

CƠ SỞ LÝ THUYẾT MẬT MÃ (Giới thiệu)

Đỗ Thanh Nghị
Khoa Mạng máy tính & TT

dtngghi@cit.ctu.edu.vn

CẦN THƠ, 8 - 2024

Giới thiệu

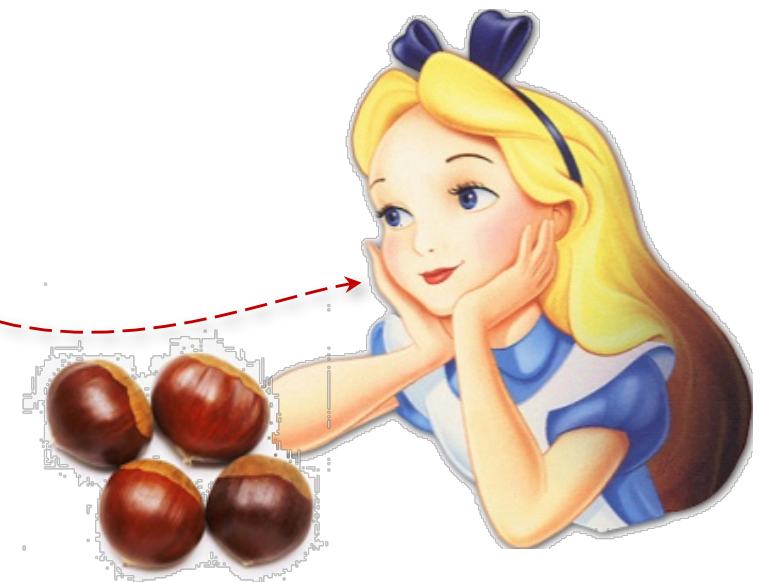
- Tại sao phải học lý thuyết mật mã?
- Mục tiêu
- Nội dung
- Tổ chức lớp học
- Phương pháp giảng dạy
- Đánh giá
- Tài liệu tham khảo

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 lý thuyết mật mã?

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

Các vấn đề anh vừa
nêu liên quan đến kiến
thức của môn học!

Là môn học gì ạ?

Tôi khuyên anh nên đi
học môn **Cơ sở lý
thuyết mật mã**. ☺ ...



Mục tiêu môn học

- Biết
 - Cơ sở lý thuyết mật mã
 - Thuật toán mật mã khoá bí mật, mật mã khoá công khai, hàm băm
- Hiểu và vận dụng:
 - Mật mã và ứng dụng
 - 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

Tổ chức lớp học

- Lý thuyết: 30t (sinh viên không sử dụng điện thoại trong giờ học)
- Thực hành: 30t (tính điểm từng buổi)
- Ngôn ngữ lập trình: Python/Java
- Điểm thực hành: 30%
- Thi cuối kỳ: 70%, tự luận

Tài liệu tham khảo

- Phạm Nguyên Khang, *Bài giảng An toàn và Bảo mật thông tin*, Trường CNTT&TT, ĐHCT
- William Stallings, *Cryptography and Network security: Principles and Practice*, Prentice Hall, 2006, 680 pages
 - <http://williamstallings.com/Crypto/Crypto4e.html>
- Phan Đình Diệu, *Lý thuyết mật mã và an toàn thông tin*, NXB Đại học Quốc gia Hà nội, 2002.