PHỤ LỤC - ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN

MẪU ĐỀ CƯƠNG CHI TIẾT

Trường Đại học Giao thông vận tải TP Hồ Chí Minh

Khoa : CÔNG NGHỆ THÔNG TIN

Bộ môn: MẠNG MÁY TÍNH & TRUYỀN THÔNG

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN

1.Tổng quát về học phần

Tên Học phần	**AN TOÀN THÔNG TIN** (*INFORMATION SECURITY*)

Mã số HP: 123033

Số tín chỉ	**3TC(2,1,0)**										
Số tiết - Tổng	**60**	LT	**30**	BT/ TL		TN/ TH	**30**	BTL		TKMH/ DAMH	
	Thực tập bên ngoài: buổi.										
Đánh giá (Thang điểm 10)	Qúa trình:			**40%**			Kiểm tra, bài tập trên lớp, Báo cáo bài tập lớn theo nhóm				
	Thi cuối kỳ:			**60%**			Thi viết + *trắc nghiệm*				
Môn tiên quyết	- Kỹ thuật lập trình									MS: 122001	
Môn học trước	-									MS:	
Môn song hành	-									MS:	
CTĐT ngành	***Ngành Công nghệ thông tin*** ***Ngành Truyền thông và Mạng máy tính***										
Trình độ Khối kiến thức	*Đại học* *Thuộc khối KT: Chuyên ngành*										
Ghi chú khác	Sinh viên không được vắng quá 20% số tiết học										

Ghi chú: - Những chữ viết tắt: LT; lý thuyết, BT: bài tập, TL: thảo luận, TN: thí nghiệm, TH thực hành, BTL: bài tập lớn, TKMH: thiết kế môn học, DAMH: Đồ án môn học;

- Bài tập lớn: mỗi tín chỉ có không quá 1 BTL, mỗi học phần có không quá 3 BTL

- TKMH, DAMH: là các đồ án hoặc thiết kế môn học có mã học phần riêng;

- Giờ lý thuyết: 1 TC = 15 tiết; giờ BT,TL, TN,TH: 1TC =30 tiết.

2. Mục tiêu của học phần:

- **Kiến thức**: Sinh viên được trang bị các kiến thức cơ bản về mã hóa, xác thực và các vấn đề liên quan đến an toàn và bảo mật thông tin.
- **Kỹ năng**: Làm quen với các giải thuật mã hóa, các cơ chế xác thực và các ứng dụng. Phát triển tư duy về xây dựng hệ thống an toàn.
- **Thái độ**: Yêu cầu sinh viên lên lớp đầy đủ các giờ học lý thyết và thực hành.

Mô tả tóm tắt học phần:

Học phần này bao gồm phần lý thuyết và thực hành. Về lý thuyết, học phần cung cấp các kiến thức về các dạng mã hóa từ cổ điển đến hiện đại, các cơ chế xác thực và chữ ký điện tử. Phần thực hành, sinh viên hiện thực một số giải thuật đã học ở phần lý thuyết.

3. Nội dung học phần:

Chương 1 Tổng quan về an toàn thông tin
Chương 2 Các lỗ hổng trong bảo mật và các điểm yếu của mạng
Chương 3 Kỹ thuật mã hoá
Chương 4 Chữ ký điện tử và chứng chỉ số
Chương 5 Các ứng dụng bảo mật hệ thống thông tin

3.1 Nội dung khái quát

TT	Tên mục/ tiểu mục	Lý thuyết (Số tiết)	BT/TL (Số tiết)	TN/TH (Số tiết)	BTL/DA (Số tiết)	Tổng số tiết/ TC
1	***Chương 1.*** Tổng quan về an toàn thông tin	2				2
2	***Chương 2.*** Các lỗ hổng trong bảo mật và các điểm yếu của mạng	5		5		10
3	***Chương 3.*** Kỹ thuật mã hoá	6		6		12
4	***Chương 4.*** Chữ ký điện tử và chứng chỉ số	5		5		10
5	***Chương5.*** Các	5		5		10

	ứng dụng bảo mật hệ thống thông tin					
	Cộng:					

(TH: thực hành; BT: bài tập; TL: thảo luận; TKMH: thiết kế môn học; BTL: bài tập lớn; DA: đồ án môn học)

