ĐỀ CƯƠNG ÔN TẬP KHÓA D22VT

MÔN: AN TOÀN MẠNG THÔNG TIN

I. Phần lý thuyết

1. An toàn mạng truyền thông: khái niệm, kiến trúc, dịch vụ an toàn, các cơ chế an toàn, mô hình an toàn mạng.
2. Các kiểu tấn công mạng: tấn công chủ động, tấn công tích cực. Các ví dụ minh họa.
3. Mô hình mật mã hóa khóa đối xứng
4. Mật mã khối: cấu trúc mật mã khối Feistel và các quá trình mã hóa, giải mã trong giải thuật mật mã khối Feistel
5. Tiêu chuẩn mật mã hóa dữ liệu DES: cấu trúc, các phép hoán vị, các vòng mật mã, thuật toán sinh khóa con, tính an toàn của DES.
6. Phương pháp mật mã hóa nhiều lần 2DES và 3DES: sơ đồ và phân tích tính an toàn.
7. Tiêu chuẩn mật mã hóa tiên tiến AES: cấu trúc, các hàm biến đổi, tạo khóa, thực hiện mật mã và giải mật mã.
8. Các chế độ và ứng dụng của mật mã khối.
9. Tạo số giả ngẫu nhiên và mật mã dòng.
10. Mật mã hóa khóa công khai: nguyên lý, ứng dụng và các yêu cầu đối với các hệ mật mã khóa công khai.
11. Giải thuật RSA: tạo khóa, mật mã, giải mật mã, tính an toàn của RSA.
12. Giải thuật trao đổi khóa Diffie-Hellman và phân tích tính an toàn của giải thuật.
13. Hệ thống mật mã hóa Elgamal.
14. Hàm băm: khái niệm, ứng dụng, các yêu cầu và độ an toàn của hàm băm.
15. Mã xác thực bản tin MAC: khái niệm, hoạt động và các giải thuật tạo mã xác thực HMAC và CMAC.
16. Quản lý và phân phối khóa: Các phương pháp phân phối khóa đối xứng và phân phối khóa công khai. Phân phối khóa công khai sử dụng chứng thư số, chứng thực khóa công khai sử dụng thẩm quyền chứng thư CA.
17. Chữ ký số: phương pháp tạo và xác minh chữ ký số. Chữ ký số sử dụng RSA và giải thuật chữ ký số DSA.
18. Chứng thư X509: khái niệm, cấu trúc chứng thư, khuôn dạng chứng thư. Mô hình hạ tầng khóa công khai PKI.
19. Xác thực người sử dụng: nguyên lý, các phương pháp xác thực người dùng.
20. Giao thức IPSec trong an toàn mạng Internet: khái niệm, hoạt động, giao thức AH và ESP, chế độ truyền tải và chế độ đường hầm.
21. Giao thức SSL/TLS: cấu trúc bản ghi SSL, các giai đoạn hoạt động của SSL, các cải tiến cơ bản của giao thức TLS so với SSL.
22. Giao thức PGP S/MIME cho an toàn thư điện tử.

II. Phần bài tập

+ Dạng 1: Bài tập RSA
+ Dạng 2: Tấn công RSA
+ Dạng 3: Chữ ký số sử dụng RSA
+ Dạng 4: Chứng chỉ X509

III. Định dạng đề thi

+ Hai câu lý thuyết
+ Hai câu bài tập