



ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN: AN TOÀN VÀ AN NINH MẠNG

1. Thông tin về các giảng viên học phần

STT	Họ và tên	Chức danh, học vị	Địa chỉ liên hệ	Điện thoại/Email	Ghi chú
1	Nguyễn Đại Thọ	TS	PTN ATTT	nguyendaitho@vnu.edu.vn	Trưởng học phần
2	Lê Đình Thanh	TS	PTN ATTT	thanhld@vnu.edu.vn	Giảng viên
3	Đoàn Minh Phương	ThS	BM M&TTMT	phuongdm@vnu.edu.vn	Giảng viên

2. Thông tin chung về học phần

- Tên học phần: An toàn và an ninh mạng
- Mã số học phần: INT3307
- Số tín chỉ: 3
- Giờ tín chỉ đối với các hoạt động (LT/ThH/TH): 39/6/0
- Học phần tiên quyết: INT2209 – Mạng máy tính
- Các yêu cầu đối với học phần (nếu có):
- Bộ môn, Khoa phụ trách học phần: Bộ môn M&TTMT, Khoa CNTT

3. Mục tiêu học phần

- Kiến thức:

Các bài giảng cung cấp cho học viên những kiến thức sau đây:

- Các khái niệm cơ bản về an ninh truyền thông và an ninh hệ thống
 - Tổng quan về các giải thuật và giao thức mã hóa khối đối xứng, mật mã khóa công khai, các phương pháp xác thực, hàm băm, chữ ký số, và các kỹ thuật quản lý khóa
 - Một số dịch vụ xác thực phổ biến ở mức ứng dụng
 - Một số phương thức chủ yếu đảm bảo an ninh thư điện tử
 - Cơ chế an ninh mạng ở tầng IP
 - Một số phương thức chuẩn đảm bảo an ninh cho các giao tác trên nền Web
- Kỹ năng:

Các bài tập rèn luyện cho học viên những kỹ năng sau đây:

- Vận dụng các phương pháp mật mã học trong các giao thức mạng phục vụ mục đích đảm bảo an ninh truyền thông
- Thảo luận về những vấn đề chính yếu liên quan đến an ninh mạng
- 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 căn bản đảm bảo an ninh truyền thông và an ninh hệ thống trong các tình huống cần thiết
- Đề xuất và xây dựng các giải pháp đảm bảo an ninh của các hệ thống mạng

4. Chuẩn đầu ra

Mục tiêu Nội dung	Bậc 1	Bậc 2	Bậc 3	Bậc 4
1. Kiến thức				
1.3 Kiến thức chung của khối ngành (M3)				
1.3.2 Hiểu được đặc thù chuyên nghiệp trong công nghệ, phân biệt được những nét đặc trưng của yêu cầu chuyên nghiệp trong công nghệ	X			
1.3.4 Hiểu và vận dụng được các khái niệm cơ bản của lý thuyết xác suất		X		
1.4 Kiến thức chung của nhóm ngành (M4)				
1.4.1 Hiểu và vận dụng được các kiến thức cơ bản về Toán rời rạc để xây dựng các thuật toán, tối ưu các giải pháp trong công nghệ		X		
1.4.6 Hiểu các khái niệm cơ bản về mạng máy tính, các bộ phận, các giao thức, cách thức truyền dữ liệu trên mạng			X	
1.5 Kiến thức của ngành và bổ trợ (M5)				
1.5.3 Vận dụng được các kiến thức trong lĩnh vực quản trị mạng		X		
1.5.4 Hiểu và vận dụng được kiến thức chuyên sâu theo định hướng “Mạng máy tính” bao gồm các chuyên đề về quản trị mạng, thực hành an ninh mạng, mạng không dây, truyền thông đa phương tiện, lập trình mạng, ...			X	
1.5.5 - Hiểu và vận dụng được kiến thức chuyên sâu theo định hướng “Truyền thông”, bao gồm các chuyên đề về mạng không dây, mạng quang, thiết kế và quản trị mạng viễn thông, mã hóa, ...			X	
2. Kỹ năng				
2.1 Kỹ năng cứng				
2.1.1 Các kỹ năng nghề nghiệp				
2.1.1.1 Vận dụng các kiến thức cơ bản về Toán và Vật lý trong khoa học công nghệ và đời sống	X			
2.1.1.5 Biết tìm kiếm, cập nhật, tổng hợp, khai thác thông tin		X		
2.1.1.6 Đọc hiểu tài liệu tiếng Anh chuyên ngành		X		
2.1.1.8 Biết sử dụng các kiến thức chuyên môn một cách linh hoạt		X		
2.1.2 Kỹ năng lập luận tư duy và giải quyết vấn đề				

