NỘI DUNG ÔN TẬP

MÔN HỌC: NHẬP MÔN ĐẢM BẢO VÀ AN NINH THÔNG TIN

BÀI 1: TỔNG QUAN

- Các kỹ thuật tấn công cơ bản
  - Eavesdropping
  - Cryptanalysis
  - Password Pilfering
  - Identity Spoofing
  - Intrusion
  - Denial of Service
- Lý lịch của những kẻ tấn công
  - Phân biệt các nhóm attacker khác nhau
  - Thứ tự thực hiện hành động của hacker
- Mô hình bảo mật cơ bản
  - Các thành phần của mô hình
  - Mô hình phòng thủ theo chiều sâu

BÀI 2: CÁC PHẦN MỀM GÂY HẠI

- Trojan
  - Phân biệt Trojan với các loại mã độc khác
  - Mục đích của Trojan
  - Các con đường để Trojan xâm nhập vào hệ thống
  - Phân loại
  - Biện pháp phòng chống
- Virus và Worm
  - Phân biệt Virus, Worm và các loại mã độc khác
  - Các tính chất chính của Virus máy tính
  - Phân loại
  - Các công cụ tạo Virus và Worm
  - Phân biệt các kỹ thuật cơ bản của Virus
  - Biện pháp phòng chống

BÀI 3: CÁC GIẢI THUẬT MÃ HOÁ DỮ LIỆU

- Phân loại các giải thuật mã hoá dữ liệu
- Các giải thuật mã hoá cổ điển (lý thuyết, bài tập):
  - Mã thay thế đơn giản
  - Mã dịch chuyển
  - Mã PlayFair

- Các giải thuật mã hoá hiện đại
    - Phân loại
    - Đặc điểm chính của giải thuật DES
    - Đặc điểm chính của giải thuật AES

BÀI 4: MÃ HOÁ KHOÁ CÔNG KHAI

- Đặc điểm chính của giải thuật mã hoá khoá công khai
- Giao thức trao đổi khoá Diffie-Hellman
- Giải thuật mã hoá RSA (giải thuật tạo cặp khoá, mã hoá và giải mã)

BÀI 5: CHỨNG THỰC DỮ LIỆU

- Mã chứng thực thông điệp (MAC)
    - Khái niệm
    - Các công dụng cơ bản
- Hàm băm
    - Khái niệm
    - Các công dụng cơ bản
    - Các hàm băm thông dụng: MD5, SHA
- Chữ ký số
    - Khái niệm
    - Tạo và kiểm tra chữ ký số

BÀI 6: MỘT SỐ GIAO THỨC BẢO MẬT MẠNG

- IPSec
    - Đặc điểm, ứng dụng
    - Các phương thức
- SSL/TLS
    - Ứng dụng, thành phần, cấu trúc, các giao thức
    - Thiết lập kết nối SSL
- PGP: Khái niệm và các chức năng chính
- Kerberos: Cấu trúc, cơ chế hoạt động và ứng dụng