TRƯỜNG ĐẠI HỌC
CÔNG NGHỆ VÀ QUẢN LÝ HỮU NGHỊ
KHOA: CÔNG NGHỆ THÔNG TIN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

Hà Nội, ngày 05 tháng 6 năm 2024

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN
AN TOÀN VÀ BẢO MẬT THÔNG TIN

1. Thông tin chung về học phần

1.1. Tên học phần: A**n toàn và bảo mật thông tin**

Mã học phần: IT00082

1.2. Số tín chỉ: 3

1.3. Bộ môn phụ trách: Khoa học máy tính, Khoa Công nghệ thông tin

1.4. Tên giảng viên đảm nhận giảng dạy:

TT	Học hàm, học vị, họ tên	Số điện thoại	Email	Ghi chú
1	ThS. Nguyễn Viết Huy	0979776427	huyvt@utm.edu.vn	
2	ThS. Lê Khắc Lưu	0987754050	khacluu@utm.edu.vn	
3	ThS. Trần Thị Thu Phương	0766110996	phuongtt@ utm.edu.vn	
4	ThS. Đỗ Thành Công	0987509112	congdt@utm.edu.vn	
5	ThS. Đỗ Thị Thanh Nga	0889393126	ngadt@utm.edu.vn	
6	ThS. Lê Văn Ba	0969919101	balv@utm.edu.vn	

1.5. Loại học phần: Tự chọn

1.6. Điều kiện tiên quyết:

1.7. Phân bổ thời gian:

+ Lý thuyết: 30 tiết
+ Thực hành, Semina: 30 tiết
+ Tự học: 90 giờ
+ Hoạt động khác:

2. Mục tiêu học phần

2.1. Mục tiêu chung của học phần

Học phần An toàn và bảo mật thông tin nhằm cung cấp cho sinh viên những kiến thức nền tảng và có hệ thống về các nguyên lý, kỹ thuật và công nghệ bảo vệ thông tin trong môi trường máy tính và mạng. Sau khi hoàn thành học phần, sinh viên có thể nhận diện được các mối đe dọa an ninh, phân tích các kỹ thuật tấn công phổ biến, áp dụng các thuật toán mật mã cổ điển và hiện đại để mã hóa, xác thực và đảm bảo tính toàn vẹn dữ liệu, đồng thời hiểu và sử dụng được các mô hình, công cụ bảo mật trong thực tế như tường lửa, chữ ký số, mã hóa khóa công khai và bảo mật web/email.

2.2. Mục tiêu cụ thể của học phần

Mã mục tiêu	Mô tả mục tiêu	Ghi chú
G1	Trình bày được các nguyên lý bảo mật thông tin: tính bí mật, toàn vẹn, xác thực, không chối bỏ. Phân tích được các kiểu tấn công, phần mềm độc hại, mô hình an toàn mạng và các kỹ thuật bảo vệ hệ thống.	PLO5
G2	Áp dụng các kỹ thuật mã hóa/hàm băm trong phân tích và bảo vệ dữ liệu. Thực hiện các thao tác kiểm tra tính toàn vẹn, xác thực và phân phối khóa trong mô hình mạng bảo mật.	PLO9
G3	Thực hiện công việc với tinh thần cam kết cao, hình thành đạo đức nghề nghiệp, tuân thủ pháp luật và tinh thần trách nhiệm cao.	PLO15

