TRƯỜNG ĐẠI HỌC KNH TẾ - KỸ THUẬT CÔNG NGHIỆP

KHOA CÔNG NGHỆ THÔNG TIN

BỘ MÔN: MẠNG MÁY TÍNH VÀ CÔNG NGHỆ ĐA PHƯƠNG TIỆN

ĐỀ CƯƠNG CHI TIẾT
HỌC PHẦN: AN TOÀN THÔNG TIN

1. THÔNG TIN CHUNG

Tên học phần (tiếng Việt):	AN TOÀN THÔNG TIN
Tên học phần (tiếng Anh):	NETWORK SECURITY
Mã môn học:	
Khoa/Bộ môn phụ trách:	Mạng máy tính và công nghệ đa phương tiện
Giảng viên phụ trách chính:	Ths. Nguyễn Hoàng Chiến
	Email: nhchien@uneti.edu.vn
GV tham gia giảng dạy:	Ths. Nguyễn Thu Hiền, Đào Thụy Ánh.
Số tín chỉ:	3 (39, 12, 45, 90)
Số tiết Lý thuyết:	39
Số tiết TH/TL:	12
	39+12/2 = 15 tuần x 3 tiết/tuần
Số tiết Tự học:	90
Tính chất của học phần:	Bắt buộc
Học phần học trước:	Mạng máy tính
Học phần tiên quyết:	Mạng máy tính
Các yêu cầu của học phần:	Sinh viên có tài liệu học tập

2. MÔ TẢ HỌC PHẦN

An toàn thông tin là học phần kiến thức cơ sở khối ngành và ngành của chương trình đào tạo đại học ngành Công nghệ thông tin. Học phần được bố trí giảng dạy sau học phần Toán rời rạc và Mạng máy tính. Học phần trang bị cho sinh viên những kiến thức cơ bản về các khái niệm mang tính chất cơ sở của lĩnh vực an toàn mạng, nguyên lý hoạt động của các giải thuật mã hóa đối xứng hiện đại và sơ đồ mã hóa khối tổng quát Feistel. Các phương thức mã hóa liên hợp nhiều khối và cách thức chung quản lý các khóa bí mật. Các ứng dụng bảo mật, chữ ký số, và trao đổi khóa bí mật của mật mã khóa công khai. Các cơ chế xác thực thông báo và tác giả của thông báo. Các ứng dụng của các phương pháp mật mã, xác thực và chữ ký số trong lĩnh vực an toàn mạng.

3. MỤC TIÊU CỦA HỌC PHẦN ĐỐI VỚI NGƯỜI HỌC

Kiến thức:

Trang bị cho sinh viên các kiến thức cơ bản về an toàn truyền thông trên mạng Internet. Nắm được các phương pháp mã hóa đối xứng và mã hóa khóa công khai, các kỹ thuật xác thực và chữ ký số. Một số dịch vụ xác thực phổ biến ở mức ứng dụng. Biết một số phương thức chủ yếu đảm bảo an toàn thư điện tử, cơ chế an toàn mạng ở mức IP và một số phương thức chuẩn đảm bảo an toàn cho các giao tác trên Web.

Kỹ năng:

- Sử dụng các giải thuật mã hóa, mã xác thực thông báo và băm. Vận dụng suy luận toán học đánh giá độ an toàn hệ thống.
- Phân tích phát hiện các yếu điểm của các hệ thống mạng và các hiểm họa tấn công. Áp dụng một cách thích hợp các kỹ thuật an toàn mạng thông dụng.
- Đề xuất và xây dựng các giải pháp đảm bảo an toàn truyền thông.

Phẩm chất đạo đức và trách nhiệm:

Nghiêm túc, trách nhiệm, chủ động, tích cực, chăm chỉ, cẩn thận.

