TRƯỜNG ĐH GIAO THÔNG VẬN TẢI TP. HỒ CHÍ MINH

KHOA CÔNG NGHỆ THÔNG TIN

BỘ MÔN MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN

1. Tổng quát về học phần

Tên học phần	**Tiếng Việt: AN TOÀN THÔNG TIN** **Tiếng Anh: INFORMATION SECURITY**				**Mã HP: 123033**
Số tín chỉ	**3 TC(2,1,3)**				
Số tiết	LT	BT	TH	Tổng	Tự học
	30	-	30	60	90 giờ
Đánh giá học phần	Quá trình: 40%				Thi cuối kỳ: 60%
Thang điểm	10				
Môn tiên quyết	-				MS:
Môn học trước	-				MS:
Môn song hành	-				MS:

Ghi chú:

- Từ viết tắt: LT: lý thuyết; BT: bài tập; TH thực hành, thí nghiệm, thảo luận; BTN: bài tập nhóm.

- Giờ lý thuyết: 1 tín chỉ = 15 tiết (LT&BT); giờ TH: 1 tín chỉ = 30 tiết; 1TC tự học tối thiểu là 30 giờ.

2. Mô tả học phần

Học phần cung cấp các kiến thức chung về An toàn thông tin như các khái niệm; tầm quan trọng; các nguy cơ đối với An toàn thông tin trong môi trường máy tính song song đó là giải thích các khái niệm; hệ thống lại các kiến thức toán đại số cần thiết cho môn học; một số giải pháp và Bộ tiêu chuẩn đánh giá An toàn thông tin cho cá nhân và tổ chức..

Sinh viên có khả năng áp dụng một số công cụ ứng dụng của Hệ mật mã trên Hệ điều hành máy tính để thiết lập An toàn cho hệ thống thông tin và ứng dụng truyền thông trong môi trường mạng. Đồng thời có khả năng vận dụng kiến thức để phân tích, triển khai, đánh giá giải pháp ATTT cho Hệ thống thông tin.

Thái độ học tập chủ động, tích cực trong việc nắm bắt kiến thức được hướng dẫn, tìm tòi cập nhật kiến thức theo sự phát triển của Công nghệ và chính sách trong nước và quốc tế. Có sự tự tin, lòng nhiệt tình và chuyên nghiệp trong hoạt động nhóm.

3. Tài liệu học tập

3.1. Sách, giáo trình, tài liệu tham khảo

TT	Tên tác giả	Năm XB	Tên sách, giáo trình, tên bài báo, văn bản	NXB, tên tạp chí/ nơi ban hành VB
I	**Tài liệu chính**			

1	TS. Lê Văn Phùng	2018	**An toàn thông tin**	NXB Thông tin và truyền thông
2	Nguyễn Khanh Văn	2014	**Giáo trình Cơ sở An toàn Thông tin**	ĐH BK Hà Nội
II	**Tài liệu tham khảo**			
1	Christof Paar, JanPelzl	2010	**Understanding Cryptography A textbook for Students and Practitioners**	Springer
2	William Stallings	2005	**Cryptography and Network Security Principles and Practices, 4 th Edition**	William Stallings
3	A.Menezes, P.Van Oorschot, SVanstone	1996	**Handbook of Applied Cryptography**	CRC Press

3.2. Danh mục địa chỉ web hữu ích cho HP

TT	Nội dung tham khảo	Link trang web	Ngày cập nhật
1	- Các tiêu chuẩn An toàn thông tin quốc gia (TCVN) và quốc tế (ISO/IEC) - Quy định pháp luật về An toàn thông tin của Việt Nam.	http://tracuu.tcvn.vn/sdomain/front/tieu-chuan-viet-nam Cổng thông tin điện tử tổng cục tiêu chuẩn đo lường chất lượng	12/08/2021
2	- Quy định pháp luật về An toàn thông tin của Việt Nam. - Các giải pháp ATTT	https://ais.gov.vn/ Website của Cục An toàn thông tin – Bộ Thông tin và truyền thông.	12/08/2021

4. Mục tiêu học phần

Mục tiêu [1]	Mô tả **[2]** *Học phần này trang bị cho sinh viên:*	Chuẩn đầu ra CTĐT **[3]**
CO1	Giải thích các khái niệm, vấn đề liên quan đến An toàn thông tin. Phân loại, nhận dạng và thiết lập các thuật toán mã hóa của các hệ Mật mã. Phân tích mô hình hệ thống, các Bộ tiêu chuẩn trong nước và quốc tế, áp dụng giải pháp tăng ATTT cho hệ thống thông tin của Doanh nghiệp.	PLO2
CO2	Lựa chọn mô hình thiết kế, mô hình triển khai Hệ thống thông tin áp dụng các giải pháp công nghệ ứng dụng Hệ mật mã giúp tăng ATTT.	PLO2 PLO5 PLO6