3. Chuẩn đầu ra của học phần

Mục tiêu học phần	CĐR HP (CLO)	Mô tả chuẩn đầu ra *Sau khi học xong học phần này, người học có thể:*	CĐR CTĐT (PLO)	Mức độ đóng góp của CLO vào PLO
a. Về kiến thức	**CLO1**	Trình bày được các nguyên lý và thuật ngữ cơ bản trong bảo mật thông tin.	**PLO5**	**3**
	CLO2	Phân tích được các mối đe dọa, phương pháp tấn công và cơ chế phòng thủ.	**PLO5**	**3**
	CLO3	Áp dụng được các thuật toán mật mã cổ điển và hiện đại trong bài toán thực tế.	**PLO5**	**3**
b.Về kỹ năng	**CLO4**	Vận dụng phối hợp tốt giữa thiết lập cơ chế bảo mật và an toàn dữ liệu trong giao dịch thương mại điện tử. Vận dụng tốt các phần mềm diệt Virus, có kĩ năng phát hiện và loại bỏ phần mềm có hại.	**PLO9**	**3**
	CLO5	Giải thích và triển khai được các kỹ thuật bảo mật hệ thống và truyền thông.	**PLO9**	**3**
	CLO6	Vận dụng thành thạo cài đặt được các thuật toán mã hóa dữ liệu đơn giản. Thiết lập được cơ chế bảo mật an ninh mạng.	**PLO9**	**3**
c.Về tự chủ và trách nhiệm	**CLO7**	Có thái độ tích cực với việc học tập, nhận thức được tầm quan trọng của việc tự học và phát triển bản thân trong suốt sự nghiệp.	**PLO13**	**3**
	CLO8	Có khả năng vận dụng hiệu quả các kiến thức và công nghệ mới để giải quyết các vấn đề thực tế, tối ưu hóa quy trình phát triển bảo trì phần mềm và đề xuất giải pháp sáng tạo.	**PLO14**	**3**

5. Nội dung chi tiết học phần

Nội dung *(Ghi chi tiết từng chương, mục)*	Đáp ứng CĐR của học phần	**Phân bổ thời lượng cho các hoạt động giảng dạy và học tập**			
		Thời lượng giảng dạy (Tiết)			Thời gian sinh viên tự học (Giờ)
		Lý thuyết	Seminar	Thực hành / Thực tập	
(1)	(2)	(3)	(4)	(5)	(6)
Chương 1: Tổng quan về bảo mật **1.1 Giới thiệu chung về bảo mật thông tin** 1.1.1 Mở đầu về bảo mật thông tin 1.1.2 Nguy cơ và các hiểm họa đối với hệ thống thông tin 1.1.3 Phân loại tấn công phá hoại an toàn **1.2 Dịch vụ cơ chế tấn công** 1.2.1 Các dịch vụ an toàn 1.2.2 Các cơ chế an toàn 1.2.3 Tấn công phá hoại an ninh **1.3 Mô hình an toàn mạng** **1.4 Bảo mật thông tin trong hệ cơ sở dữ liệu** 1.4.1 Giới thiệu chung 1.4.2 Một số mô hình bảo mật cơ sở dữ liệu 1.4.3 Sơ lược kiến trúc của 1 hệ bảo mật CSDL	CLO1	4		3	30

Nội dung *(Ghi chi tiết từng chương, mục)*	Đáp ứng CĐR của học phần	**Phân bổ thời lượng cho các hoạt động giảng dạy và học tập**			
		Thời lượng giảng dạy (Tiết)			Thời gian sinh viên tự học (Giờ)
		Lý thuyết	Seminar	Thực hành / Thực tập	
(1)	(2)	(3)	(4)	(5)	(6)
Chương 2: Kẻ xâm nhập, phần mềm có hại và tường lửa **2.1 Kẻ xâm nhập** 2.1.1 Khái niệm 2.1.2 Các kỹ thuật xâm phạm 2.1.3 Đoán mật khẩu 2.1.4 Phát hiện xâm nhập 2.1.5 Quản trị mật khẩu **2.2 Phần mềm có hại** 2.2.1 Các kiểu phần mềm có hại khác ngoài Virus 2.2.2 Virus 2.2.3 Phần mềm ngăn chặn hành vi 2.3 **Tràn bộ đệm** 2.3.1 Ví dụ tràn bộ nhớ 2.3.2 Tấn công tràn bộ nhớ 2.3.3 Code che đậy (Shellcode) 2.3.4 Bảo vệ tràn bộ nhớ **2.4 Bức tường lửa** 2.4.1 Mở đầu 2.4.2 Bức tường lửa – các lọc gói 2.4.3 Bức tường lửa – cổng giao tiếp ở tầng ứng dụng (hoặc proxy)	CLO2 CLO5 CLO8	4		2	25