3.2 Nội dungchi tiết và phương pháp giảng dạy, đánh giá

Kiến thức (Biết cái gì)	**Kỹ năng (Làm được gì?)**	**PP giảng dạy**	**PP đánh giá**
Chương 1: **Tổng quan về an toàn thông tin** 1.1 Mở đầu 1.2 Sự cần thiết phải bảo vệ thông tin 1.3 Virus và các biện pháp phòng chống virus 1.4 Các đặc trưng xâm nhập 1.5 Đặc trưng kỹ thuật của an toàn bảo mật Tham khảo [ ]	Biết cách làm cho hệ thống và máy tính an toàn. Hạn chế được tấn công mạng	Giảng viên thuyết trình, làm mẫu các nội dung căn bản và hướng dẫn sinh viên tự đọc sách và thực hành	- Bài tập thực hành trên máy
Chương 2. **Các lỗ hổng trong bảo mật và các điểm yếu của mạng** 2.1 Giao thức TCP/IP 2.2 Lỗ hổng bảo mật trên Internet 2.3 Một số phương thức tấn công 2.4 Các biện pháp phát hiện hệ thống bị tấn công 2.5 Các biện pháp phòng ngừa Tham khảo: [][]	Biết cách vá lỗi những lỗ hổng trên bảo mật. Biết được một số cách tấn công mạng và phòng thủ	Giảng viên thuyết trình, làm mẫu các nội dung căn bản và hướng dẫn sinh viên tự đọc sách và thực hành	- Bài tập thực hành trên máy
Chương 3. **Kỹ thuật mã hoá** 3.1 Giới thiệu 3.2 Khái niệm mã hóa và giải mã 3.3 Kỹ thuật mã hóa khóa bí mật 3.4 Giới thiệu mã hóa DES	Có kiến thức cơ bản về mã hóa, xác thực và các vấn đề liên quan đến an toàn và bảo mật	Giảng viên thuyết trình, làm mẫu các nội dung căn bản và hướng dẫn	- Bài tập thực hành trên máy

3.5 Ưu, nhược điểm của mã hóa đối xứng 3.6 Cơ sở hạ tầng khóa công khai 3.7. Mã khóa công khai RSA (RIVEST-SHAMIR-ADELMAN) 3.8 Các hệ thống lai 3.9 So sánh hệ khóa bí mật và khóa công khai Tham khảo: [][][]	thông tin	sinh viên tự đọc sách và thực hành	
Chương 4. Chữ ký điện tử và chứng chỉ số 4.1 Giới thiệu 4.2 Một số khái niệm cơ bản 4.3 Vấn đề xác thực và chữ kí điện tử 4.4 Hoạt động của một hệ thống chữ kí điện tử 4.5 Phân loại các hệ thống chữ kí điện tử 4.6 Thuật toán chữ kí điện tử DSA 4.7 Giải thuật băm bảo mật SHA 4.8 Chứng chỉ số Tham khảo [][]	Hiểu được chữ ký điện tử và chứng chỉ số. Triển khai được hệ thống.	Giảng viên thuyết trình, làm mẫu các nội dung căn bản và hướng dẫn sinh viên tự đọc sách và thực hành	- Bài tập thực hành trên máy
Chương 5. **Các ứng dụng bảo mật hệ thống thông tin** 5.1 Các giao thức 5.2 Hệ thống xác thực 5.3 Ứng dụng bảo mật trong thanh toán điện tử 5.4 Ứng dụng bảo mật trong SSL Tham khảo [][]	Nắm được các giao dịch an toàn. Cấu hình được hệ thống dung SSL.	Giảng viên thuyết trình, làm mẫu các nội dung căn bản và hướng dẫn sinh viên tự đọc sách và thực hành	- Bài tập thực hành trên máy

3.3 Phân bổ thời gian chi tiết

Nội dung	**Phân bổ số tiết cho hình thức dạy - học**			**Tổng**
	Lên lớp	**Thực hành,**	**Tự**	