CO3	Thành thạo việc tự học tập, tích lũy và cập nhật kiến thức theo xu thế phát triển của lĩnh vực ATTT. Tích cực trong hoạt động cá nhân hoặc nhóm dưới dạng Bài tập thực hành.	PLO6 PLO7

5. Chuẩn đầu ra học phần

Mục tiêu HP [1]	CĐR HP [2]	Mô tả CĐR [3]	Chuẩn đầu ra CTĐT [4]
CO1	CLO1.1	Giải thích các khái niệm, vấn đề chung liên quan đến An toàn thông tin.	PI2.1
	CLO1.2	Phân loại, nhận dạng và thiết lập các thuật toán mã hóa của các hệ Mật mã.	PI2.2 PI2.3
CO2	CLO2.1	Triển khai các ứng dụng của mật mã vào Xây dựng hệ thống thông tin đảm bảo ATTT.	PI5.1
	CLO2.2	Lựa chọn và thiết kế mô hình Hệ thống thông tin áp dụng các giải pháp công nghệ ứng dụng Hệ mật mã tăng ATTT.	PI2.2
	CLO2.3	Đánh giá Hệ thống thông tin qua bộ tiêu chuẩn ATTT	PI6.2
CO3	CLO3.1	Làm việc độc lập hoặc theo nhóm với các hoạt động và hình thức được qui định	PI6.3
	CLO3.2	Tự học tập, tích lũy và cập nhật kiến thức theo xu thế phát triển của lĩnh vực ATTT.	PI7.1, PI7.2

Ma trận năng lực tích hợp giữa chuẩn đầu ra của học phần và chuẩn đầu ra của chương trình đào tạo:

CLOs	PLO2			PLO5	PLO6		PLO7	
	PI2.1	PI2.2	PI2.3	PI5.1	PI6.2	PI6.3	PI7.1	PI7.2
CLO1.1	3							
CLO1.2		4	3					
CLO2.1				3				
CLO2.2		4						
CLO2.3					5			
CLO3.1						4		
CLO3.2							3	2
Giá trị lớn nhất của năng lực	**3**	**4**	**3**	**3**	**5**	**4**	**3**	**2**

6. Hướng dẫn cách học, chi tiết cách đánh giá môn học

Cách học:

- Sinh viên phải tham dự tối thiểu 80% số tiết của học phần;
- Làm và nộp các bài tập;
- Tự nghiên cứu các vấn đề được giao ở nhà hoặc thư viện;
- Thực hiện đầy đủ các phần thuyết trình của nhóm;

- Tham dự thi kết thúc học phần.

Điểm tổng kết môn học được đánh giá xuyên suốt quá trình học, gồm 2 cột điểm: điểm quá trình (40%) và điểm thi cuối kỳ (60%). Điểm đánh giá:

Thành phần đánh giá [1]	**Dạng bài đánh giá [2]**	**Chuẩn đầu ra học phần (CLOs) [3]**	**Hình thức đánh giá [4]**	**Tiêu chí đánh giá [5]**	**Trọng số [6]**
Đánh giá quá trình.	Bài tập áp dụng, bài tập thực hành	CLO2.1	Căn cứ vào số lượng và nội dung bài tập đã nộp	A1.1	5%
	Bài tập nhóm và thuyết trình	CLO2.2 CLO3.1 CLO3.2	Các đề tài tìm hiểu, triển khai, phân tích, thiết kế mô hình hệ thống sử dụng các ứng dụng Hệ mật.	A1.2	15%
	Kiểm tra giữa kỳ	CLO1.1 CLO1.2	Trắc nghiệm	A1.3	20%
Đánh giá cuối kỳ	Thi trắc nghiệm	CLO1.1 CLO1.2 CLO2.1 CLO2.2 CLO2.3	Trắc nghiệm	A3.1	60%

Ma trận thống kê số lượng câu hỏi, bài tập kiểm tra, đánh giá kết quả học tập được thể hiện trong bảng dưới