Nội dung *(Ghi chi tiết từng chương, mục)*	Đáp ứng CĐR của học phần	**Phân bổ thời lượng cho các hoạt động giảng dạy và học tập**			
		Thời lượng giảng dạy (Tiết)			Thời gian sinh viên tự học (Giờ)
		Lý thuyết	Seminar	Thực hành / Thực tập	
(1)	(2)	(3)	(4)	(5)	(6)
2.4.4 Bức tường lửa - cổng giao tiếp mức mạch vòng 2.4.5 Máy chủ Bastion 2.4.6 Kiểm soát truy cập 2.4.7 Các hệ thống máy tính tin cậy 2.4.8 Mô hình Bell LaPadula 2.4.9 Tiêu chuẩn chung dữ liệu **2.5. Các Phương Pháp Tấn Công** **2.6. Các Phương Pháp Tấn Công web.**					
Chương 3: Mã cổ điển **2.1 Mã đối xứng** 3.1.1 Các khái niệm cơ bản 3.1.2 Các yêu cầu 3.1.3 Mật mã 3.1.4 Thám mã 3.1.5 Tìm duyệt tổng thể (Brute-Force) 3.1.6 Độ an toàn **3.2 Các mã thế cổ điển thay thế** 3.2.1 Mã Ceasar 3.2.2 Các mã bảng chữ đơn 3.2.3 Mã playfair 3.2.4 Các mã đa bảng	CLO1 CLO3 CLO2 CLO5 CLO8	4		3	35

Nội dung *(Ghi chi tiết từng chương, mục)*	Đáp ứng CĐR của học phần	**Phân bổ thời lượng cho các hoạt động giảng dạy và học tập**			
		Thời lượng giảng dạy (Tiết)			Thời gian sinh viên tự học (Giờ)
		Lý thuyết	Seminar	Thực hành / Thực tập	
(1)	(2)	(3)	(4)	(5)	(6)
3.2.5 Mã Vigenere 3.2.6 Phương pháp thám mã Kasiski **3.3 Các mã thế cổ điển hoán vị** 3.3.1 Mã Rail Fence 3.3.2 Mã tích **3.4 Một số vấn đề khác** 3.4.1 Máy quay 3.4.2 Dấu tin					
Chương 4: Cơ sở toán học **4.1 Số học trên Modulo** 4.1.1 Định nghĩa Modulo 4.1.2 Các phép toán số học trên Modulo	CLO2 CLO3	4		2	25
Chương 5: HÀM HASH **5.1. Tổng quan về hàm Hash** **5.2. Hàm băm MD4** **5.3. Hàm băm MD5** **5.4. Hàm băm SHS** **5.5. Hàm băm SHA** **5.6. Xây dựng hàm băm trên cơ sở mật mã đối xứng**	CLO2 CLO3 CLO4 CLO6 CLO7 CLO8	4		8	30

Nội dung *(Ghi chi tiết từng chương, mục)*	Đáp ứng CĐR của học phần	**Phân bổ thời lượng cho các hoạt động giảng dạy và học tập**			
		Thời lượng giảng dạy (Tiết)			Thời gian sinh viên tự học (Giờ)
		Lý thuyết	Seminar	Thực hành / Thực tập	
(1)	(2)	(3)	(4)	(5)	(6)
5.7. Tấn công hàm Hash theo kiểu ngày sinh nhật					
Thảo luận trên lớp, Kiểm tra giữa kỳ	CLO2	0		5	
Chương 6: Mã khóa công khai và quản lý khóa. **6.1 Mã công khai** 6.1.1 Mã khoá công khai 6.1.2 Tại sao lại phải dùng mã khoá công khai 6.1. 3 Các đặc trưng của khoá công khai 6.1.4 Ứng dụng khoá công khai **6.2 RSA** 6.2.1 Khởi tạo khoá RSA 6.2.2 Sử dụng RSA 6.2.3 Lũy thừa 6.2.4 Mã hiệu quả 6.2.5 Giải mã hiệu quả 6.2.6 Sinh khoá RSA	CLO2 CLO4 CLO6 CLO7 CLO8	5		5	35

