Đề thi môn Nhập môn An toàn thông tin (60’)

Sinh viên nộp đề thi kèm bài tự luận. Cho phép sử dụng tài liệu

(Không sử dụng máy tính xách tay và các thiết bị di động cầm tay)

Chữ ký của người coi thi	Chữ ký của người chấm thi	Xác nhận của Bộ môn

Họ tên sinh viên: Mã số sinh viên: Lớp:

Phần 1. Các câu hỏi: lựa chọn những câu trả lời đúng.

1. Cơ sở của các hệ mật khoá công khai dựa trên
    a. Phép thế, hoán vị, hàm một chiều;
    b. Bài toán khó, hàm một chiều, thông tin cửa bẫy;
    c. Bài toán khó, hàm một chiều, hàm phi tuyến;
    d. Hàm một chiều, khả năng khó giả mạo, khoá khó đoán.
2. Kiến trúc An toàn thông tin OSI tập trung vào những vấn đề:
    a. Tấn công, cơ chế an toàn thông tin, dịch vụ an toàn thông tin;
    b. Tấn công, mật mã, dịch vụ bảo mật và xác thực, khả năng ngăn chặn tấn công;
    c. Cơ chế an toàn thông tin, dịch vụ an toàn thông tin, khả năng ngăn chặn tấn công.
3. Trong hệ mật khoá công khai, để bảo mật truyền dữ liệu gửi từ A đến B cần:
    a. Sử dụng khoá công khai của A;
    b. Sử dụng khoá công khai của B;
    c. Sử dụng khoá phiên do A tạo ra;
    d. Xin cấp phát khoá phiên từ bên thứ 3;
    e. Sử dụng khoá riêng được phân phối của B.
4. Làm thế nào để tăng tính an toàn của hệ mật không hoàn hảo
    a. Khoá có độ dài bằng độ dài bản tin rõ;
    b. Khoá sử dụng một lần;
    c. Bản tin mật được nén lại;
    d. Nén bản tin rõ;
    e. Giảm entropy của bản tin rõ.
5. Hệ mật RSA là:
    a. Phương pháp mật mã khối
    b. Sử dụng thay thế để làm tăng tính nhập nhằng;
    c. Sử dụng bài toán khó phân tích số;

d. Sử dụng khoá mật có độ dài 256 bit;
e. Sử dụng đường cong Elliptic.

6. Bên cấp phát chứng thư số bảo vệ danh sách CRL bằng:
   a. Bảo mật danh sách CRL;
   b. Chống giả mạo và sửa đổi danh sách bằng chữ ký số;
   c. Dùng cả hai phương pháp trên.
7. Những vấn đề an toàn hệ thống gồm:
   a. Tấn công, Mã mật đường truyền, Ghi nhật ký;
   b. Phát hiện tấn công, ngăn chặn tấn công, phát hiện và giảm thiểu điểm yếu hệ thống
   c. Cơ chế an toàn thông tin, dịch vụ an toàn thông tin, khả năng ngăn chặn tấn công.
8. Chế độ làm việc của hệ mật:
   a. Phân chia thông điệp thành các khối, cách thức liên kết các khối để thực hiện mã hóa, thường tổ chức khối thành các chuỗi;
   b. Các phương thức sinh khóa, lưu trữ khóa và phân phối khóa;
   c. Cơ chế mã hóa, giải mã, và quản trị khóa.
9. Sơ đồ Diffie-Helman là phương pháp:
   a. Mật mã bảo mật dữ liệu;
   b. Phân phối khóa phiên;
   c. Phương pháp đánh giá độ an toàn hệ mật.
10. Phân loại tấn công theo tác động vào hệ thống tính toán:
    a. Tấn công chủ động và tấn công thụ động;
    b. Tấn công mã độc, rò rỉ thông tin, ngăn chặn truy cập;
    c. Tấn công vào tính mật, tấn công xác thực.

Điền các lựa chọn vào bảng sau:

Câu	1	2	3	4	5	6	7	8	9	10
KQ										

Phần 2. Tự luận

1. Thuật toán RSA
   a. Thực hiện việc tạo khoá cho RSA với p = 11, q = 23.
   b. Một thông điệp gồm 20 ký tự ASCII. Để mã hóa với khóa tính được ở trên thì thông điệp phải chia thành khối như thế nào ?

2. Phân tích sơ đồ trao đổi khoá sau: A và B chia sẻ với nhau khoá phiên mới Ks_{AB}, Giữa A và B có khoá chính Km_{AB}.
   Sơ đồ trao đổi khoá:
   B1: A -> B: ID_A, N_A.

B2: B -> A: $E_{KmAB}[N_A, Ks_{AB}]$.
B3: A -> B: $E_{KsAB}[N_A]$.

- A và B có tin tưởng được rằng bên kia được chia sẻ khoá Ks_{AB} ? Vì sao ?
- Điều chỉnh sơ đồ để có thể tránh được tấn công người đứng giữa.