Phần – Chương	Bậc 1	Bậc 2	Bậc 3	Bậc 4	Bậc 5
Chương 1: Tổng quan về an toàn thông tin	5	5			
Chương 2. Các lỗ hổng trong bảo mật và các điểm yếu của mạng		5	5		
Chương 3. Kỹ thuật mã hoá.			5	5	5
Chương 4. Chữ ký điện tử và chứng chỉ số.			5	5	5
Chương 5. Các ứng dụng bảo mật hệ thống thông tin			5	5	5
TỔNG	**5**	**10**	**20**	**15**	**15**

Rubric A1.1: Bài tập áp dụng, thực hành

Tiêu chí đánh giá	Mức độ đạt chuẩn quy định					Trọng số
	MỨC 1 (0-3.9)	**MỨC 2 (4.0-5.4)**	**MỨC 3 (5.5-6.9)**	**MỨC 4 (7.0-8.4)**	**MỨC 5 (8.5-10)**	
Thái độ tham dự tích cực	Thực hiện từ dưới 40 số bài tập	Thực hiện từ 40-54% số bài tập	Thực hiện từ 55-69% số bài tập	Thực hiện từ 70-84% số bài tập	Thực hiện từ 85% số bài tập trở lên	30%
Chất lượng bài nộp	Hoàn thành đúng dưới 39% yêu cầu	Hoàn thành đúng từ 40-54% yêu cầu trở lên	Hoàn thành đúng từ 55-69% yêu cầu trở lên	Hoàn thành đúng từ 70-84% yêu cầu trở lên	Hoàn thành đúng 85% yêu cầu trở lên	70%

Rubric A1.2: Bài tập nhóm và thuyết trình

Tiêu chí đánh giá	Mức độ đạt chuẩn quy định					Trọng số
	MỨC 1 (0-3.9)	**MỨC 2 (4.0-5.4)**	**MỨC 3 (5.5-6.9)**	**MỨC 4 (7.0-8.4)**	**MỨC 5 (8.5-10)**	
Nội dung báo cáo	Không đáp ứng yêu cầu tối thiểu.	- Nội dung phù hợp với yêu cầu. - Chưa tìm hiểu rộng các giải thuật, giải pháp … đối	- Nội dung phù hợp với yêu cầu. Sử dụng thuật ngữ đơn giản, dễ hiểu. - Chưa tìm hiểu rộng, so sánh các thuật giải, giải pháp … đối với đối	- Nội dung phù hợp với yêu cầu. Sử dụng thuật ngữ đơn giản, dễ hiểu. - Có tìm hiểu rộng, so sánh các thuật giải, giải	- Nội dung phù hợp với yêu cầu. Sử dụng thuật ngữ đơn giản, dễ hiểu. - Có tìm hiểu rộng, phân tích, so sánh các thuật	**30%**

		với đối tượng tìm hiểu. - Minh họa và giải thích chưa rõ ràng.	tượng tìm hiểu. - Minh họa, demo và giải thích rõ ràng.	pháp … đối với đối tượng tìm hiểu. - Minh họa, demo và giải thích rõ ràng.	giải, giải pháp … đối với đối tượng tìm hiểu. - Minh họa, demo và giải thích rõ ràng phong phú phương thức.	
Làm việc nhóm	Dưới 50% thành viên tham gia thực hiện/trình bày.	Từ 50% thành viên tham gia thực hiện/trình bày.	Từ 60% thành viên tham gia thực hiện/trình bày.	Từ 80% thành viên tham gia thực hiện/trình bày.	100% thành viên tham gia thực hiện/trình bày.	**10%**
Kỹ năng thuyết trình	Nói nhỏ, không tự tin, không tương tác với người nghe.	Nói không rõ lời, thiếu tự tin, ít tương tác với người nghe.	Nói rõ ràng, tự tin, nhưng tương tác chưa tốt với người nghe.	Nói rõ ràng, tự tin và tương tác tốt với người nghe.	Nói rõ ràng, tự tin, mạch lạc, thu hút sự chú ý của người nghe, tương tác tốt với người nghe.	**30%**
Tham gia thảo luận	Trả lời đúng dưới 50% số câu hỏi của GV. Không tham gia thảo luận với bài làm nhóm khác	Trả lời đúng từ 50% số câu hỏi của GV. Không tham gia thảo luận với bài làm nhóm khác	Trả lời đúng từ 60% số câu hỏi của GV. Tham gia thảo luận với bài làm nhóm khác với 1-2 câu hỏi.	Trả lời đúng từ 75% số câu hỏi của GV. Tham gia thảo luận với bài làm nhóm khác với 1-2 câu hỏi.	Trả lời đúng tất cả các câu hỏi của GV. Tham gia tranh luận với bài làm nhóm khác về nội dung trình bày của nhóm đó.	**30%**