Nội dung *(Ghi chi tiết từng chương, mục)*	Đáp ứng CĐR của học phần	**Phân bổ thời lượng cho các hoạt động giảng dạy và học tập**			
		Thời lượng giảng dạy (Tiết)			Thời gian sinh viên tự học (Giờ)
		Lý thuyết	Seminar	Thực hành / Thực tập	
(1)	(2)	(3)	(4)	(5)	(6)
6.2.7 An toàn của RSA **6.3 Quản lý khóa – Chữ ký điện tử** 6.3.1 Phân phối khoá 6.3.2 Phân phối khoá công khai 6.3.3 Phân phối công khai các khoá mật 6.3.4 Trao đổi khoá hỗn hợp **6.4 Phân phối khóa Diffie -Helman** 6.4.1 Yêu cầu 6.4.2 Khởi tạo Diffie Hellman 6.4.3 Trao đổi khoá Diffie Hellman					
Chương 7: An toàn IP và Web **7.1 An toàn IP** 7.1.1 IPSec 7.1.2 Kiến trúc an toàn IP 7.2 **An toàn Web** 7.2.1 Khái niệm 7.2.2 SSL (Secure Socket Layer) 7.2.3 Kiến trúc SSL **7.3.3 Thanh toán điện tử an toàn** 7.3.1 Yêu cầu	CLO2 CLO4 CLO5 CLO6 CLO7 CLO8 CLO9 CLO10	5		2	35

Nội dung *(Ghi chi tiết từng chương, mục)*	Đáp ứng CĐR của học phần	**Phân bổ thời lượng cho các hoạt động giảng dạy và học tập**			
		Thời lượng giảng dạy (Tiết)			Thời gian sinh viên tự học (Giờ)
		Lý thuyết	Seminar	Thực hành / Thực tập	
(1)	(2)	(3)	(4)	(5)	(6)
7.3.2 Thanh toán điện tử an toàn 7.3.3 Chữ ký kép 7.3.4 Yêu cầu trả tiền– người mua 7.3.5 Yêu cầu trả tiền – người bán 7.3.6 Giấy phép cổng trả tiền 7.3.7 Nhận trả tiền **7.4 An toàn thư điện tử** 7.4.1 Dịch vụ PGP 7.4.2 Mở rộng thư Internet đa mục đích/an toàn S/MIME					
Tổng cộng		30	0	30	90

6. Ma trận chuẩn đầu ra của học phần với CĐR của CTĐT

BẢNG ĐÁNH GIÁ MỨC ĐỘ TƯƠNG THÍCH CĐR CỦA HỌC PHẦN VỚI CĐR CỦA CHƯƠNG TRÌNH ĐÀO TẠO

TT	**Chuẩn đầu ra học phần (CLO)**	**Đáp ứng chuẩn đầu ra của CTĐT (PLO)**
1	**Chuẩn đầu ra về kiến thức**	
	CLO 1	PLO5
	CLO 2	PLO5
	CLO 3	PLO5
2	**Chuẩn đầu ra về kỹ năng**	
	CLO 4	PLO9
	CLO 5	PLO9
	CLO 6	PLO9

TT	Chuẩn đầu ra học phần (CLO)	Đáp ứng chuẩn đầu ra của CTĐT (PLO)
3	**Mức tự chủ và trách nhiệm nghề nghiệp**	
	CLO 7	PLO13
	CLO8	PLO14

7. Tài liệu giảng dạy

7.1. Tài liệu chính

[1] An Toàn Toàn Bảo Mật Hệ Thống Thông Tin (2021) – Hoàng Xuân Dậu - Học viện Công nghệ Bưu chính Viễn thông.