4. CHUẨN ĐẦU RA HỌC PHẦN

Mã CĐR	**Mô tả CĐR học phần** *Sau khi học xong môn học này, người học có thể:*	**CĐR của CTĐT**
G1	**Về kiến thức**	
G1.1.1	Nắm được các khái niệm mang tính chất cơ sở của lĩnh vực an toàn mạng, nguyên lý hoạt động của các giải thuật mã hóa đối xứng hiện đại.	1.1.2; 1.1.3; 1.2.1
G1.1.2	Cung cấp các phương thức mã hóa liên hợp nhiều khối và cách thức chung quản lý các khóa bí mật.	1.2.3; 1.3.2
G1.2.1	Biết một số phương thức chủ yếu đảm bảo an toàn thư điện tử, cơ chế an toàn mạng	1.4.2; 1.4.3
G2	**Về kỹ năng**	
G2.1.1	Sử dụng các giải thuật mã hóa, mã xác thực thông báo và băm. Vận dụng suy luận toán học đánh giá độ an toàn hệ thống.	2.1.3
G2.1.2	Phân tích phát hiện các yếu điểm của các hệ thống mạng và các hiểm họa tấn công. Áp dụng một cách thích hợp các kỹ thuật an toàn mạng thông dụng.	2.1.4
G2.2.1	Đề xuất và xây dựng các giải pháp đảm bảo an toàn truyền thông.	2.1.5
G2.2.2	Khả năng làm việc theo nhóm để giải quyết các vấn đề trong an toàn hệ thống.	2.1.5
G3	**Năng lực tự chủ và trách nhiệm**	
G3.1.1	Rèn luyện tính chủ động trong học tập và rèn luyện.	3.1.1
G3.2.1	Tổng hợp cập nhật được những thay đổi về hệ điều hành, những xu hướng phát triển trong tương lai.	3.2.1
G3.2.2	Thi hành và tuân thủ đạo đức nghề nghiệp ngành CNTT	3.2.3

5. NỘI DUNG MÔN HỌC, KẾ HOẠCH GIẢNG DẠY

Tuần thứ	Nội dung	Số tiết LT	Số tiết TH	Tài liệu học tập, tham khảo
1	**Chương 1. GIỚI THIỆU** *1.1 Khái niệm an toàn mạng* *1.2 Các yếu tố xác lập an toàn thông tin* 1.2.1 Các dịch vụ an toàn 1.2.2 Các cơ chế an toàn 1.2.3 Các hình thức tấn công *1.3 Mô hình an toàn mạng*	3		1, 2, 3, 4
2	**Chương 2. MÃ HÓA ĐỐI XỨNG CỔ ĐIỂN** *2.1. Mô hình mã hóa đối xứng* *2.2. Các hệ mã hóa thay thế cổ điển* 2.2.1. Hệ mã hóa Caesar 2.2.2. Hệ mã hóa đơn bảng 2.2.3. Hệ mã hóa Playfair 2.2.4. Hệ mã hóa Vigenère 2.2.5. Hệ mã hóa khóa tự động 2.2.6. Hệ mã hóa độn một lần *2.3. Các kỹ thuật mã hóa hoán vị cổ điển* 2.4.1. Hệ mã hóa hàng rào 2.4.2. Hệ mã hóa hàng *2.4. Mã hóa kết hợp*	3		1, 2, 3, 4
3	**Chương 3. MÃ HÓA ĐỐI XỨNG HIỆN ĐẠI** *3.1. Nguyên lý của các hệ mã hóa khối* 3.1.1. Mạng S-P 3.1.2. Sơ đồ mã hóa Feistel *3.2. Chuẩn mã hóa dữ liệu DES*	3		1, 2, 3, 4

