TRƯỜNG ĐẠI HỌC NHA TRANG
Khoa: Công nghệ Thông tin
Bộ môn: Hệ thống Thông tin

CỘNG HOÀ XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

CHƯƠNG TRÌNH HỌC PHẦN

1. Thông tin chung về học phần

Tên học phần: An toàn bảo mật hệ thống thông tin.
Mã học phần:
Số tín chỉ: 3
Học phần tiên quyết: Kỹ thuật lập trình, Hệ quản trị Cơ sở dữ liệu, Mạng máy tính
Đào tạo trình độ: Đại học
Giảng dạy cho các ngành: Công nghệ Thông tin
Bộ môn quản lý: Bộ môn Hệ thống Thông tin
Phân bổ thời gian trong học phần:

- Nghe giảng lý thuyết: 30 tiết
- Làm bài tập trên lớp: 10 tiết
- Thảo luận: 5 tiết
- Thực hành, thực tập: 0 tiết
- Tự nghiên cứu: 90 tiết

2. Mô tả tóm tắt học phần

Học phần trang bị cho người học kiến thức về những cơ chế, mô hình và kỹ thuật để giữ bí mật, bảo đảm tính toàn vẹn và sẵn sàng trong các hệ thống thông tin. Những chủ đề chính bao gồm các phương pháp bảo vệ dữ liệu: Cơ bản về mã hoá, thiết kế bảo mật cơ sở dữ liệu, kiểm soát dòng thông tin, kiểm định… Người học có kỹ năng ứng dụng các kỹ thuật bảo mật vào các hệ thống thông tin.

3. Chủ đề và chuẩn đầu ra của học phần

3.1. Danh mục chủ đề của học phần

1. Yêu cầu của hệ an toàn bảo mật.
2. Mã hóa đối xứng cổ điển.
3. Mã hóa đối xứng hiện đại.
4. Mã hóa khóa công khai.
5. Mã chứng thực thông điệp và hàm băm.
6. Giao thức bảo mật.
7. Bảo mật cơ sở dữ liệu.

3.2. Chuẩn đầu ra của quá trình dạy - học từng chủ đề của học phần

Chủ đề 1: Yêu cầu của hệ an toàn bảo mật.

Nội dung	Mức độ
Kiến thức	
1. Các hình thức tấn công một hệ truyền tin.	2
2. Tính bí mật, tính chứng thực, tính không thoái thác.	2
Thái độ	
1. Việc tấn công trên mạng là không thể tránh khỏi	
2. Cần có các hình thức bảo vệ an toàn	

Kỹ năng	
1. Phân loại các hình thức tấn công.	3
2. Xác định được những chức năng cần áp dụng mã hóa trong các phần mềm.	2

Chủ đề 2: Mã hóa đối xứng cổ điển.

Nội dung	Mức độ
Kiến thức	
1. Ceasar, đơn bảng, đa bảng, hoán vị	2
2. Phá mã: vét cạn khóa, thống kê tần suất	3
3. Phá mã trong trường hợp known-plaintext, chosen plaintext	3
Thái độ	
1. Thay thế và hoán vị là hai phương pháp cơ bản để biến đổi bản rõ thành bản mã -> bảo mật 2. Khóa bí mật cần phải lớn để chống phá mã vét cạn. 3. Ngoài vét cạn, có thể phá mã bằng các kỹ thuật khác không lường trước	
Kỹ năng	
1. Lập trình thực hiện các phương pháp mã hóa đối xứng cổ điển.	2
2. Phá mã một bản mã cổ điển đơn giản.	3

Chủ đề 3: Mã hóa đối xứng hiện đại.

Nội dung	Mức độ
Kiến thức	
1. Mã dòng: A5/1, RC4	3
2. Mã khối: hệ mã Fiestel, mã DES.	3
3. Mô hình ứng dụng mã khối: ECB, CBC, CTR, OFB, CFB.	2
4. Tính chứng thực và không thoái thác của mã đối xứng	2
Thái độ	
1. Đặc điểm mã dòng: sử dụng bộ sinh số để tạo khóa dài 2. Đặc điểm mã khối: dùng phép biến đổi phức tạp để mã hóa khối dữ liệu, chống phá mã trong trường hợp known-plaintext, chosen plaintext **3.** Mã đối xứng có tính chứng thực.	
Kỹ năng	
1. Lập trình thực hiện mã A5/1, RC4, DES.	3
2. Lập trình sử dụng thư viện DES trong .NET Framework, Java	2
3. Mã hóa file trên máy tính, mã hóa dữ liệu trong lập trình mạng	2

Chủ đề 4: Mã hóa khóa công khai.