7.2. Tài liệu tham khảo

[2] Sumitra, K., & Chandrasekhar Rao, D. (2024). Information Security Lecture Notes. Website

8. Nhiệm vụ của giảng viên và sinh viên

Nội dung	Nhiệm vụ của giảng viên	Nhiệm vụ của sinh viên	CĐR HP
Chương 1: Tổng quan về bảo mật	Giảng viên cung cấp cho sinh viên Slides bài giảng, giáo trình tài liệu tham khảo	Sinh viên đọc tài liệu trước khi lên lớp	CLO1
1.1 Giới thiệu chung về bảo mật thông tin **1.2 Dịch vụ cơ chế tấn công** **1.3 Mô hình an toàn mạng**	Giảng viên giới thiệu về lịch sử phát triển của bảo mật. Nêu các dịch vụ, mô hình , bảo mật an toàn thông tin	Đọc Slide bài giảng chương 1 Nhận biết và giải quyết bài toán. Xem Chương 1 trong giáo trình An toàn và bảo mật dữ liệu từ	CLO2 CLO5 CLO8

Nội dung	Nhiệm vụ của giảng viên	Nhiệm vụ của sinh viên	CĐR HP
Bảo mật thông tin trong hệ cơ sở dữ liệu		trang 1 đến trang 14. Đọc chương 1 trong tài liệu tham khảo [1]	
Chương 2: Kẻ xâm nhập, phần mềm có hại và tường lửa **2.1 Kẻ xâm nhập** **2.2 Phần mềm có hại** **2.3 Tràn bộ đệm** **2.4 Bức tường lửa**	Giảng viên giới thiệu về Các phần mềm có hại, Nêu các hình thức tấn công xâm nhập. Nêu vai trò quan trọng của bảo mật. Giao bài tập cho sinh viên	Đọc chương 7 trong giáo trình từ trang 78 đến trang 98. Sinh viên đọc [1],[2],[3],[5],[12] Sinh viên làm bài tập theo sự chỉ dẫn của giảng viên Sinh viên làm bài tập theo sự chỉ dẫn của giảng viên	CLO1 CLO3 CLO2 CLO5 CLO8
Chương 3: Mã cổ điển **3.1 Mã đối xứng** **3.2 Các mã thế cổ điển thay thế** **3.3 Các mã thế cổ điển hoán vị** **3.4 Một số vấn đề khác**	Giảng viên giới thiệu về các thám mã cổ điển, các loại thám mã Hướng dẫn sinh viên chuyển đổi số giữa các hệ đếm. Giao bài tập cho sinh viên.	Đọc Slide bài giảng chương 3 Đọc chương 3 trong giáo trình từ trang 14 đến 21. Sinh viên đọc [1],[2],[3],[12]	CLO2 CLO3

Nội dung	Nhiệm vụ của giảng viên	Nhiệm vụ của sinh viên	CĐR HP
		Sinh viên làm bài tập theo sự hướng dẫn của giảng viên.	
Chương 4: Cơ sở toán học **4.1 Số học trên Modulo** **4.2 Một số thuật toán trên Zn** **4.3 Giới thiệu lý thuyết số**	Giảng viên giới thiệu về Cơ sở toán học Giao bài tập cho sinh viên.	Đọc Slide bài giảng chương 3. Đọc chương 3 trong giáo trình từ trang 21 đến trang 30. Sinh viên đọc [1],[2],[3],[12] Sinh viên làm bài tập theo sự hướng dẫn của giảng viên. Đọc trước chương 4 trong giáo trình	CLO2 CLO3 CLO4 CLO6 CLO7 CLO8
Chương 5: HÀM HASH **5.1. Tổng quan về hàm Hash** **5.2. Hàm băm MD4** **5.3. Hàm băm MD5** **5.4. Hàm băm SHS**	Giảng viên giới thiệu về HÀM HASH. Các hàm băm Md4, Md5, SHS.. Giao bài tập cho sinh viên.	Đọc Slide bài giảng chương 5. Sinh viên làm bài tập theo sự hướng dẫn của giảng viên. Đọc trước chương 4 trong giáo trình	CLO2