Rubric A1.3: Kiểm tra giữa kỳ

Tiêu chí đánh giá	**Mức độ đạt chuẩn quy định**					**Trọng số**
	MỨC 1 (0-3.9)	**MỨC 2 (4.0-5.4)**	**MỨC 3 (5.5-6.9)**	**MỨC 4 (7.0-8.4)**	**MỨC 5 (8.5-10)**	
Trả lời đúng câu hỏi trắc nghiệm	Hoàn thành đúng dưới 39% yêu cầu	Hoàn thành đúng từ 40-54% yêu cầu trở lên	Hoàn thành đúng từ 55-69% yêu cầu trở lên	Hoàn thành đúng từ 70-84% yêu cầu trở lên	Hoàn thành đúng 85% yêu cầu trở lên	100%

Rubric A2.1: Trắc nghiệm cuối kỳ

	Mức độ đạt chuẩn quy định	**Trọng số**

Tiêu chí đánh giá	MỨC 1 (0-3.9)	MỨC 2 (4.0-5.4)	MỨC 3 (5.5-6.9)	MỨC 4 (7.0-8.4)	MỨC 5 (8.5-10)	
Số câu trả lời đúng	Hoàn thành đúng dưới 39% yêu cầu	Hoàn thành đúng từ 40-54% yêu cầu trở lên	Hoàn thành đúng từ 55-69% yêu cầu trở lên	Hoàn thành đúng từ 70-84% yêu cầu trở lên	Hoàn thành đúng 85% yêu cầu trở lên	100%

7. Dự kiến danh sách cán bộ tham gia giảng dạy

STT [1]	Họ và tên [2]	Email [3]	Đơn vị công tác [4]
1.	ThS. Trần Đức Doanh	doanhtd@ut.edu.vn	Khoa CNTT – UT
2.	ThS. Bùi Dương Thế	duongthe@ut.edu.vn	Khoa CNTT – UT
3.	ThS. Nguyễn Duy Hiếu	hieu.nguyen@ut.edu.vn	Khoa CNTT – UT
4.	ThS. Hồ Đăng Thế	the.ho@ut.edu.vn	Trung tâm DITC – UT

8. Phân bố thời gian chi tiết

Nội dung	PP giảng dạy	Phân bổ số tiết cho hình thức dạy - học				Tổng số tiết trên lớp
		Lên lớp		TH	Tự học (giờ)	
		LT	BT			
Phần						
Chương 1 - Tổng quan về an toàn thông tin 1.1. Kiến thức chung về ATTT 1.2. Các đặc trưng về kỹ thuật ATTT 1.3. Bộ tiêu chuẩn ATTT 1.4. An toàn thông tin cá nhân.	Phương pháp dạy học thuyết minh, giải thích, đặt và định hướng giải quyết vấn đề	4			12	**4**
Chương 2 – Các lỗ hổng trong bảo mật và các điểm yếu của mạng 2.1. Giới thiệu chung 2.2. Lỗ hổng hệ điều hành 2.3. Lỗ hổng giao thức truyền thông. 2.4. Các biện pháp phát hiện và phòng chống tấn công HTTT	Phương pháp dạy học thuyết minh, giải thích, đặt và định hướng giải quyết vấn đề	4		4	18	**8**
Chương 3 – Kỹ thuật mã hóa 3.1. Tổng quan về Mật mã và Các kỹ thuật giấu tin 3.2. Cơ sở toán học 3.3. Mã hóa cổ điển 3.4. Mã hóa hiện đại	Phương pháp dạy học thuyết minh, giải thích, minh họa.	8	2	10	25	**20**
Chương 4 – Chữ ký điện tử và chứng chỉ số 4.1. Tổng quan về Chữ ký điện tử và Chứng chỉ Số 4.2. Thuật toán chữ kí điện tử DSA, RSA, Elgamal, DSS, ECDSA 4.3. Hàm băm bảo mật 4.4. Chứng chỉ số - Hệ thống xác thực.	Phương pháp dạy học thuyết minh, giải thích, đặt và giải quyết vấn đề	4	2	10	20	**16**
Chương 5 – Các ứng dụng bảo mật hệ thống thông tin sử dụng Kỹ thuật mã hóa		5	1	6	15	**12**

