trường hợp còn lại, khóa công khai được coi là *không hợp lệ*.

Vẽ mô hình tin cậy PGP tương ứng.