Nội dung	Nhiệm vụ của giảng viên	Nhiệm vụ của sinh viên	CĐR HP
5.5. Hàm băm SHA **5.6. Xây dựng hàm băm trên cơ sở mật mã đối xứng** **5.7. Tấn công hàm Hash theo kiểu ngày sinh nhật**			
Chương 6: Mã khóa công khai và quản lý khóa. **6.1 Mã công khai** **6.2 RSA** **6.3 Quản lý khóa** **6.4 Phân phối khóa Diffie - Helman**	Giảng viên giới thiệu về Mã khóa công khai và quản lý khóa. Lấy ví dụ về mã khóa công khai và quản lý khóa Giao bài tập cho sinh viên	Đọc chương 6 trong giáo trình từ trang 42 đến trang 64. Sinh viên đọc [1],[2],[3],[5],[12] Sinh viên làm bài tập theo sự chỉ dẫn của giảng viên Đọc trước chương 6 trong giáo trình	CLO2 CLO4 CLO6 CLO7 CLO8
Kiểm tra giữa kỳ	Giảng viên giao bài tập và hướng dẫn cách thực hiện.	Làm bài tập dưới sự quản lý của giảng viên.	CLO2 CLO4 CLO5 CLO6

Nội dung	Nhiệm vụ của giảng viên	Nhiệm vụ của sinh viên	CĐR HP
	Kiểm tra, đánh giá kết quả thực hiện bài tập của sinh viên		CLO7 CLO8 CLO9 CLO10
			CLO1
Chương 7: An toàn IP và Web **7.1 An toàn IP** **7.2 An toàn Web** **7.3.3 Thanh toán điện tử an toàn** **7.4 An toàn thư điện tử**	Giảng viên giới thiệu về An toàn IP và Web Nêu vai trò của An toàn IP và Web Nêu ví dụ thực tế Giao bài tập cho sinh viên	Đọc chương 6 trong giáo trình từ trang 64 đến trang 78. Sinh viên đọc [1],[2],[3],[5],[12] Sinh viên làm bài tập theo sự chỉ dẫn của giảng viên Sinh viên làm bài tập theo sự chỉ dẫn của giảng viên	CLO2 CLO5 CLO8

9. Phương pháp giảng dạy và hình thức kiểm tra đánh giá kết quả học tập.

9. Phương pháp giảng dạy và hình thức kiểm tra đánh giá kết quả học tập.

9.1. Phương pháp giảng dạy học phần.

CLO	Bài giảng lý thuyết	Thảo luận nhóm	Thực hành	Bài tập cá nhân	Dự án/Đồ án

CLO1	x	x		x	
CLO2	x	x	x	x	
CLO3	x	x	x	x	x
CLO4		x	x	x	x
CLO5		x			x
CLO6	x	x	x	x	x
CLO7		x		x	x
CLO8	x	x	x	x	x

CLO	Phương pháp giảng dạy	Phương pháp học tương ứng
CLO1	Giảng giải, phân tích	Nghe giảng, ghi chú, đọc tài liệu
CLO2	Tình huống, giải thích	Tự học, thực hành
CLO3	Thực hành, mô phỏng	Làm bài tập, mô phỏng
CLO4	Dự án nhóm, trình bày	Làm việc nhóm, phát triển dự án
CLO5	Học theo dự án, thảo luận	Làm bài tập nhóm, cộng tác
CLO6	Trực quan, phần mềm hỗ trợ	Trải nghiệm phần mềm, thực hành
CLO7	Tự định hướng, phản hồi	Tự học, phản tỉnh, nhật ký học tập
CLO8	Tình huống, cập nhật công nghệ	Nghiên cứu tài liệu mới, sáng tạo