	3.3. Hệ mã hóa 3DES *3.4. Chuẩn mã hóa tiên tiến AES*			
4	*3.5. Các hệ mã hóa khối khác* 3.5.1. Giải thuật IDEA 3.5.2. Giải thuật Blowfish 3.5.3. Giải thuật RC5 3.5.4. Giải thuật CAST-128 *3.6. Các phương thức mã hóa liên hợp* 3.6.1. Phương thức ECB 3.6.2. Phương thức CBC 3.6.3. Phương thức CFB 3.6.4. Phương thức OFB 3.6.5. Phương thức CTR *3.7. Triển khai chức năng mã hóa* *3.8. Quản lý và phân phối khóa*	3		1, 2, 3, 4
5	**Chương 4. MẬT MÃ KHÓA CÔNG KHAI** *4.1 Nguyên lý của các hệ mật mã khoá công khai* *4.2 Hệ mã hoá RSA*	3		1, 2, 3, 4
6	*4.3 Hệ trao đổi khoá Diffie-Hellman* *4.4 Hạn chế của mật mã khoá công khai*	3		1, 2, 3, 4
7	**Bài thảo luận (thực hành môn học) số 1** **Kiểm tra định kỳ lần 1**		6	1, 2, 3, 4
8	**Chương 5. XÁC THỰC VÀ CHỮ KÝ SỐ** *5.1 Khái niệm xác thực thông báo* *5.2 Mã xác thực thông báo (MAC)* *5.3. Hàm băm*	3		1, 2, 3, 4

9	*5.4 An toàn hàm băm và MAC* *5.5 Chữ ký số*	3		1, 2, 3, 4
10	**Chương 6. CÁC ỨNG DỤNG XÁC THỰC** *6.1. Hệ thống xác thực Kerberos* 6.1.1. Đặt vấn đề 6.1.2. Một giải pháp đơn giản 6.1.3. Một giải pháp an toàn hơn 6.1.4. Kerberos 4 6.1.5. Kerberos 5	3		1, 2, 3, 4
11	*6.2. Dịch vụ chứng thực X.509* 6.2.1. Chức năng của dịch vụ X.509 6.2.2. Khuôn dạng chứng thực X.509 6.2.3. Xác minh chứng thực 6.2.4. Thu hồi chứng thực 6.2.5. Các thủ tục xác thực dựa trên X.509	3		1, 2, 3, 4
12	**Chương 7. AN TOÀN THƯ ĐIỆN TỬ** *7.1. Chương trình PGP* 7.1.1. Chức năng xác thực 7.1.2. Chức năng bảo mật 7.1.3. Kết hợp xác thực và bảo mật 7.1.4. Chức năng nén 7.1.5. Chức năng tương thích thư điện tử 7.1.6. Chức năng phân và ghép 7.1.7. Quản lý khóa *7.2. Chuẩn S/MIME* 7.2.1. Các chức năng của S/MIME 7.2.2. Các thông báo S/MIME	3		1, 2, 3, 4

	7.2.3. Xử lý chứng thực			
13	**Chương 8. AN TOÀN IP** *8.1. Khái niệm IPSec* *8.2. Kiến trúc IPSec* *8.3. Giao thức xác thực AH* *8.4. Giao thức xác thực/mã hóa ESP* *8.5. Kết hợp các liên kết an toàn* *8.6. Quản lý khóa*	3		1, 2, 3, 4
14	**Chương 9. AN TOÀN WEB** *9.1. Dich vụ an toàn mức giao vận SSL* 9.1.1. Kiến trúc SSL 9.1.2. Giao thức chuyển đổi bản ghi SSL 9.1.3. Các giao thức chuyên dụng của SSL *9.2. Giao thức SET*	3		1, 2, 3, 4
15	**Bài thảo luận (thực hành môn học) số 2** **Kiểm tra định kỳ lần 2**		6	1, 2, 3, 4