Nội dung	PP giảng dạy	Phân bổ số tiết cho hình thức dạy - học				Tổng số tiết trên lớp
		Lên lớp		TH	Tự học (giờ)	
		LT	BT			
5.1. Giao thức SSL/TLS 5.2. Giao thức IPSec. 5.3. Firewall, VPN	Phương pháp dạy học thuyết minh, giải thích, đặt và giải quyết vấn đề					

9. Nội dung chi tiết

Tuần / Chương	Nội dung	CLOs	Hoạt động dạy và học	Dạng bài đánh giá	Tài liệu học tập
Tuần 1/Chương 1	**Lý thuyết:** Chương 1: Tổng quan về an toàn thông tin 1.1. Kiến thức chung về ATTT - Các đặc trưng xâm nhập. - Yếu tố con người trong ATTT 1.2. Các đặc trưng về kỹ thuật ATTT 1.3. Bộ tiêu chuẩn ATTT - TCVN ISO/IEC 27XXX - ISO/IEC 27XXX 1.4. An toàn thông tin cá nhân. **Thực hành:** Thực hiện các biện pháp tăng an toàn máy tính cá nhân.	CLO1.1 CLO1.2	**Thầy, Cô:** - Giới thiệu thông tin về Thầy, Cô. - Các vấn đề liên quan đến môn học. - Cách thức dạy và học - Giới thiệu lướt qua đề cương môn học. - Nhắc gợi nhớ lại các khái niệm, các thuật ngữ về thông tin, dữ liệu, an toàn bảo mật hệ thống mạng,… mà sinh viên đã được học từ các môn học trước. - Giảng các slide cho chương 1 **Sinh viên:** - Thảo luận về các nội dung của bài giảng. - Thảo luận, so sánh, đánh giá một cách tổng quan - Làm bài tập cá nhân.	A1.1 A1.3 A2.1	Chương mở đầu Tài liệu[1] Chương 1, Tài liệu[2]
Tuần 2-3/Chương 2	**Lý thuyết:** Chương 2. Các lỗ hổng trong bảo mật và các điểm yếu của mạng 2.1. Kiến thức chung về Lỗ hổng 2.2. Lỗ hổng hệ điều hành	CLO1.1 CLO1.2 CLO2.1 CLO2.2 CLO2.3	**Thầy, Cô:** - Giảng các slide chương 2	A1.1 A1.2 A1.3 A2.1	Chương mở đầu Tài liệu[1] Chương 1, Tài liệu[2]

Tuần / Chương	Nội dung	CLOs	Hoạt động dạy và học	Dạng bài đánh giá	Tài liệu học tập
	2.3. Lỗ hổng giao thức truyền thông. 2.4. Các biện pháp phát hiện và phòng chống tấn công HTTT **Thực hành:** 1. Thực hành Sniffing 2. Xây dựng mô hình Bảo mật mạng cho HTTT và Chính sách ATTT cho Doanh nghiệp. 3. Phương thức tấn công SQL injection, DOS, DDOS		- Đưa ra thảo luận các vấn đề liên quan trong thực tế **Sinh viên:** - Thảo luận về nội dung bài giảng. - Đưa ra thảo luận các vấn đề liên quan trong thực tế. - Làm bài tập cá nhân về nhà		
Tuần 4-8/Chương 3	Chương 3. Kỹ thuật mã hoá. 3.1. Tổng quan về Mật mã và Các kỹ thuật giấu tin 3.2. Cơ sở toán học 3.3. Mã hóa cổ điển 3.4. Mã hóa hiện đại - Cơ sở hạ tầng khóa công khai. - Các chế độ mã hóa. - Các hệ thống lai. **Thực hành:** Bài tập vận dụng các Hệ mật. Hiện thực các giải thuật Euclid, Euclid mở rộng, xét số nguyên tố. Viết chương trình các Hệ mật: Hill, Virgenere, DES, DSA, RSA, Mã dòng ... mã hóa dữ liệu gửi qua môi trường Mạng máy tính. Một số phương thức tấn công hệ mật. Sử dụng công cụ Cryptool để hiểu và phân tích hoạt động của các Hệ mật.	CLO1.1 CLO1.2 CLO2.1 CLO2.2 CLO2.3	**Thầy, Cô:** - Giảng các slide chương 3 - Đưa ra các bài tập ứng dụng cho từng loài hệ mật. - Đưa ra các thảo luận về hệ mật trong thực tế, các phương pháp tấn công hệ mật. **Sinh viên:** - Thảo luận các vấn đề được GV đưa ra. - Tìm hiểu về các loại hệ mật tương ứng khác ngoài các hệ mật đã được giới thiệu trong các phân loại hệ mật. - Làm các bài tập cá nhân và bài tập nhóm.	A1.1 A1.2 A1.3 A2.1	Chương 2, Tài liệu[1] Chương 2,3,4 Tài liệu[2]