9.2. Hình thức kiểm tra, đánh giá

BẢNG ĐÁNH GIÁ KẾT QỦA HỌC TẬP CỦA NGƯỜI HỌC

Thành phần đánh giá	Bài đánh giá	Phương pháp/ hình thức đánh giá	Tiêu chí đánh giá	Thời điểm đánh giá	Hệ số	Đáp ứng CĐR học phần	Trọng số
Al. Đánh giá quá trình	A1.1. Điểm chuyên cần	Đánh giá mức độ chuyên cần	- Thời gian lên lớp nghe giảng - Tinh thần thái độ học tập - Mức độ tham gia các hoạt động semina, làm bài tập... (9.2.1)	Toàn bộ các tuần	1	CLO1-CLO6	10%
	A1.2. Bài kiểm tra 1	Bài kiểm tra số 1 (thực hành trên máy)	ự luận hoặc trắc nghiệm (kiến thức chương 1–3) (9.2.2)	Tuần thứ 4		CLO1-CLO6	40%
	A1.4 . Bài kiểm tra 2	Trình bày Bài tập tổng hợp theo nhóm	Mô phỏng tấn công đơn giản, phân tích mật mã, cấu trúc bảo mật(9.2.3)	Tuần thứ 10		CLO1-CLO8	
A2. Đánh giá cuối kỳ	Bài thi cuối kỳ	Thi trắc nghiệm	- Mức độ hoàn thành các câu hỏi trắc nghiệm từ dễ đến khó câu hỏi trắc nghiệm	Sau khi kết thúc toàn bộ môn học.	1	CLO1-CLO8	50%

Thành phần đánh giá	Bài đánh giá	Phương pháp/ hình thức đánh giá	Tiêu chí đánh giá	Thời điểm đánh giá	Hệ số	Đáp ứng CĐR học phần	Trọng số
			- Thái độ nghiêm túc tham gia kỳ thi (9.2.4)				

9.2.1 Tiêu chí đánh giá điểm chuyên cần:

Tiêu chí đánh giá	Mức độ đạt chuẩn quy định					
	MỨC 1	**MỨC 2**	**MỨC 3**	**MỨC 4**	**MỨC 5**	**Trọng số**
	0	**(5.5-6.9)**	**(7.0-8.4)**	**(8.5-8.9)**	**(9,0-10,0)**	
Đi học	Đi học quá ít	Đi học không đều	Đi học khá đều	Đi học chuyên cần	Đi học đầy đủ tất cả các buổi	50%
	(<80%)	(<81-85%)	(86-90%)	(91-95%)	(96-100%)	
Đóng góp tại lớp	Không tham gia hoạt động nào tại lớp	Hiếm khi tham gia phát biểu, đóng góp cho bài học tại lớp.	Thỉnh thoảng tham gia phát biểu, trao đổi ý kiến tại lớp.	Thường xuyên phát biểu và trao đổi ý kiến liên quan đến bài học.	Tham gia tích cực các hoạt động: phát biểu, trao đổi ý kiến liên quan đến bài học.	50%
		Đóng góp không hiệu quả.	Phát biểu ít khi có hiệu quả.	Các đóng góp cho bài học là hiệu quả.	Các đóng góp rất hiệu quả.	