6. MA TRẬN MỨC ĐỘ ĐÓNG GÓP CỦA NỘI DUNG GIẢNG DẠY ĐỂ ĐẠT ĐƯỢC CHUẨN ĐẦU RA CỦA HỌC PHẦN

Mức 1: Thấp
Mức 2: Trung bình
Mức 3: Cao

Chương	Nội dung giảng dạy	Chuẩn đầu ra học phần									
		G1.1.1	G1.1.2	G1.2.1	G2.1.1	G2.1.2	G2.2.1	G2.2.2	G3.1.1	G3.2.1	G3.2.2
1	***Chương 1: Giới thiệu***										
	1.1 Khái niệm an toàn mạng	2									
	1.2 Các yếu tố xác lập an toàn thông tin 1.2.1 Các dịch vụ an toàn 1.2.2 Các cơ chế an toàn 1.2.3 Các hình thức tấn công	2									
	1.3 Mô hình an toàn mạng	2	2	2							
2	***Chương 2: Mã hoá đối xứng cổ điển***										
	2.1. Mô hình mã hóa đối xứng				2	2	2				
	2.2. Các hệ mã hóa thay thế cổ điển 2.2.1. Hệ mã hóa Caesar 2.2.2. Hệ mã hóa đơn bảng 2.2.3. Hệ mã hóa Playfair 2.2.4. Hệ mã hóa Vigenère 2.2.5. Hệ mã hóa khóa tự động 2.2.6. Hệ mã hóa độn một lần				2	2	2				
	2.3. Các kỹ thuật mã hóa hoán vị cổ điển				2	2	2				
	2.3.1. Hệ mã hóa hàng rào				2	2	2				
	2.3.2. Hệ mã hóa hàng				2	2	2				
	2.4. Mã hóa kết hợp				2	2	2				
	Chương 3: Mã hoá đối xứng hiện đại										
	3.1. Nguyên lý của các hệ mã hóa khối 3.1.1. Mạng S-P 3.1.2. Sơ đồ mã hóa Feistel			2							
	3.2. Chuẩn mã hóa dữ liệu DES				2	2	2				
	3.3. Hệ mã hóa 3DES				2	2	2				
	3.4. Chuẩn mã hóa tiên tiến AES				2	2	2				
	3.5. Các hệ mã hóa khối khác 3.5.1. Giải thuật IDEA 3.5.2. Giải thuật Blowfish 3.5.3. Giải thuật RC5 3.5.4. Giải thuật CAST-128				2	2	2				
	3.6. Các phương thức mã hóa				2	2	2				

	liên hợp 3.6.1. Phương thức ECB 3.6.2. Phương thức CBC 3.6.3. Phương thức CFB 3.6.4. Phương thức OFB 3.6.5. Phương thức CTR										
	3.7. Triển khai chức năng mã hóa				2	2	2	2			
	3.8. Quản lý và phân phối khóa				2	2	2	2			
	Chương 4: Mật mã khoá công khai										
	4.1 Nguyên lý của các hệ mật mã khoá công khai 4.2 Hệ mã hoá RSA	2	2	2							
	4.3 Hệ trao đổi khoá Diffie-Hellman				2	2	2				
	4.4 Hạn chế của mật mã khoá công khai	2	2	2							
	Chương 5: Xác thực và chữ ký số										
	5.1 Khái niệm xác thực thông báo	2	2	2							
	5.2 Mã xác thực thông báo (MAC)	2	2	2							
	5.3. Hàm băm	2	2	2							
	5.4 An toàn hàm băm và MAC	2	2	2							
	5.5 Chữ ký số	2	2	2							
	***Chương 6:* Các ứng dụng xác thực**										
	6.1. Hệ thống xác thực Kerberos 6.1.1. Đặt vấn đề 6.1.2. Một giải pháp đơn giản 6.1.3. Một giải pháp an toàn hơn 6.1.4. Kerberos 4 6.1.5. Kerberos 5	2	2	2	2	2	2				
	6.2. Dịch vụ chứng thực X.509 6.2.1. Chức năng của dịch vụ X.509 6.2.2. Khuôn dạng chứng thực X.509 6.2.3. Xác minh chứng thực 6.2.4. Thu hồi chứng thực 6.2.5. Các thủ tục xác thực dựa trên X.509				2	2	2				
	Chương 7. An toàn thư điện tử										
	7.1. Chương trình PGP 7.1.1. Chức năng xác thực 7.1.2. Chức năng bảo mật	2	2	2	2	2	2				

