TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI
KHOA CÔNG NGHỆ THÔNG TIN
BỘ MÔN KHOA HỌC MÁY TÍNH
TRẦN VĂN DŨNG
****

BÀI GIẢNG

AN TOÀN VÀ BẢO MẬT THÔNG TIN

SỐ TÍN CHỈ: 3

HÀ NỘI - 2012

Mở đầu

Gần đây, môn học "An toàn và bảo mật thông tin" đã được đưa vào giảng dạy tại hầu hết các Khoa Công nghệ Thông tin của các trường đại học và cao đẳng. Do các ứng dụng trên mạng Internet ngày các phát triển và mở rộng, nên an toàn thông tin trên mạng đã trở thành nhu cầu bắt buộc cho mọi hệ thống ứng dụng. Để đáp ứng yêu cầu học tập và tự tìm hiểu của sinh viên các chuyên ngành Công nghệ Thông tin, Bộ môn Khoa học máy tính, Khoa Công nghệ Thông tin, trường đại học Giao thông đã tổ chức biên soạn bài giảng này. Nội dung của nó được dựa trên một số tài liệu, nhưng chủ yếu là hai cuốn sách của Giáo sư William Stallings "Cryptography and Network Security: Principles and Practice" và "Network Security Essentials". Cuốn sách trên đã được dùng làm tài liệu giảng dạy tại nhiều trường đại học. Đồng thời giáo trình này cũng được hoàn thiện từng bước dựa trên bài giảng của tác giả cho 10 khóa sinh viên Khoa Công nghệ Thông tin vừa qua. Với mục đích trang bị các kiến thức cơ sở vừa đủ và giúp cho sinh viên hiểu được bản chất của các khía cạnh an ninh trên mạng, trong giáo trình tác giả đã cố gắng trình bày tóm tắt các phần lý thuyết cơ bản và đưa ra các ứng dụng thực tế.

Giáo trình gồm 8 chương. Chương đầu nêu tổng quan về bảo mật; chương 2 tóm tắt sơ lược về mã cổ điển; chương 3 trình bày những khái niệm cơ bản về trường số học; chương 4 giới thiệu về mã khối và chuẩn mã dữ liệu DES và chuẩn mã nâng cao AES; chương 5 nêu về mã công khai, RSA và chữ ký điện tử DDS; chương 6 đưa ra các ứng dụng xác thực bao gồm việc quản lý khóa, hệ thống xác thực Kerberos, hạ tầng khóa công khai PKI, an toàn thư điện tử và chuẩn xác thực X509; chương 7 giới thiệu một số ứng dụng an ninh mạng như an toàn IP, Web, thanh toán điện tử an toàn và giao thức quản trị mạng SNMP; cuối cùng chương 8 tóm tắt về kẻ xâm nhập, quản trị mật khẩu, biện pháp phòng chống của bức tường lửa và các hệ thống tin cậy.

Do lần đầu biên soạn và chưa có nhiều kinh nghiệm thực tế, nên không tránh khỏi những sai sót và lỗi in ấn nhất định. Tác giả xin vui lòng tiếp nhận mọi sự đóng góp giúp cho giáo trình "An toàn và bảo mật thông tin" ngày càng tốt hơn. Mọi ý kiến xây dựng xin gửi về theo địa chỉ sau: Trần Văn Dũng, Khoa Công nghệ Thông tin, Đại học Giao thông Vận tải, Láng Thượng, Đống đa, Hà nội.

Trần Văn Dũng

MỤC LỤC