

CHƯƠNG TRÌNH TRÌNH ĐỘ ĐẠI HỌC/CAO ĐẲNG/LIÊN THÔNG
NGÀNH ĐÀO TẠO: TIN HỌC

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN
An toàn thông tin (Information Security)

I. Thông tin về học phần

- Mã học phần: TH03031
- Số tín chỉ: 2TC (2,0 – 0 – 4)
- Giờ tín chỉ đối với các hoạt động học tập: 30 tiết
 - + Nghe giảng lý thuyết trên lớp: 20 tiết
 - + Làm bài tập trên lớp: 10 tiết
 - + Thảo luận trên lớp: 0
 - + Thực hành trong phòng thí nghiệm: 0
 - + Thực tập thực tế ngoài trường: 0
 - + Tự học: 60 tiết
- Đơn vị phụ trách học phần:
 - Bộ môn: Khoa học máy tính
 - Khoa: Công nghệ thông tin
- Là học phần: bắt buộc
- Học phần học trước: Mạng máy tính và lập trình mạng

II. Thông tin về đội ngũ giảng viên:

- Họ và tên: Nguyễn Văn Hoàng
- Chức danh, học hàm, học vị: Thạc sĩ
- Địa chỉ liên hệ: Bộ môn Khoa học máy tính
- Điện thoại, email: 04.62617523, nvhoang@hua.edu.vn
- Thông tin về trợ giảng (nếu có) (họ tên, địa chỉ liên hệ, điện thoại, email):

III. Mục tiêu học phần:

- Về kiến thức: Kiến thức nền tảng trong an toàn thông tin
- Về kỹ năng: Rèn luyện tư duy trừu tượng hóa, phân tích và giải quyết vấn đề; kỹ năng đọc tài liệu và kỹ năng lập trình
- Về các mục tiêu khác (thái độ học tập):

IV. Mô tả nội dung vắn tắt của học phần:

TH03031. An toàn thông tin (Information security). (2TC: 2 - 0 - 4). Học phần giới thiệu các vấn đề cơ bản trong lĩnh vực an toàn thông tin cũng như các giải pháp cho các vấn đề đó. Học

phần tập chung vào các vấn đề như tính bí mật, tính toàn vẹn và tính tin cậy. *Học phần học trước: Mạng máy tính và lập trình mạng*

V. Nhiệm vụ của sinh viên:

- Dự lớp: 2 tín chỉ
- Bài tập: 1 tín chỉ
- Dụng cụ học tập

VI. Tài liệu học tập:

- Giáo trình/bài giảng

Bài giảng: Giảng viên soạn

Giáo trình: William Stallings: Cryptography and Network security principles and practices, 4th edition

- Các tài liệu khác:

Menezes, Alfred J., Paul C. van Oorschot, and Scott A. Vanstone: Handbook of Applied Cryptography. CRC Press, October, 1996.

Schneier, Bruce: Applied Cryptography. 2nd ed. New York, NY: John Wiley & Sons, 1996.

VII. Tiêu chuẩn đánh giá sinh viên:

Đánh giá theo quy định chung của Trường

VIII. Nội dung chi tiết học phần: (ghi tên chương, mục, tiểu mục)

Chương 1. Mở đầu

- 1.1. Thông tin là gì?
- 1.2. Dữ liệu là gì?
- 1.3. Quan hệ giữa dữ liệu và thông tin
- 1.4. Vị trí của an toàn thông tin
- 1.5. Các bài toán chính trong an toàn thông tin

Chương 2. Nghệ thuật giấu thư

- 2.1. Giới thiệu một số phương pháp giấu thư cổ điển
- 2.2. Các phương pháp giấu thư hiện đại
- 2.3. Nguyên lý của nghệ thuật giấu thư và steganalysis
- 2.4. Lý thuyết về Cover Models
- 2.5. Tóm tắt

Chương 3. Giới thiệu về các mật mã cổ điển

- 3.1. Một số mã chuyển vị
- 3.2. Một số mã thế
- 3.3. Mã hóa 1 bảng mã và nhiều bảng mã
- 3.4. Khoa học mật mã và Khoa học thám mã
- 3.5. Tóm tắt

Chương 4. Mật mã có đối xứng hiện đại

- 4.1. Tổng quan mã khối

- 4.2. Tiếp cận của Horst Feistel
- 4.3. DES và AES
- 4.4. Tổng quan về mã dòng
- 4.5. Mã RC4
- 4.6. Các chế độ vận hành của mã khối
- 4.7. Tóm tắt

Chương 5. Mật mã không đối xứng

- 5.1. Bài toán trao đổi khóa
- 5.2. Lược đồ trao đổi khóa Diffie-Hellman
- 5.3. Lược đồ mã hóa khóa công khai
- 5.4. Giới thiệu một số mật mã khóa công khai
- 5.5. Tóm tắt

Chương 6. Đảm bảo tính toàn vẹn

- 6.1. Tổng quan về đảm bảo tính toàn vẹn
- 6.2. Hàm băm mật mã
- 6.3. Phương pháp Merkle-Damgard trong xây dựng hàm băm mật mã
- 6.4. Mã xác thực thông điệp (MAC)
- 6.5. Phương pháp Hash-then-Authenticate trong xây dựng MAC
- 6.6. Giới thiệu một số hàm MAC
- 6.7. Tóm tắt

Chương 7. Đảm bảo tính tin cậy

- 7.1. Tổng quan về tính tin cậy
- 7.2. Chữ ký số, chứng chỉ số và cơ quan cấp và xác thực chứng chỉ số
- 7.3. Một số lược đồ chữ ký số
- 7.4. Hạ tầng khóa công khai (PKI)
- 7.5. Tóm tắt

Chương 8. Tóm tắt

IX. Hình thức tổ chức dạy học:

Lịch trình chung: (ghi tổng số giờ tín chỉ cho mỗi cột)

Nội dung	Hình thức tổ chức dạy học học phần					Tổng
	Lên lớp			Thực hành, thí nghiệm, điền dã	Tự học, tự nghiên cứu	
	Lý thuyết	Bài tập	Thảo luận			
Chương 1	3	0	0	0		3
Chương 2	3	0	0	0		3
Chương 3	3	0	0	0		3
Chương 4	6	0	0	0		6

Chương 5	3	0	0	0		3
Chương 6	3	0	0	0		3
Chương 7	3	0	0	0		3
Bài tập	3	0	0	0		3
Chương 8	3	0	0	0		3
Tổng	30	0	0	0		30

X. Yêu cầu của giảng viên đối với học phần:

- Yêu cầu của giảng viên về điều kiện để tổ chức giảng dạy học phần như: giảng đường có máy chiếu, không quá rộng, số lượng sinh viên không quá đông (<40)
- Yêu cầu của giảng viên đối với sinh viên như: sinh viên dự lớp đầy đủ, nghiên cứu tài liệu, giáo trình trước khi lên lớp.

Trưởng bộ môn
(Ký và ghi rõ họ tên)

Phụ trách học phần
(Ký và ghi rõ họ tên)

Trưởng khoa
(Ký và ghi rõ họ tên)

Duyệt của Trường
(Ký và ghi rõ họ tên)