	7.1.3. Kết hợp xác thực và bảo mật 7.1.4. Chức năng nén 7.1.5. Chức năng tương thích thư điện tử 7.1.6. Chức năng phân và ghép 7.1.7. Quản lý khóa										
	7.2. Chuẩn S/MIME 7.2.1. Các chức năng của S/MIME 7.2.2. Các thông báo S/MIME 7.2.3. Xử lý chứng thực				2	2	2				
	Chương 8. An toàn IP										
	8.1. Khái niệm IPSec	2	2	2							
	8.2. Kiến trúc IPSec				2	2	2				
	8.3. Giao thức xác thực AH				2	2	2				
	8.4. Giao thức xác thực/mã hóa ESP				2	2	2				
	8.5. Kết hợp các liên kết an toàn				2	2	2	2			
	8.6. Quản lý khóa				2	2	2	2			
	Chương 9. An toàn Web										
	9.1. Dịch vụ an toàn mức giao vận SSL 9.1.1. Kiến trúc SSL 9.1.2. Giao thức chuyển đổi bản ghi SSL 9.1.3.Các giao thức chuyên dụng của SSL	2	2	2	2	2	2				

7. PHƯƠNG THỨC ĐÁNH GIÁ HỌC PHẦN

(vị trí của x tùy thuộc theo mỗi tiêu chí trong CĐR học phần cần kiểm tra đánh giá để đảm bảo CĐR của học phần đáp ứng theo mong muốn của CĐR CTĐT)

TT	Điểm thành	Quy định *(Theo QĐ Số:*	Chuẩn đầu ra học phần

			G1.1.1	G1.1.2	G1.2.1	G1.2.2	G2.1.1	G2.1.2	G2.2.1	G2.2.2	G3.1.1	G3.2.1	G3.2.2
1	Điểm quá trình (40%)	1. Kiểm tra thường xuyên + Hình thức: *Tham gia thảo luận, kiểm tra 15 phút hỏi đáp.* + Số lần: *Tối thiểu 1 lần/sinh viên* + Hệ số: *1*	x	x	x	x	x	x	x	x	x	x	
		2. Kiểm tra định kỳ lần 1 + Hình thức: *Tự luận.* + Thời điểm: *tuần 7.* + Hệ số: *2*	x	x			x	x		x	x		x
		3. Kiểm tra định kỳ lần 2 + Hình thức: *Tự luận.* + Thời điểm: *tuần 15.* + Hệ số: *2*	x	x	x	x	x	x	x	x	x	x	x
		4. Kiểm tra định kỳ lần 3 + Hình thức: *Nộp bài tập lớn theo đề tài ứng dụng.* + Thời điểm: *Tuần 15* + Hệ số: *2*	x	x	x	x	x	x	x	x	x	x	x
		5. Kiểm tra chuyên cần + Hình thức: *Điểm danh theo thời gian tham gia học trên lớp* + Hệ số: *3*	x	x	x	x	x	x	x	x	x	x	x
2	Điểm thi kết thúc	+ Hình thức: *Tự luận* + Thời điểm: *Theo lịch thi học kỳ*											

