ÔN TẬP AN TOÀN THÔNG TIN

Cấu trúc đề thi cuối kỳ:
Câu 1 (3 điểm): (Câu 1 → 5)
Câu 2 (3 điểm): (Dạng câu 6,7) (Chữ ký điện tử RSA hoặc trao đổi khóa diffie-hellman)
Câu 3 (2 điểm): (Câu 8 → 13)
Câu 4 (2 điểm): (Câu 14 → 20)

Câu 1:
Trung tâm tin học của ngành công nghệ thông tin có nhiệm vụ đào tạo các khóa học ngắn hạn về CNTT cho các sinh viên của trường. Hiện nay trung tâm có một website http://www.ttth.vinhuni.edu.vn để sinh viên xem, đăng ký và thanh toán học phí các khóa học qua website. Sau khi thi xong sinh viên cũng có thể xem kết quả của các khóa học qua website này. Khi đăng ký học các khóa học sinh viên phải cung cấp đầy đủ thông tin cá nhân để trung tâm lưu trữ quản lý. Khi thanh toán học phí trực tuyến sinh viên phải cung cấp thông tin về thẻ ngân hàng thanh toán và được xác thực thông qua điện thoại. Thông tin các khóa học cũng được website cung cấp cho sinh viên tham khảo và chọn lựa. Giáo viên sau khi giảng dạy thì nhập các kết quả thi của sinh viên thông qua website bằng tài khoản người dùng trên website.

Hãy nêu và giải thích tính bí mật, tính sẵn sàng, tính toàn vẹn, tính chống chối bỏ của an toàn HTTT đối với website của trung tâm.

Câu 2:
Nhà ăn của trường Đại học Vinh có một Website ĐẶT THỰC ĐƠN CÁC MÓN ĂN TRỰC TUYẾN (http://www.cantin.vinhuni.edu.vn) nhằm giúp cho các nhân viên, giáo viên và sinh viên (gọi chung là khách hàng) của trường có thể tìm và đặt thực đơn các món ăn cho bữa ăn sáng/trưa/tối thông qua website và thức ăn sẽ được giao tới tận phòng/khoa của khách hàng mà khách hàng yêu cầu. Website có hiển thị danh mục và giá cả của các món ăn để khách hàng tham khảo. Để có thể đặt các món ăn, khách hàng phải đăng ký làm thành viên của Website. Để đăng ký thành viên thì khách hàng phải cung cấp thông tin cá nhân như họ tên, số điện thoại, địa chỉ email, mã số giáo viên/mã sinh viên để hệ thống lưu trữ và quản lý. Khi đặt món khách hàng có thể thanh toán đơn đặt hàng trực tuyến hoặc trả tiền mặt ngay khi nhận các món ăn. Khi thanh toán thực đơn trực tuyến khách hàng phải cung cấp thông tin về thẻ ngân hàng thanh toán và được xác thực thông qua điện thoại.

Hãy nêu và giải thích tính bí mật, tính sẵn sàng, tính toàn vẹn, tính chống chối bỏ của an toàn HTTT đối với website nhà ăn

Câu 3:
Đường sắt Việt Nam sử dụng website www.dsvn.vn để giúp hành khách đặt và mua vé trực tuyến. Thông qua website, các nhà ga quản lý được quá trình bán, mua vé của người dân cũng như thể hiện các tính ưu việt khác thông qua các nghiệp vụ điều hành. Website hiển thị các thông tin cần thiết mà khách hàng mong muốn: tuyến tàu, giá vé, thời gian chạy, thời gian đến, tình trạng số chỗ cho mỗi toa ... Để có thể đặt vé, hành khách truy cập vào website và tra cứu thông tin: chọn ngày đi, ga đi, ga đến, thời gian phù hợp, loại ghế ... cũng như bắt buộc phải cung cấp đúng thông tin cá nhân: họ tên người đi, thông tin giấy tờ tùy thân (số CMND hoặc thẻ căn cước, số hộ chiếu ...), năm sinh và một số thông tin bổ sung khác. Khách hàng cũng có thể thanh toán trực tuyến hoặc thanh toán tại các địa điểm chỉ định (ngân hàng, nhà ga, đại lý, các điểm thu hộ ...). Quản lý ga/nhân viên tùy theo chức năng, nhiệm vụ được giao thực hiện

