

# AN TOÀN & BẢO MẬT THÔNG TIN

Giảng viên: Ths Phạm Thanh Bình  
Bộ môn Kỹ thuật máy tính & mạng  
*<http://dhthuyloi.blogspot.com>*

# Nội dung:

- ◆ Giới thiệu chung
- ◆ Mật mã đối xứng
- ◆ Mật mã khoá công khai và ứng dụng
- ◆ Các ứng dụng trong an ninh mạng
- ◆ An ninh hệ thống

# Chương 1:

## *GIỚI THIỆU CHUNG*

- ◆ Các mối đe dọa
- ◆ Những kẻ xâm nhập
- ◆ Mất mát dữ liệu do sự cố

# Bài 1.1 – Các mối đe dọa

Mục tiêu	Mối đe dọa
Sự bí mật của dữ liệu	Lộ bí mật
Sự toàn vẹn của dữ liệu	Sai lệch, mất mát dữ liệu
Sự sẵn sàng của hệ thống	Từ chối dịch vụ

# Sự bí mật của dữ liệu

- ◆ Dữ liệu thường chỉ phục vụ cho một số người cụ thể.
- ◆ Những người không đủ thẩm quyền sẽ không được phép truy nhập vào dữ liệu, không thể đọc được dữ liệu.

# Sự toàn vẹn của dữ liệu

- ◆ Những người dùng không đủ thẩm quyền sẽ không thể sửa đổi được dữ liệu
- ◆ Sửa đổi dữ liệu không chỉ là thay đổi hay xoá nội dung của dữ liệu, mà còn là sự di chuyển dữ liệu và thêm vào các dữ liệu giả

# Sự sẵn sàng của hệ thống

- ◆ Hệ thống luôn sẵn sàng hoạt động, không ai ngoài admin có thể làm cho hệ thống ngừng hoạt động
- ◆ DoS (Denial of Service - Từ chối dịch vụ) là hình thức tấn công nhằm đe dọa sự sẵn sàng của hệ thống



# Bài 1.2 – Những kẻ xâm nhập

- ◆ Khi thiết kế một hệ thống để chống lại những kẻ xâm nhập, điều quan trọng là phải hiểu được loại đối thủ mà ta muốn chống
- ◆ Công sức bỏ ra để thực hiện bảo mật phụ thuộc vào đối tượng xâm nhập



# Một số đối tượng xâm nhập

- ◆ Những người dùng tò mò, không có chuyên môn thích đọc trộm dữ liệu
- ◆ Các chuyên gia kỹ thuật muốn thử thách bản thân (sinh viên, lập trình viên hệ thống, người vận hành...)
- ◆ Những kẻ tấn công vì tiền như nhân viên hoặc lập trình viên của ngân hàng
- ◆ Gián điệp do thám thông tin thương mại hoặc quân sự
- ◆ *Virus máy tính*

# Bài 1.3 – Mất dữ liệu do sự cố

- ◆ Tai nạn ngẫu nhiên: hoả hoạn, lũ lụt, động đất, chiến tranh, bạo loạn...
- ◆ Phần cứng hoặc phần mềm bị lỗi
- ◆ Lỗi do con người: Entry dữ liệu không chính xác, lắp nhầm băng hoặc đĩa, chạy nhầm chương trình, mất đĩa hoặc băng...



*Cần có một giải pháp tổng thể (gồm cả chiến lược và kỹ thuật) để đảm bảo an toàn của hệ thống*

# *Hết Phần 1*