9.2.2 Tiêu chí đánh giá bài kiểm tra:

Tiêu chí	Bài kiểm tra số 1	Thang điểm	Chuẩn đầu ra liên quan
1. Nhận biết lý thuyết cơ bản	Trình bày đúng khái niệm về bảo mật thông tin, tấn công, mã hóa cổ điển (Ceasar, Playfair...)	2.0 điểm	CLO1
2. Phân tích kỹ thuật xâm nhập – phần mềm độc hại	Mô tả được quy trình tấn công, kiểu mã độc, cơ chế kiểm soát truy cập hoặc phòng chống	2.0 điểm	CLO2
3. Vận dụng giải bài toán mã hóa cổ điển	Giải được các ví dụ mã Ceasar, Vigenere, Rail Fence... và giải mã ngược lại	3.0 điểm	CLO3
4. Trình bày và tư duy logic	Bố cục bài làm rõ ràng, trình bày có sơ đồ minh họa hoặc lập luận đúng logic	2.0 điểm	CLO3, CLO5
5. Phản xạ và sáng tạo cá nhân *(tùy chọn)*	Có đề xuất giải pháp, liên hệ thực tế hoặc đánh giá ví dụ nâng cao	1.0 điểm	CLO2, CLO5
1. Nhận biết lý thuyết cơ bản	Trình bày đúng khái niệm về bảo mật thông tin, tấn công, mã hóa cổ điển (Ceasar, Playfair...)	2.0 điểm	CLO1
Tổng điểm		**10 điểm**	

9.2.3 Tiêu chí đánh giá bài tập nhóm:

Tiêu chí đánh giá	Mô tả yêu cầu	Thang điểm (0–10)	Chuẩn đầu ra liên quan
1. Xác định đúng vấn đề bảo mật cần giải quyết	Nhận diện được kiểu tấn công, cơ chế mã hóa, kỹ thuật bảo vệ phù hợp đề tài	2.0 điểm	CLO2
2. Phân tích và triển khai giải pháp/mô hình	Vận dụng đúng thuật toán, công cụ hoặc phương pháp mô phỏng (ví dụ: mã hóa, phát hiện tấn công, shellcode)	3.0 điểm	CLO3
3. Đánh giá và nhận xét kết quả	Phân tích hiệu quả của giải pháp, ưu/nhược điểm, đề xuất cải tiến	2.0 điểm	CLO2, CLO3
4. Hình thức trình bày và tổ chức báo cáo	Báo cáo logic, hình ảnh minh họa rõ ràng, trình bày đúng yêu cầu kỹ thuật	2.0 điểm	CLO3
5. Làm việc nhóm và phân công rõ ràng	Có chia công hợp lý, mỗi thành viên tham gia, phản ánh đúng năng lực cá nhân	1.0 điểm	CLO5
1. Xác định đúng vấn đề bảo mật cần giải quyết	Nhận diện được kiểu tấn công, cơ chế mã hóa, kỹ thuật bảo vệ phù hợp đề tài	2.0 điểm	CLO2
TỔNG ĐIỂM		10	

9.2.4 Tiêu chí đánh giá bài thi cuối kỳ (trắc nghiệm máy):

Mức độ Bloom	Mô tả năng lực đánh giá	CLO liên quan	Số câu TN (dự kiến)	Tỷ trọng (%)	Điểm tương ứng
Nhận biết	Ghi nhớ khái niệm, mô hình, nguyên lý bảo mật, loại tấn công, tên thuật toán	CLO1, CLO2	12	20%	2
Thông hiểu	Mô tả được cách hoạt động của mã hóa, hàm băm, tường lửa, chữ ký số	CLO2, CLO3	15	25%	2.5
Vận dụng	Áp dụng được mã hóa cơ bản, chọn thuật toán, xác định lỗi bảo mật tình huống	CLO4, CLO5	15	25%	2.5
Phân tích	Phân tích kịch bản tấn công, đánh giá mức độ an toàn hệ thống	CLO4, CLO6, CLO9	18	30%	3
Tổng cộng			**60**	**100%**	**10 điểm**

10. Thông tin về người/ nhóm biên soạn

STT	Họ và tên	Học hàm/ học vị	Ghi chú
1	Lê Khắc Lưu	Thạc sĩ	
2	Lê Văn Ba	Thạc sĩ	

PHÊ DUYỆT

Phê duyệt BGH	Phê duyệt của Khoa	Người biên soạn
PGS.TS Nguyễn Xuân Sơn	**TS. Lê Đức Huy**	**ThS. Lê Khắc Lưu**