Mục tiêu Nội dung	Bậc 1	Bậc 2	Bậc 3	Bậc 4
2.1.2.1 Có kỹ năng phát hiện vấn đề		X		
2.1.2.2 Có kỹ năng đánh giá và phân tích vấn đề		X		
2.1.2.3 Có kỹ năng giải quyết vấn đề chuyên môn		X		
2.1.2.4 Có kỹ năng mô hình hóa		X		
2.1.3 Kỹ năng nghiên cứu và khám phá kiến thức				
2.1.3.2 Có kỹ năng dùng thực nghiệm để khám phá kiến thức		X		
2.1.3.4 Có kỹ năng áp dụng kiến thức vào thực tế		X		
2.1.4 Kỹ năng tư duy theo hệ thống				
2.1.4.1 Có tư duy logic		X		
2.1.4.2 Có tư duy phân tích, tổng hợp		X		
2.1.4.3 Có tư duy toàn cục		X		
2.1.5 Hiểu bối cảnh xã hội và ngoại cảnh				
2.1.5.1 Hiểu biết bối cảnh xã hội và cơ quan	X			
2.1.5.2 Nhận thức được vai trò và trách nhiệm của cá nhân với xã hội và cơ quan công tác	X			
2.1.5.3 Biết nắm bắt nhu cầu xã hội đối với kiến thức khoa học chuyên ngành	X			
2.1.7 Năng lực vận dụng kiến thức, kỹ năng vào thực tiễn				
2.1.7.1 Có năng lực phân tích yêu cầu	X			
2.1.7.2 Có năng lực thiết kế giải pháp	X			
2.2 Kỹ năng mềm				
2.2.1. Các kỹ năng cá nhân				
2.2.1.1 Có tư duy sáng tạo	X			
2.2.1.2 Có tư duy phản biện		X		
2.2.1.3 Biết đề xuất sáng kiến		X		
2.2.4. Kỹ năng giao tiếp				
2.2.4.1 Biết cách lập luận, sắp xếp ý tưởng		X		
3. Về phẩm chất đạo đức				
3.1 Phẩm chất đạo đức cá nhân				
3.1.1 Trung thực		X		
3.1.4 Nhiệt tình		X		

5. Tóm tắt nội dung môn học

Học phần giới thiệu các nguyên lý cơ bản của an toàn và an ninh mạng, trong đó tập trung vào các công nghệ và giao thức chuẩn đã được sử dụng rộng rãi để đảm bảo an toàn cho các dữ liệu truyền qua mạng.

Học phần bắt đầu bằng một chương giới thiệu về lĩnh vực an toàn và an ninh mạng, sau đó được tổ chức thành hai phần. Phần thứ nhất gồm hai chương điểm lại những kiến thức mật mã học cơ bản bao gồm các chủ đề về mã hóa đối xứng, mật mã khóa công khai, xác thực thông báo, hàm băm, và chữ ký số là nền tảng chung cho các ứng dụng an ninh mạng. Phần thứ hai trải dài trong bốn chương là nội dung chính của học phần. Chúng đề cập đến một loạt các ứng dụng và chuẩn an ninh mạng quan trọng bao gồm hệ thống xác thực phân tán Kerberos, các chứng thực X.509v3, giao thức an toàn giao vận SSL/TLS, giao thức an toàn Web HTTPS, chuẩn truyền thông an toàn SSH, chương trình thư điện tử PGP, chuẩn mở rộng khuôn dạng thư điện tử S/MIME, và giao thức an toàn tầng IP IPsec.

6. Nội dung chi tiết môn học

Chương 1. Giới thiệu

- 1.1. Bối cảnh
- 1.2. Các khái niệm an toàn thông tin
- 1.3. Kiến trúc an ninh OSI
- 1.4. Các tấn công an ninh
- 1.5. Các dịch vụ an ninh
- 1.6. Các cơ chế an ninh
- 1.7. Mô hình an ninh mạng
- 1.8. Tổng quan về mật mã học

Chương 2. Mã hóa đối xứng và bảo mật thông báo

- 2.1. Các nguyên tắc mã hóa đối xứng
- 2.2. Các giải thuật mã hóa đối xứng
- 2.3. Các số ngẫu nhiên và giả ngẫu nhiên
- 2.4. Mã hóa luồng và giải thuật RC4
- 2.5. Các chế độ hoạt động của các giải thuật mã hóa khối