	Lý thuyết	Bài tập	Thảo luận	thí nghiệm	nghiên cứu	
Chương 1: **Tổng quan về an toàn thông tin** 1.1 Mở đầu 1.2 Sự cần thiết phải bảo vệ thông tin 1.3 Virus và các biện pháp phòng chống virus 1.4 Các đặc trưng xâm nhập 1.5 Đặc trưng kỹ thuật của an toàn bảo mật Tham khảo [2][3][4][5]	3		1	0		4
Chương 2. **Các lỗ hổng trong bảo mật và các điểm yếu của mạng** 2.1 Giao thức TCP/IP 2.2 Lỗ hổng bảo mật trên Internet 2.3 Một số phương thức tấn công 2.4 Các biện pháp phát hiện hệ thống bị tấn công 2.5 Các biện pháp phòng ngừa Tham khảo: [2][3][4][5]	3	2	1	8		14
Chương 3. **Kỹ thuật mã hoá** 3.1 Giới thiệu 3.2 Khái niệm mã hóa và giải mã 3.3 Kỹ thuật mã hóa khóa bí mật 3.4 Giới thiệu mã hóa DES	6	2	2	8		18

3.5 Ưu, nhược điểm của mã hóa đối xứng 3.6 Cơ sở hạ tầng khóa công khai 3.7. Mã khóa công khai RSA (RIVEST-SHAMIR-ADELMAN) 3.8 Các hệ thống lai 3.9 So sánh hệ khóa bí mật và khóa công khai Tham khảo: [1][2]						
Chương 4. Chữ ký điện tử và chứng chỉ số 4.1 Giới thiệu 4.2 Một số khái niệm cơ bản 4.3 Vấn đề xác thực và chữ kí điện tử 4.4 Hoạt động của một hệ thống chữ kí điện tử 4.5 Phân loại các hệ thống chữ kí điện tử 4.6 Thuật toán chữ kí điện tử DSA 4.7 Giải thuật băm bảo mật SHA 4.8 Chứng chỉ số Tham khảo [1][2]	2	1	1	4		8
Chương 5. **Các ứng dụng bảo mật hệ thống thông tin** 5.1 Các giao thức 5.2 Hệ thống xác thực 5.3 Ứng dụng bảo mật trong thanh toán điện tử	4	1	1	10		16

5.4 Ứng dụng bảo mật trong SSL Tham khảo [1][2][6]						

4. Tài liệu học tập

[1] D. Stinson. Mật mã: lý thuyết và thực hành. Boca Raton, FL: CRC Press, bản dịch 1996, Học viện mật mã.

[2] William Stallings. Cryptography and Network Security: Principles and Practice. Prentice Hall, third edition, 2003.

[3] Andrew S. Tanenbaum, *Computer Networks*, Prentice Hall, New Jersey, Fourth Edition, 2003.

[4] Man Young Rhee, Wilay, *Internet Security - Cryptographic Principles, Algorithms and Protocols,* 2003.

[5] William Stallings, *Network Security Essentials: Applications and Standards*, Prentice Hall, New Jersey, 1999.

[6] Wasim.E. Rajput. *Commerce Systems-Architecture & Application,* 2000.

5. Các hiểu biết, các kỹ năng cần đạt được sau khi học môn học

Có được kiến thức cơ bản về lĩnh vực lập trình mạng và có khả năng viết được các ứng dụng mạng.

6. Hướng dẫn cách đánh giá học phần

Sinh viên phải dự lớp đủ các tiết theo quy định

Đánh giá Kết quả học phần:

+ Điểm chuyên cần : 10%

+ Bài tập : 10%

+ Báo cáo bài tập lớn : 20%

+ Thi cuối học kỳ : 60%

+ Hình thức thi cuối kỳ : Thi tự luận + trắc nghiệm.

7. Danh sách giảng viên dự kiến

- GV giảng dạy lý thuyết:
  + Ths. Đặng Nhân Cách
  + TS. Lê Văn Quốc Anh
-
- Giảng viên trợ giảng:

-
-

- GV dạy thực hành, thí nghiệm
  + Ths. Đặng Nhân Cách
  +TS. Lê Văn Quốc Anh

Tp. Hồ Chí Minh ngày 29 tháng 09 năm 2014

TRƯỞNG KHOA	TRƯỞNG BỘ MÔN	GIẢNG VIÊN LẬP ĐỀ CƯƠNG
PGS.TS. Nguyễn Hữu Khương	Ths. Lê Quốc Tuấn	Ths. Đặng Nhân Cách