Tuần / Chương	Nội dung	CLOs	Hoạt động dạy và học	Dạng bài đánh giá	Tài liệu học tập
Tuần 9-12/Chương 4	**Lý thuyết:** Chương 4. Chữ ký điện tử và chứng chỉ số. 4.1. Tổng quan về Chữ ký điện tử và Chứng chỉ Số 4.2. Thuật toán chữ kí điện tử DSA, RSA, Elgamal, DSS, ECDSA 4.3. Hàm băm bảo mật 4.4. Chứng chỉ số - Hệ thống xác thực. **Thực hành:** - Triển khai mô hình mạng có server xác thực (CA). - Hiện thực chữ ký điện tử DSA, RSA	CLO1.1 CLO1.2 CLO2.1 CLO2.2 CLO2.3	**Thầy, Cô:** - Giảng các slide chương 4 - Đưa ra thảo luận các vấn đề liên quan trong thực tế **Sinh viên:** - Thảo luận về nội dung bài giảng. - Đưa ra thảo luận các vấn đề liên quan trong thực tế - Làm bài tập cá nhân và bài tập nhóm - Báo cáo đồ án môn học.	A1.1 A1.2 A1.3 A2.1	Chương 4,5, Tài liệu[1] Chương 5,6,7 Tài liệu[2]
Tuần 13-15/Chương 5	**Lý thuyết:** Chương 5. Các ứng dụng bảo mật hệ thống thông tin 5.1. Giao thức SSL/TLS 5.2. Giao thức IPSec. 5.3. Firewall, VPN **Thực hành:** - Triển khai SSL/TLS cho website - Xây dựng hệ thống Kaberos	CLO1.1 CLO1.2 CLO2.1 CLO2.2 CLO2.3	**Thầy, Cô:** - Giảng các slide chương 4 - Đưa ra thảo luận các vấn đề liên quan trong thực tế **Sinh viên:** - Thảo luận về nội dung bài giảng. - Đưa ra thảo luận các vấn đề liên quan trong thực tế - Làm bài tập cá nhân và bài tập nhóm - Báo cáo đồ án môn học.	A1.1 A1.2 A1.3 A2.1	Chương 6,8, Tài liệu[1]

10. Hướng dẫn tự học

Tuần/ Buổi học/ [1]	Nội dung [2]	CĐR học phần [3]	Hoạt động tự học của SV [4]
Tuần 1/ Chương 1 Tổng quan về an toàn thông tin	- Các đặc trưng xâm nhập HTTT - Các đặc trưng của kỹ thuật ATTT - Bộ tiêu chuẩn ATTT - An toàn thông tin máy tính cá nhân	CLO1.1 CLO1.2	- Đọc tài liệu của chương, tài liệu tham khảo về các Bộ tiêu chuẩn ATTT TCVN ISO/IEC 27xxx, ISO/IEC 27xxx - Liên hệ các kiến thức đã học: Mạng căn bản, Quản trị mạng, An ninh mạng - Làm bài tập đảm bảo ATTT cá nhân.
Tuần 2/ Chương 2 Các lỗ hổng trong bảo mật và các điểm yếu của mạng	- Kiến thức chung về lỗ hổng bảo mật - Lỗ hổng hệ điều hành	CLO1.1 CLO1.2 CLO2.1 CLO2.2 CLO2.3	- Đọc tài liệu của chương - Liên hệ các vấn đề liên quan trong thực tế về các lỗ hổng bảo mật đã được công bố và bản vá. - Làm bài tập cá nhân và bài tập nhóm. - Đọc Tài liệu [1] Trang 19 - 31
Tuần 3/ Chương 2 Các lỗ hổng trong bảo mật và các điểm yếu của mạng	- Lỗ hổng giao thức. - Lỗ hổng thiết lập và quản trị hệ thống thông tin. - Các biện pháp phát hiện và phòng chống tấn công HTTT.	CLO1.1 CLO1.2 CLO2.1 CLO2.2 CLO2.3	- Đọc tài liệu của chương - Sử dụng các công cụ thăm dò, nghe lén, xâm nhập hệ thống máy tính và mạng. - Làm bài tập cá nhân và bài tập nhóm. - Đọc Tài liệu [1] Trang 19 – 31 - Đọc Tài liệu [2] Trang 155 - 171
Tuần 4/ Chương 3 Kỹ thuật mã hóa	Giới thiệu. - Kiến thức chung về kỹ thuật mật mã - Cơ sở toán học - Mã hóa cổ điển: Mã dịch vòng, Mã hóa thay thế	CLO1.1 CLO1.2 CLO2.1 CLO2.2 CLO2.3	- Đọc tài liệu của chương, nắm được các kiến thức chung về kỹ thuật mật mã. - Củng cố lại kiến thức toán học cơ sở: modulo, cấu trúc đại số, giải thuật Euclid, Eclid mở rộng, Định lý Fermat, định lý phần dư Trung hoa. - Làm bài tập cá nhân. - Đọc Tài liệu [1] Trang 45 - 96
Tuần 5/ Chương 3 Kỹ thuật mã hóa	- Mã hóa cổ điển: Mã chuyển vị, mã hóa dòng	CLO1.1 CLO1.2 CLO2.1 CLO2.2 CLO2.3	- Đọc tài liệu của chương - Làm bài tập áp dụng các hệ mã hóa cổ điển: chuyển vị, thay thế, mã hóa dòng. - Đọc Tài liệu [1] Trang 129 - 165