Chương 3. Mật mã khóa công khai và xác thực thông báo

- 3.1. Các phương pháp xác thực thông báo
- 3.2. Hàm băm và giải thuật SHA
- 3.3. Các phương pháp mã xác thực thông báo
- 3.4. Các giải thuật mật mã khóa công khai
- 3.5. Chữ ký số

Chương 4. Phân phối khóa và xác thực người dùng

- 4.1. Phân phối khóa đối xứng sử dụng mã hóa đối xứng
- 4.2. Hệ thống xác thực Kerberos
- 4.3. Phân phối khóa sử dụng mã hóa bất đối xứng
- 4.4. Các chứng thực X.509
- 4.5. Cơ sở hạ tầng khóa công khai

Chương 5. An ninh mức giao vận

- 5.1. Vấn đề an ninh Web
- 5.2. Giao thức SSL
- 5.3. Chuẩn TLS
- 5.4. Giao thức HTTPS
- 5.5. Giao thức SSH

Chương 6. An ninh thư điện tử

- 6.1. Chương trình PGP
- 6.2. Chuẩn S/MIME

Chương 7. An ninh IP

- 7.1. Khái niệm an ninh IP
- 7.2. Chính sách an ninh IP
- 7.3. Giao thức ESP
- 7.4. Kết hợp các liên kết an ninh
- 7.5. Trao đổi khóa Internet

7. Học liệu

7.1. Học liệu bắt buộc

[1] William Stallings. *Network Security Essentials: Applications and Standards, Fourth Edition*. Prentice Hall, 2011.

[2] Vincent Nestler, Gregory White, Wm. Arthur Conklin, and Matthew Hirsch. *Principles of Computer Security: CompTIA Security+ and Beyond, Lab Manual, Second Edition*. McGraw-Hill, 2011.

[3] Mark Ciampa. *Security+ Guide to Network Security Fundamentals, Third Edition*. Course Technology, 2008.

7.2 Học liệu tham khảo

[4] William Stallings. *Cryptography and Network Security: Principles and Practice, Fifth Edition*. Prentice Hall, 2010.

[5] Wm. Arthur Conklin and Gregory White. *Principles of Computer Security, CompTIA Security+ and Beyond (Exam SY0-301), Third Edition*. McGraw-Hill, 2011.

8. Hình thức tổ chức dạy học

8.1. Phân bổ lịch trình giảng dạy trong 1 học kỳ (15 tuần)

Hình thức dạy	Số tiết/tuần	Từ tuần ...đến tuần...	Địa điểm
Lý thuyết	3	1-13	Giảng đường
Thực hành	3	12-15	Giảng đường
Tự học bắt buộc			

8.2 Lịch trình dạy cụ thể

Tuần	Tiết	Nội dung giảng dạy lý thuyết/thực hành	Nội dung sinh viên tự học
1	1	Chương 1	Đọc thêm chương 1 trong giáo trình bắt buộc của Stallings
	2		
	3		
2	4	Hướng dẫn làm bài tập thực hành	Tự làm các bài tập thực hành 1.1, 1.3, 2.1 và 6.2 trong tài liệu của Nestler et al.
	5		
	6		
3	7	Chương 2	Đọc thêm chương 2 trong giáo trình bắt buộc của

	8		Stallings. Tự làm các bài tập thực hành 11.2 và 11.3 trong tài liệu của Ciampa
	9		
4	10		
	11	Chương 3	Đọc thêm chương 3 trong giáo trình bắt buộc của Stallings Tự làm bài tập thực hành 11.1 trong tài liệu của Ciampa
	12		
5	13		
	14		
	15		
6	16	Chương 4	
	17		
	18		
7	19		
	20		
	21		
8	22	Chương 5	Đọc thêm chương 5 trong giáo trình bắt buộc của Stallings Tự làm các bài tập lý thuyết cuối chương 4 và từ đề thi các năm trước Tự làm các bài tập thực hành 8.2, 8.3, và 8.4 trong tài liệu của Nestler et al.
	23		
	24		
9	25		
	26		
	27		
10	28	Hướng dẫn làm bài tập thực hành	Nộp bài tập thực hành của năm chương đầu
	29		
	30		
11	31	Chữa bài tập lý thuyết	Làm một số bài tập lý thuyết các chương 4 và 5 trên lớp
	32		
	33		
12	34	Chương 6	Đọc thêm chương 7 trong giáo trình bắt buộc của Stallings Tự làm các bài tập lý thuyết cuối chương 7 và từ đề
	35		