	học phần (60%)	+ Tính chất: *Bắt buộc*											

8. PHƯƠNG PHÁP DẠY VÀ HỌC

- Giảng viên giới thiệu học phần, tài liệu học tập, tài liệu tham khảo, các địa chỉ website để tìm tư liệu liên quan đến môn học. Nêu nội dung cốt lõi của chương và tổng kết chương, sử dụng bài giảng điện tử và các mô hình giáo cụ trực quan trong giảng dạy. Tập trung hướng dẫn học, tư vấn học, phản hồi kết quả thảo luận, bài tập lớn, kết quả kiểm tra và các nội dung lý thuyết chính mỗi chương.
- Các phương pháp giảng dạy có thể áp dụng: Phương pháp thuyết trình; Phương pháp thảo luận nhóm; Phương pháp mô phỏng; Phương pháp minh họa; Phương pháp miêu tả, làm mẫu.
- Sinh viên chuẩn bị bài từng chương, làm bài tập đầy đủ, trau dồi kỹ năng làm việc nhóm để chuẩn bị bài thảo luận, làm các câu hỏi trắc nghiệm mẫu để củng cố kiến thức.
- Trong quá trình học tập, sinh viên được khuyến khích đặt câu hỏi phản biện, trình bày quan điểm, các ý tưởng sáng tạo mới dưới nhiều hình thức khác nhau.

9. QUY ĐỊNH CỦA HỌC PHẦN

9.1. Quy định về tham dự lớp học

- Sinh viên/học viên có trách nhiệm tham dự đầy đủ các buổi học. Trong trường hợp nghỉ học do lý do bất khả kháng thì phải có giấy tờ chứng minh đầy đủ và hợp lý.
- Sinh viên vắng quá 50% buổi học dù có lý do hay không có lý do đều bị coi như không hoàn thành khóa học và phải đăng ký học lại vào học kỳ sau.
- Tham dự các tiết học lý thuyết
- Thực hiện đầy đủ các bài tập được giao trong cuốn tài liệu học tập.
- Tham dự kiểm tra giữa học kỳ.
- Tham dự thi kết thúc học phần.
- Chủ động tổ chức thực hiện giờ tự học.

9.2. Quy định về hành vi lớp học

- Học phần được thực hiện trên nguyên tắc tôn trọng người học và người dạy. Mọi hành vi làm ảnh hưởng đến quá trình dạy và học đều bị nghiêm cấm.
- Sinh viên phải đi học đúng giờ quy định. Sinh viên đi trễ quá 15 phút sau khi giờ học bắt đầu sẽ không được tham dự buổi học.
- Tuyệt đối không làm ồn, gây ảnh hưởng đến người khác trong quá trình học.
- Tuyệt đối không được ăn uống, nhai kẹo cao su, sử dụng các thiết bị như điện thoại, máy nghe nhạc trong giờ học.

10. TÀI LIỆU HỌC TẬP, THAM KHẢO

10.1 Tài liệu học tập

[1]. TS Lê Văn Phùng, *An toàn thông tin*, NXB Thông tin & Truyền Thông, 2018.

10.2. Tài liệu tham khảo

[2]. Thái Hồng Nhị, Phạm Minh Việt, *An toàn thông tin mạng máy tính, truyền tin số và truyền dữ liệu*, NXB Khoa học và kỹ thuật, 2004.

[3]. Đỗ Trung Tuấn, *An toàn cơ sở dữ liệu,* NXB ĐH Quốc Gia Hà Nội, 2018.

[4]. Trần Đức Sự, Nguyễn Văn Tảo, Trần Thị Lượng, *Giáo trình an toàn bảo mật dữ liệu*, NXB ĐH Thái Nguyên, 2015.

11. HƯỚNG DẪN THỰC HIỆN

- ✓ Các Khoa, Bộ môn phổ biến đề cương chi tiết cho toàn thể giáo viên thực hiện.
- ✓ Giảng viên phổ biến đề cương chi tiết cho sinh viên vào buổi học đầu tiên của học phần.
- ✓ Giảng viên thực hiện theo đúng đề cương chi tiết đã được duyệt.

Hà Nội, Ngày .... tháng .... năm 2018

Trưởng khoa	**Trưởng bộ môn**	**Người biên soạn**
(Ký và ghi rõ họ tên)	*(Ký và ghi rõ họ tên)*	*(Ký và ghi rõ họ tên)*