TRƯỜNG ĐẠI HỌC CÔNG NGHIỆP
THÀNH PHỐ HỒ CHÍ MINH

KHOA CÔNG NGHỆ THÔNG TIN

ĐỀ THI CUỐI KỲ

Môn thi : Nhập môn an toàn thông tin
Lớp/Lớp học phần: DHTH15
Ngày thi: 13/12/2021 – tiết 8-9
Thời gian làm bài: 60 phút
(Không kể thời gian phát đề)

Đề 501

Họ và tên thí sinh ……; MSSV: ……

Câu 1: LO4 *(3 điểm)*

a. Khóa phiên (Session Key) là gì? Nêu ứng dụng của khóa phiên.
b. Khóa phiên có ưu điểm gì so với khóa bí mật chia sẻ (secret key) như thế nào?
c. Trình bày và giải thích một giao thức phát sinh khóa phiên mà bạn biết.

Câu 2: LO3 *(3 điểm)*

Cho p = 17, *q* = 31, e = 7, sử dụng thuật toán chữ ký số RSA để thực hiện

a. Phát sinh cặp khóa công khai (PU) và khóa riêng phần (PR).
b. Tạo và thẩm tra chữ ký RSA trên thông điệp M=5

Câu 3: LO5 *(4 điểm)*

Trường Đại học Công Nghiệp Tp. HCM (IUH), vừa trang bị một phòng nghiên cứu dành cho các thành viên trong câu lạc bộ Nghiên cứu trẻ. Câu lạc bộ Nghiên cứu trẻ này trung bình khoảng 50 thành viên là các cán bộ, giảng viên và sinh viên của IUH. Phòng nghiên cứu này trang bị khoảng 50 chổ ngồi ngồi nghiên cứu, 30 bộ máy tính, một máy Server, hai máy in và một số thiết bị văn phòng khác. Máy server để hỗ trợ điều khiển cũng như chia sẽ tài nguyên cho các thành viên, các máy tính được cài đặt các phần mềm cần thiết để các thành viên sử dụng nghiên cứu. Trường mong muốn phòng nghiên cứu được cài đặt và cấu hình làm sao mà các thành viên có thể ra vào và sử dụng cái tài nguyên một cách thuận tiện nhưng vẫn có cơ chế theo dõi một cách tự động làm cơ sở để truy cứu khi cần thiết.

a. Theo bạn, phòng nghiên cứu trên nên dùng phương pháp nào (chữ ký số, xác thực và điều khiển truy cập bằng mật khẩu (fixed password, OTP), thẻ từ, camera, sinh trắc học (vân tay hoặc khuôn mặt, võng mạc,…)) mà các thành viên có thể vào ra một cách thuận tiện nhưng vẫn kiểm soát được khi cần thiết. Bạn hãy mô tả giải pháp một cách chi tiết nhất và nêu lý do tại sao đây là giải pháp hợp lý nhất.
b. Theo bạn, để có thể kiểm soát việc sử dụng thiết bị, ứng dụng được cài đặt trong phòng nghiên cứu chúng ta thể dùng phương pháp nào (chữ ký số, xác thực và điều khiển truy cập bằng mật khẩu (fixed password, OTP), thẻ từ, camera, sinh trắc học (vân tay hoặc khuôn mặt, võng mạc,…)). Bạn hãy mô tả một cách chi tiết nhất và nêu lý do tại sao đây là giải pháp hợp lý nhất?

---------- Hết ----------

(Sinh viên được tham khảo tài liệu)