các thao tác nghiệp vụ liên quan đến quy định đặt chỗ, bán vé, hủy vé, đổi ngày, cập nhật thông tin liên quan đến giá vé, giảm giá, các ưu đãi, khuyến cáo ... cũng thông qua cổng thông tin này.

Hãy nêu và giải thích tính bí mật, tính sẵn sàng, tính toàn vẹn, tính chống chối bỏ của an toàn HTTT đối với website Đường sắt Việt Nam.

Câu 4:

Ngân hàng Vietcombank là một ngân hàng chuyên cung cấp cho khách hàng đầy đủ các dịch vụ tài chính hàng đầu trong lĩnh vực thương mại quốc tế; trong các hoạt động truyền thống như kinh doanh vốn, huy động vốn, tín dụng, tài trợ dự án…cũng như mảng dịch vụ ngân hàng hiện đại: kinh doanh ngoại tệ và các công vụ phái sinh, dịch vụ thẻ, ngân hàng điện tử…

Sở hữu hạ tầng kỹ thuật ngân hàng hiện đại, Vietcombank có nhiều lợi thế trong việc ứng dụng công nghệ tiên tiến vào xử lý tự động các dịch vụ ngân hàng, phát triển các sản phẩm, dịch vụ ngân hàng điện tử dựa trên nền tảng công nghệ cao. Không gian giao dịch công nghệ số (Digital lab) cùng các dịch vụ: VCB Internet Banking, VCB Money, SMS Banking, Phone Banking,…đã, đang và sẽ tiếp tục thu hút đông đảo khách hàng bằng sự tiện lợi, nhanh chóng, an toàn, hiệu quả, tạo thói quen thanh toán không dùng tiền mặt cho đông đảo khách hàng.

Hãy nêu và giải thích tính bí mật, tính sẵn sàng, tính toàn vẹn, tính chống chối bỏ của an toàn HTTT đối với công ty/doanh nghiệp được mô tả ở trên.

Câu 5:

Bệnh viện Hồng Đức là một trong những bệnh viện tốt nhất tại Việt Nam. Hàng năm, Hồng Đức khám và điều trị cho hàng trăm ngàn bệnh nhân, hơn 5.000 bệnh nhân nội trú và phẫu thuật nội soi hơn 2.000 ca. Tính đến thời điểm hiện tại Hồng Đức đã đạt được nhiều thành tựu trong việc khám và điều trị bệnh cho bệnh nhân. Không ngừng nỗ lực để phục vụ cộng đồng tốt hơn và để đáp ứng nhu cầu của xã hội. Bệnh viện được trang bị đồng bộ với kỹ thuật và công nghệ y khoa hiện đại nhất, đáp ứng các yêu cầu chẩn đoán, điều trị theo phương pháp mới cũng như các kỹ thuật cao cấp. Đặc biệt bệnh viện đã áp dụng tối đa hệ thống thông tin vào tất cả các hoạt động của bệnh viện từ việc quản lý nhân viên, bệnh nhân, thiết bị đến việc xử lý các quy trình nghiệp vụ như đăng ký khám bệnh trực tuyến, khám bệnh và điều trị bệnh từ xa, điều trị bệnh, mổ, xét nghiệm, nội soi, thanh toán viện phí trực tuyến, liên kết với các công ty bảo hiểm trong việc điều trị cho các bệnh nhân có mua bảo hiểm…

Hãy nêu và giải thích tính bí mật, tính sẵn sàng, tính toàn vẹn, tính chống chối bỏ của an toàn HTTT đối với công ty/doanh nghiệp được mô tả ở trên

Câu 6:

Hãy trình bày quá trình tạo chữ ký số theo cơ chế RSA khi Alice muốn gửi thông điệp M đến Bob với giá trị băm của M là 15, p=23, q=11, e=19.