	36		thi các năm trước Tự làm các bài tập thực hành 3.2, 5.3, và 8.1 trong tài liệu của Nestler et al.
13	37		
	38	Chương 7	Đọc thêm chương 8 trong giáo trình bắt buộc của Stallings Tự làm các bài tập lý thuyết cuối chương 8 và từ đề thi các năm trước Tự làm bài tập thực hành 8.5 trong tài liệu của Nestler et al.
	39		
40			
14	41		
	42		
	43	Chữa bài tập lý thuyết	Làm một số bài tập lý thuyết các chương 6 và 7 trên lớp Nộp bài tập thực hành của hai chương cuối
44			
45			
16	46	Thi cuối kỳ	Ôn tập các chương từ 4 đến 7 trong đó chú trọng vào các dạng bài tập lý thuyết đã chữa trên lớp
	47		

9. Chính sách đối với học phần và các yêu cầu khác của giảng viên

- Sinh viên tự nguyện chữa bài tập lý thuyết trên lớp, trả lời nhanh nhất câu hỏi thảo luận do giáo viên đặt ra và có ý kiến, câu hỏi hữu ích xây dựng bài giảng sẽ được cộng điểm thưởng vào điểm bài tập thực hành.
- Nếu điểm thưởng bằng hoặc vượt quá 8 điểm thì sinh viên được miễn hoàn toàn bài tập thực hành, tự động được 10 điểm cho phần đánh giá này.
- Tổng điểm thưởng và điểm bài tập thực hành không được vượt quá 10 điểm.
- Trong buổi thi cuối kỳ, sinh viên được sử dụng mọi loại tài liệu giấy (in, photocopy hoặc viết), tuy nhiên không được sử dụng các thiết bị lưu trữ điện tử như máy tính xách tay, máy tính bảng và điện thoại di động để tránh trao đổi bài.
- Sinh viên nào sao chép hoặc cố ý cho bạn sao chép bài tập thực hành sẽ bị 0 điểm cho phần đánh giá này

10. Phương pháp, hình thức kiểm tra, đánh giá kết quả học tập học phần

10.1. Mục đích và trọng số kiểm tra, đánh giá

Hình thức	Phương pháp	Mục đích	Trọng số
Bài tập thực hành	Tự làm ở nhà theo hướng dẫn trên lớp và nộp báo cáo viết	Đánh giá khả năng vận dụng kiến thức học phần vào thực tế của sinh viên	40%
Thi kết thúc học phần	Thi viết	Đánh giá kiến thức, kỹ năng sinh viên đạt được khi kết thúc học phần	60%
Tổng			100%

10.2. Tiêu chí đánh giá

- Tiêu chí đánh giá cụ thể với từng đầu điểm của học phần:

+ Bài tập thực hành: Sinh viên thực hiện đầy đủ các bước thực hành theo hướng dẫn trong đề bài của mỗi bài tập, trả lời tất cả các câu hỏi bao gồm các câu hỏi trong phần hướng dẫn, các câu hỏi tự luận và điền từ cuối mỗi bài tập.

+ Kết thúc môn: Sinh viên hiểu và vận dụng được các kiến thức và kỹ năng đã học, chú trọng vào 4 chương nội dung chính về an toàn và an ninh mạng, đặc biệt theo các dạng bài tập đã được hướng dẫn và rèn luyện thông qua các buổi chữa bài tập trên lớp

- Cụ thể việc đánh giá kiến thức, kỹ năng của sinh viên theo các mức đáp ứng được chuẩn đầu ra, mức khá, mức giỏi:

Tùy vào mức độ hoàn thành các bài tập và thi cuối kỳ mà sinh viên sẽ được phân loại thành trung bình, khá, và giỏi.

- Giỏi: Hoàn thành hết các bài tập thực hành (hoặc tích cực tham gia các hoạt động trên lớp để tích lũy số điểm thưởng tương ứng) và giải quyết tốt câu hỏi thi với mức độ hoàn thiện cao
- Khá: Hoàn thành được các bài tập thực hành và làm được các câu hỏi thi cơ bản, chưa giải quyết được một số nội dung khó hoặc chưa hoàn thiện
- Trung bình: Còn một số nội dung chưa làm được.

10.3. Lịch thi và kiểm tra

Hình thức thi và kiểm tra	Thời gian
Bài tập thực hành phần 1	Tuần 10
Bài tập thực hành phần 2	Tuần 15
Thi cuối kỳ	Theo lịch của Trường

Duyệt

Chủ nhiệm Khoa

Chủ nhiệm bộ môn