Nội dung	Mức độ
Kiến thức	
1. Lý thuyết số và hàm một chiều.	2
2. Mã hóa RSA.	3
3. Truyền khóa Diffie-Hellman.	3
4. Tính chứng thực và không thoái thác của mã công khai.	2
Thái độ	
1. Điểm yếu của mã đối xứng: tốn chi phí truyền khóa bí mật, có thể lộ khóa. 2. Số học modulo có tính bất đối xứng. Thời gian thực hiện chiều thuận và chiều nghịch là khác nhau. 3. Mã công khai: dùng 2 khóa khác nhau để mã hóa và giải mã -> không cần truyền khóa bí mật 4. Mã công khai có không thoái thác -> chữ ký điện tử 5. Mã công khai thực hiện chậm -> kết hợp với mã đối xứng	
Kỹ năng	
1. Lập trình thực hiện số học modulo trên số lớn (>100 chữ số), thuật toán Euclid mở rộng, thuật toán Miller-Rabin.	2
2. Lập trình thực hiện mã hóa RSA trên số lớn.	3
3. Lập trình sử dụng thư viện RSA trong .NET Framework, Java	2

Chủ đề 5: Mã chứng thực thông điệp và hàm hash.

Nội dung	Mức độ
Kiến thức	
1. Checksum CRC	1
2. Mã chứng thực thông điệp MAC	2
3. Nghịch lý ngày sinh và hàm Hash	2
4. Ứng dụng hàm Hash	2
5. Chữ ký điện tử	3
Thái độ	
1. Checksum: từ bản tin ngẫu nhiên thành bản tin có cấu trúc 2. MAC: checksum dùng mã khối 3. Hash: checksum dựa trên biến đổi ngẫu nhiên **4.** Hash có tính chống trùng -> dấu vân tay của thông điệp -> kết hợp với mã khóa công khai thành chữ ký điện tử.	
Kỹ năng	
1. Lập trình thực hiện hàm băm MD5, SHA.	3
2. Lập trình sử dụng thư viện RSA trong .NET Framework, Java	2
3. Ứng dụng MD5, SHA vào mã hóa password database.	2

Chủ đề 6: Giao thức bảo mật.

Nội dung	Mức độ
Kiến thức	
1. Cơ chế chống replay-attack	2
2. Chứng chỉ X509, giao thức SSL, giao thức S-MIME.	3
Thái độ	
Giao thức là các nguyên tắc áp dụng mã hóa để thiết lập một hệ truyền tin an toàn bảo mật.	
Kỹ năng	
1. Đăng ký tạo chứng chỉ X509 tại các trung tâm chứng thực	2
2. Cấu hình Webserver dùng giao thức SSL	3

Chủ đề 6: Bảo mật cơ sở dữ liệu.

Nội dung	Mức độ
Kiến thức	
1. Cơ chế phân quyền	2
2. Mã hóa cơ sở dữ liệu	3
3. Tấn công SQL Injection	3
Thái độ	
Phân quyền và mã hóa là hai hình thức phổ biến để bảo mật cơ sở dữ liệu	
Kỹ năng	
1. Sử dụng chức năng phân quyền trong các hệ quản trị cơ sở dữ liệu.	2
2. Sử dụng các chức năng mã hóa trong các hệ quản trị cơ sở dữ liệu.	2
3. Lập trình không bị tấn công SQL Injection	3

4. Phân bổ thời gian chi tiết

Chủ đề	Phân bổ số tiết cho hình thức dạy - học					Tổng
	Lên lớp			Thực hành, thực tập	Tự nghiên cứu	
	Lý thuyết	Bài tập	Thảo luận			
1	2				4	
2	4	2	1		14	
3	6	2	1		18	
4	6	2	1		18	
5	4	2	1		14	
6	4	2			12	
7	4		1		10	

5. Tài liệu

TT	Tên tác giả	Tên tài liệu	Năm xuất bản	Nhà xuất bản	Địa chỉ khai thác tài liệu
1	William Stalling	Cryptography and Network Security, 4th	2005	Prentice Hall	Thư viện
2	Trần Minh Triết, Dương Anh Đức	Mã hóa và Ứng dụng	2005	Đại học Khoa Học Tự Nhiên	Ebook
3	Mark Stamp	Information Security: Principle and Practice	2006	Wiley	Thư viện
4	Simon Sign	Mật mã, từ cổ điển đến lượng tử	2008	Nhà xuất bản Trẻ	Thư viện

6. Đánh giá kết quả học tập

TT	Các chỉ tiêu đánh giá	Phương pháp đánh giá	Trọng số (%)
1	Tham gia học trên lớp: *lên lớp đầy đủ, chuẩn bị bài tốt, tích cực thảo luận…*	*Quan sát, điểm danh*	10
2	Tự nghiên cứu: *bài tập nhóm theo tháng*	*Chấm báo cáo, bài tập*	20
3	Kiểm tra giữa kỳ	*Viết, vấn đáp*	20
4	Thi kết thúc học phần	*Viết*	50

TRƯỞNG KHOA **TRƯỞNG BỘ MÔN**

(Ký và ghi họ tên)