Câu 7:

Giả sử Alice và Bob thống nhất với nhau chọn số nguyên tố p = 11 và g = 7. Alice chọn một giá trị ngẫu nhiên bất kỳ x = 13 và bí mật x. Bob chọn một giá trị ngẫu nhiên bất kỳ y = 17 và bí mật y. Hãy trình bày quá trình tạo và trao đổi khóa phiên giữa Alice và Bob.

Câu 8:

+Trình bày thuật toán RSA. Cho biết ưu và nhược điểm của RSA

+ Nêu nguyên tắc của mã hóa khóa công khai? Tại sao trong mã hóa khóa công khai không cần dùng đến kênh an toàn để truyền khóa?

Câu 9:

Khóa là gì? Trong các hệ thống mã hóa, có các loại khóa nào? Hãy liệt kê tên (tiếng anh và tiếng việt), đặc điểm chính, đóng vai trò gì trong từng loại hệ thống mã hóa. Tại sao cần giữ bí mật khóa chỉ có người gửi và người nhận biết?

Câu 10:

Mã hóa bất đối xứng dùng 2 khóa khác nhau cho 2 quá trình mã hóa và giải mã.Trình bày (có giải thích) việc dùng phương pháp mã hóa bất đối xứng để giải quyết bài toán
a. Bảo mật dữ liệu.
b. Chứng thực nguồn gốc thông điệp
(chú ý trả lời ai là người tạo khóa)

Câu 11:

+ Hệ mã hóa đối xứng là gì? vẽ mô hình cơ bản và cho biết các thành phần cơ bản của mã hóa đối xứng? Trình bày ưu điểm và hạn chế của hệ mã đối xứng
+ Định nghĩa mã hóa đối xứng, vẽ mô hình cơ bản và cho biết các thành phần cơ bản của mã hóa đối xứng.

Câu 12:

Vẽ mô hình hệ mã hóa đối xứng và hệ mã hóa bất đối xứng? So sánh hệ mã đối xứng và hệ mã bất đối xứng

Câu 13:

Trong mã hóa khóa công khai, khóa riêng và khóa công khai có phải là 2 khóa tùy ý, không liên quan? Nếu có liên quan, tại sao không thể tính khóa riêng từ khóa công khai? Tại sao trong hệ mã RSA nếu biết khóa công khai (n,e) thì rất khó tìm khóa bí mật (n,d)

Câu 14:

Khóa phiên (Session Key) là gì? Khóa phiên khác khóa bí mật chia sẻ (secret key) như thế nào? (Vẽ mô hình KDC (Key Distribution Center))

Câu 15:

Thế nào là tấn công Man-in-the-middle. Nêu (vẽ mô hình) và giải thích một giao thức/cơ chế mà có thể bị tấn công này tấn công.

Câu 16:
Trình bày giao thức trao đổi khóa Diffie-Hellman. Nêu ưu điểm và nhược điểm của giao thức trao đổi khóa Diffie-Helman.

Câu 17:
Hàm băm là gì? Nêu và giải thích ứng dụng hàm băm trong việc lưu trữ mật khẩu (Vẽ mô hình).

Câu 18:
Hàm băm là gì? Nêu và giải thích ứng dụng hàm băm trong chữ ký điện tử (Vẽ mô hình).

Câu 19:
Hàm băm là gì? Trình bày và giải thích các tính chất của hàm băm?

Câu 20:
Chữ ký số là gì? Trình bày và giải thích quá trình tạo chữ ký số và thẩm tra chữ ký số