Tuần/ Buổi học/ [1]	Nội dung [2]	CĐR học phần [3]	Hoạt động tự học của SV [4]
Tuần 6/ Chương 3 Kỹ thuật mã hóa	- Kiến thức chung Mã hóa hiện đại. - Kiến trúc mã Feistel - Mã hóa DES	CLO1.1 CLO1.2 CLO2.1 CLO2.2 CLO2.3	- Đọc tài liệu của chương - Hệ thống lại Mã hóa khóa bí mật và Mã hóa khóa công khai, kiến trúc Feistel, các chế độ mã hóa. - Tìm kiếm và đọc các tài liệu về 2DES, 3DES; thám mã các hệ mật DES. - Tìm hiểu và viết chương trình các Hệ mật: DES, áp dụng vào việc mã hóa dữ liệu truyền thông qua môi trường Mạng máy tính. - Đọc Tài liệu [1] Trang 129 - 165
Tuần 7/ Chương 3 Kỹ thuật mã hóa	- Mã hóa AES - Ưu, nhược điểm của mã hóa đối xứng. - Cơ sở hạ tầng khóa công khai.	CLO1.1 CLO1.2 CLO2.1 CLO2.2 CLO2.3	- Đọc tài liệu của chương - Kiến thức toán về vành elliptic, giải thuật trao đổi khóa Diffie-Hellman .. - Tìm kiếm và đọc các tài liệu về thám mã các hệ mật AES. - Tìm hiểu và viết chương trình các Hệ mật, AES… áp dụng vào việc mã hóa dữ liệu truyền thông qua môi trường Mạng máy tính. - Đọc Tài liệu [1] Trang 129 - 165
Tuần 8/ Chương 3 Kỹ thuật mã hóa	- Mã hóa khóa công khai RSA (RIVEST - SHAMIR - ADELMAN) - Hệ mật Elgamal, EEC - Các hệ thống lai.	CLO1.1 CLO1.2 CLO2.1 CLO2.2 CLO2.3	- Đọc tài liệu của chương - Kiến thức toán về vành elliptic, giải thuật trao đổi khóa Diffie-Hellman .. - Hệ thống lại kiến thức về Cơ sở hạ tầng khóa công khai, và các hệ thống lai, Hệ mật RSA, Elgamal, EEC … - Đọc Tài liệu [1] Trang 168 - 185
Tuần 9/ Chương 4 Chữ ký điện tử và chứng chỉ số	- Tổng quan về Chữ ký điện tử - Vấn đề xác thực thông tin và chữ ký điện tử - Hoạt động của một hệ thống chữ kí điện tử - Phân loại các hệ thống chữ kí điện tử	CLO1.1 CLO1.2 CLO2.1 CLO2.2 CLO2.3	- Đọc tài liệu của chương - Tìm kiếm và đọc tài liệu của các thuật toán chữ ký điện tử đã giới thiệu và hiện trạng áp dụng trong thực tế tại Việt Nam và Quốc tế. - Làm bài tập nhóm - Đọc Tài liệu [1] Trang 186 - 189

