ĐỀ CƯƠNG ÔN TẬP MÔN : AN TOÀN BẢO MẬT

Câu 1.

Anh/chị hãy so sánh đặc điểm của hệ mật mã khóa đối xứng với hệ mật mã khóa bất đối xứng?

Câu 2.

Anh/chị hãy giải thích tại sao cần phải đảm bảo an toàn cho thông tin và hệ thống thông tin?

Câu 3.

Anh/chị hãy giải thích các lớp phòng vệ điển hình trong mô hình đảm bảo an toàn hệ thống thông tin có chiều sâu Defence in Depth?

Câu 4.

Anh/chị hãy giải thích các thuộc tính an ninh an toàn của hệ thống thông tin theo mô hình CIA?

Câu 5.

Anh/chị hãy giải thích quan hệ giữa mối đe dọa và lỗ hổng trong hệ thống thông tin và liệt kê các mối đe dọa thường gặp?

Câu 6.

Anh/chị hãy giải thích quan hệ giữa mối đe dọa và lỗ hổng trong hệ thống thông tin và liệt kê các mối đe dọa thường gặp?

Câu 7.

Anh/chị hãy vẽ sơ đồ cấp và sử dụng chứng chỉ số, giải thích sơ đồ?

Câu 8.

Trong hệ mã hóa DES, anh/chị hãy vẽ sơ đồ thuật toán các bước sinh khóa phụ của hệ mã, giải thích sơ đồ?

Câu 9.

Anh/chị hãy so sánh 2 loại phần mềm độc hại: virus và worm?

Câu 10.

Anh/chị hãy trình bày về biện pháp điều khiển truy nhập DAC và cho ví dụ?

Câu 11.

Anh/chị hãy phân tích các kỹ thuật kiểm soát truy nhập trên tường lửa? Liệt kê các hạn chế của tường lửa?

Câu 12.

Anh/chị hãy vẽ sơ đồ quá trình tạo và kiểm tra chữ ký số, giải thích sơ đồ?

Câu 13.

Anh/chị hãy giải thích tấn công kiểu Social Engineering và nêu các cách phòng chống?

Câu 14,

Anh/chị hãy cho biết các thành phần và chức năng của hạ tầng quản lý khóa công khai PKI?

Câu 15.

Trong hệ mã hóa DES, anh/chị hãy vẽ sơ đồ thuật toán các bước xử lý chính của hệ mã, giải thích sơ đồ?

Câu 16.

Anh/chị hãy giải thích cơ chế phát hiện xâm nhập dựa trên chữ ký của hệ thống IDS/IPS?

Câu 17.

Anh/chị hãy giải thích cơ chế phát hiện xâm nhập dựa trên bất thường của hệ thống IDS/IPS?

Câu 18.

Anh/chị hãy giải thích tấn công giả mạo địa chỉ và nêu cách phòng chống?

Câu 19.

Anh/chị hãy trình bày về cơ chế điều khiển truy nhập MAC và cho ví dụ?

Câu 20.

Anh/chị hãy trình bày sơ đồ phân loại và cách phòng chống các phần mềm độc hại?

BÀI TẬP

Câu 1.

Trong hệ mã hóa RSA cho: p = 17, q = 23, e = 29.

a. Hãy tìm khóa công khai Kp, và khóa bí mật Ks của hệ mã trên?

b. Anh/chị hãy mã hóa bản rõ m =30 và nêu công thức giải mã?

Câu 2.

Trong hệ mã hóa RSA cho: p = 31, q = 47, e = 17.

a. Hãy tìm khóa công khai K_p và khóa bí mật K_s của hệ mã trên;

b. Có bản mã thu được c=1374. Anh/chị hãy giải mã tìm bản rõ ban đầu?

Câu 3.

Trong hệ mã hóa ElGamal cho:

p = 107; alpha = 2; a = 37; k=70

a. Tìm khóa công khai và khóa bí mật của hệ mã.

b. Anh/chị hãy mã hóa bản rõ m = 55 và nêu công thức giải mã.

Câu 4.

Trong hệ chữ ký số ELGAMAL

p = 103; alpha = 3; a = 37; k=29. Thông điệp x=50

a. Tìm khóa công khai và khóa bí mật?

b. Anh/chị hãy tính chữ ký số trên x và nêu công thức để kiểm tra chữ ký số.

Câu 5.

Trong hệ mã Vigenere, mã hóa xâu

P = "DAIHOCCONGNGHEGIAOTHONGVANTAI" người ta thu được bản mã là "KAVVWJCBBOUGUSOPABHPVNTJIUTNW".

Anh/chị hãy tìm khóa mã hóa đã dùng của hệ mã trên, sử dụng khóa tìm được mã hóa xâu "Information"?

Câu 6.

Cho hệ mã Hill có M=3 (khóa là ma trận vuông cấp 3) và bảng chữ cái là Tiếng Anh, cho khóa K là ma trận sau:

$$\begin{bmatrix} 3 & 2 & 6 \\ 5 & 4 & 8 \\ 7 & 1 & 2 \end{bmatrix}$$

Hãy mã hóa xâu P = "CHIENDICHBATDAUTUNGAYMAI"