

AN TOÀN BẢO MẬT THÔNG TIN (Giới thiệu)

Phạm Nguyên Khang
BM. Khoa học máy tính

pnkhang@cit.ctu.edu.vn

CẦN THƠ, 8 - 2012

Giới thiệu

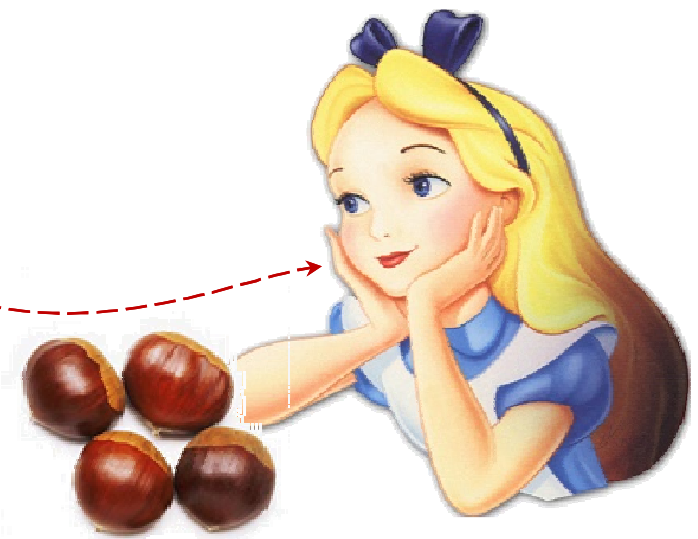
- Tại sao phải học AT & BMTT ?
- Mục tiêu
- Nội dung
- Phân phối chương trình
- Phương pháp giảng dạy
- Đánh giá
- Tài liệu tham khảo

Tình huống 1

**Mình đã biết hết
những gì bọn
chúng trao đổi
với nhau.**



Tình huống 2



Tình huống 3

- Tôi là nhà quản trị
- Cho người dùng **A** được phép đọc file M



- Tôi là nhà quản trị
- Cho phép người dùng **H** được phép đọc file M



Tình huống 4



Mua cho tôi
1000 cổ phiếu
của công ty ABC



Tôi đâu có nhờ
anh mua cổ
phiếu cho tôi.

Cô chuyển tiền
cho tôi đi chứ !



Tại sao phải học AT&BMTT ?

Thưa chuyên gia,
làm thế nào để giải
quyết các vấn đề trên ?

Các vấn đề anh vừa
nêu có thể tóm gọn
trong 4 từ.

Là 4 từ gì ạ ?

Muốn biết đó là các từ
gì, tôi khuyên anh nên
đi học môn **Bảo mật
thông tin**. Khà khà ...



Mục tiêu môn học

- Biết
 - Các khái niệm cơ bản về bảo mật thông tin
- Hiểu và vận dụng:
 - Mật mã và ứng dụng của nó trong AT&BMTT
 - Các hệ mật mã
 - Các giải thuật được sử dụng
 - Chữ ký điện tử
- Chứng thực người dùng và trao đổi khóa

Nội dung

- Giới thiệu Bảo mật thông tin
- Mật mã cổ điển
- Mật mã đối xứng (bí mật)
- Mật mã bất đối xứng (công khai)
- Giải thuật băm
- Chữ ký điện tử
- Chứng thực
- Phương pháp trao đổi khóa

Phân phối thời gian học (dự kiến)

- Lý thuyết: 16 giờ
 - Tuần 1 – tuần 7: lý thuyết (2tiết/tuần)
 - Tuần 13: ôn tập lý thuyết (2tiết)
- Thực hành: 25 giờ (5 buổi)
 - Tuần 9 – Tuần 12: (5 tiết/tuần)
- Tuần 15: thi kết thúc học phần

Phương pháp giảng dạy

- Lý thuyết:
 - Thuyết trình + Minh họa bằng chương trình máy tính
 - Đặt vấn đề + thảo luận
 - Làm bài tập nhóm
- Thực hành:
 - Bài thực hành có lời giải (ví dụ)
 - Bài thực hành có hướng dẫn (bắt buộc)
 - Bài thực hành nâng cao (điểm thưởng)

Đánh giá

- Bài tập nhóm trên lớp (20%)
- Thực hành (30%)
- Thi kết thúc học phần (50%)

- Thưởng/phạt (10%)
 - Các bài tập trên lớp
 - Các bài tập được giao về nhà
 - Các bài kiểm tra đột xuất

Tài liệu tham khảo

- Phạm Nguyễn Khang, *Bài giảng An toàn và Bảo mật thông tin*, Khoa CNTT&TT, ĐHCT
- William Stallings, *Cryptography and Network security: Principles and Practice*, Prentice Hall, 2006, 680 pages
 - <http://williamstallings.com/Crypto/Crypto4e.html>
- Introduction to Cryptography
 - <http://williamstallings.com/Crypt-Tut/Crypto%20Tutorial%20-%20JERIC.html>
- Security cartoon
 - <http://securitycartoon.com/>

Công cụ hỗ trợ thực hành

- Java (JDK)
 - <http://www.oracle.com/technetwork/java/javase/downloads/index.html>
- Môi trường phát triển tích hợp
 - Eclipse IDE for Java EE Developers
 - Hoặc Netbean
- Java™ Cryptography Architecture API Specification & Reference
 - <http://java.sun.com/j2se/1.4.2/docs/guide/security/CryptoSpec.html>