Tuần/ Buổi học/ [1]	Nội dung [2]	CĐR học phần [3]	Hoạt động tự học của SV [4]
Tuần 10 /Chương 4 Chữ ký điện tử và chứng chỉ số	- Thuật toán chữ kí điện tử DSA DSA, RSA, Elgamal, DSS, ECDSA. - Báo cáo bài tập nhóm	CLO1.1 CLO1.2 CLO2.1 CLO2.2 CLO2.3 CLO3.1	- Đọc tài liệu của chương - Hệ thống lại các thuật toán. - Làm bài tập cá nhân và bài tập nhóm - Đọc Tài liệu [1] Trang 190 - 213
Tuần 11/ Chương 4 Chữ ký điện tử và chứng chỉ số	- Hàm băm bảo mật - Giải thuật băm bảo mật SHA, MD5 - Báo cáo bài tập nhóm	CLO1.1 CLO1.2 CLO2.1 CLO2.2 CLO2.3 CLO3.1	- Đọc tài liệu của chương - Nắm được kiến thức về Hàm băm bảo mật, và giải thuật hàm băm SHA,MDx - Làm bài tập nhóm - Đọc Tài liệu [1] Trang 214 - 228
Tuần 12/ Chương 4 Chữ ký điện tử và chứng chỉ số	- Kiến thức chung về Chứng chỉ số - Hệ thống xác thực. - Báo cáo bài tập nhóm	CLO1.1 CLO1.2 CLO2.1 CLO2.2 CLO2.3 CLO3.1	- Đọc tài liệu của chương - Tìm hiểu hệ thống xác thực, triển khai trên hệ thống local và đăng ký tại các đơn vị cung cấp dịch vụ. - Làm bài tập nhóm - Đọc Tài liệu [1] Trang 230 - 251
Tuần 13/ Chương 5 Các ứng dụng bảo mật hệ thống thông tin sử dụng Kỹ thuật mã hóa	- Giao thức SSL/TLS - Báo cáo bài tập nhóm	CLO1.1 CLO1.2 CLO2.3 CLO3.1 CLO3.2	- Đọc tài liệu của chương - Tìm kiếm và đọc tài liệu về ứng dụng của Hệ mật mã trong các giao thức, ưu nhược điểm, phạm vi ứng dụng. - Làm bài bài tập nhóm - Đọc Tài liệu [2] Trang 155 - 171
Tuần 14/ Chương 5 Các ứng dụng bảo mật hệ thống thông tin sử dụng Kỹ thuật mã hóa	- Giao thức IPSec - Báo cáo bài tập nhóm	CLO1.1 CLO1.2 CLO2.3 CLO3.1 CLO3.2	- Đọc tài liệu của chương - Tìm kiếm và đọc tài liệu về ứng dụng của giao thức IPSec, ưu nhược điểm, phạm vi ứng dụng. - Làm bài tập nhóm - Đọc Tài liệu [2] Trang 155 - 171
Tuần 15/ Chương 5 Các ứng dụng bảo mật hệ thống thông tin sử dụng Kỹ thuật mã hóa	- Các ứng dụng: Firewall, VPN - Báo cáo bài tập nhóm	CLO2.1 CLO2.2 CLO2.3 CLO3.1 CLO3.2	- Đọc tài liệu của chương - Tìm kiếm và đọc tài liệu về các ứng dụng của Hệ mật mã trong Hệ thống thông tin trên thực tế. - Làm bài tập nhóm - Đọc Tài liệu [2] Trang 155 - 171

11. Hướng dẫn thực hiện

- Phạm vi áp dụng: Ngành Mạng máy tính và Truyền thông khoa CNTT

- Giảng viên: Sử dụng đề cương học phần tổng quát này làm cơ sở phục vụ giảng dạy, biên soạn bộ đề thi, kiểm tra, đánh giá hoạt động học tập của sinh viên.

- Sinh viên: Sử dụng đề cương học phần tổng quát này làm cơ sở để biết các thông tin chi tiết về học phần, từ đó xác định nội dung học tập và chủ động lên kế hoạch học tập phù hợp nhằm đạt được chuẩn đầu ra của học phần.

Đề cương chi tiết học phần được ban hành kèm theo chương trình đào tạo và công bố đến các bên liên quan theo quy định.

TRƯỞNG KHOA	TRƯỞNG BỘ MÔN	CB LẬP ĐỀ CƯƠNG
TS. Lê Văn Quốc Anh	**ThS.Trần Đức Doanh**	**ThS.Trần Đức Doanh**

CÂU HỎI TỰ HỌC, ÔN TẬP, KIỂM TRA, ĐÁNH GIÁ

1. Nội dung câu hỏi. (Phần x – Chương y)