TRƯỜNG ĐẠI HỌC QUẢNG BÌNH
KHOA KT - CNTT

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc Lập - Tự Do - Hạnh Phúc

CHƯƠNG TRÌNH ĐÀO TẠO

Trình độ đào tạo: Đại học Ngành: Công nghệ thông tin Mã số: 7480201

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN

1. Thông tin chung

1.1. Tên học phần:Lý thuyết mật mã và an toàn dữ liệu	**1.2. Tên tiếng Anh:Theoretical cryptography and safety data**
1.3. Mã học phần: TILTMM.022	**1.4. Số tín chỉ:02**
1.5. Phân bố thời gian: [1]	
- Lý thuyết:	20 tiết
- Bài tập và Thảo luận nhóm:	10 tiết
- Tự học:	60 tiết
1.6. Các giảng viên phụ trách học phần:	
- Giảng viên phụ trách chính:	ThS. Nguyễn Nương Quỳnh
- Danh sách giảng viên cùng giảng dạy:	TS. Trần Văn Cường, ThS. Nguyễn Duy Linh, TS. Nguyễn Thị Hà Phương, TS. Phan Thị Huyền Trang, TS. Hoàng Đình Tuyền, TS. Hoàng Tuấn Nhã
1.7. Điều kiện tham gia học phần:	
- Học phần tiên quyết:	Không
- Học phần học trước:	Tin học đại cương, Cấu trúc dữ liệu và giải thuật
- Học phần song hành:	Không

2. Mục tiêu

2.1. Mục tiêu chung

Trang bị cho sinh viên những kiến thức cơ bản về mật mã học. Giúp cho sinh viên hiểu và nắm được một số thuật toán mã hoá quan trọng trong mật mã cổ điển và mật mã khóa công khai. Giúp cho sinh viên hiểu và nắm được một số vấn đề quan trọng trong các dịch vụ an toàn thông tin như xác thực và đảm bảo tínhtoàn vẹn. Giúp cho sinh viên hiểu được một số thủ tục ứng dụng trong thực tế như chữ ký số, trao đổi và phân phối khoá.

2.2. Mục tiêu cụ thể

[1]Một tín chỉ được quy định tối thiểu bằng 15 giờ học lý thuyết và 30 giờ tự học, chuẩn bị cá nhân có hướng dẫn hoặc bằng 30 giờ thực hành, thí nghiệm, thảo luận và 15 giờ tự học, chuẩn bị cá nhân có hướng dẫn hoặc bằng 45 giờ thực tập tại cơ sở, làm tiểu luận, bài tập lớn, đồ án, khóa luận tốt nghiệp.

2.2.1. Về kiến thức

Sinh viên nắm vững được tính chất, ý nghĩa và công dụng của các nhóm thuật toán chính trong lĩnh vực mật mã: mã hóa cổ điển, mã hóa đối xứng, mã hóa bất đối xứng, chữ ký điện tử.

2.2.2. Về kỹ năng

Rèn luyện các kỹ năng cần thiết nhất để sinh viên có thể tiếp tục nghiên cứu sâu hơn về các thuật toán mật mã và ứng dụng trong thực tiễn.

2.2.3. Về thái độ

Sinh viên có thái độ nghiêm túc trong học tập, có ý thức nâng cao thêm kiến thức về mật mã. Sinh viên tìm hiểu tài liệu về môn học theo sự hướng dẫn của giảng viên.

3. Chuẩn đầu ra (CLO)

Bảng 1. Chuẩn đầu ra của HP

Sau khi học xong học phần, SV có khả năng:

Ký hiệu CLO	Nội dung CLO
CLO1	Hiểu các khái niệm, các vấn đề cơ bản của lý thuyết mật mã và an toàn dữ liệu.
CLO2	Hiểu các thuật toán mã hóa cổ điển và hệ mật mã DES.
CLO3	Hiểu các thuật toán mật mã khóa công khai và chữ ký số.
CLO4	Phân tích, đánh giá ưu điểm và hạn chế của các hệ mật và vận dụng các hệ mật ứng dụng vào thực tiễn.
CLO5	Có ý thức tự học, tự nhiên cứu và ý thức được sự cần thiết phải thường xuyên học tập nâng cao trình độ

4. Mối liên hệ giữa chuẩn đầu ra học phần (CLO) và chuẩn đầu ra chương trình đào tạo (PLO)

Mức độ đóng góp, hỗ trợ của CLO để đạt được PLO được xác định cụ thể qua bảng sau:

Bảng 2.Mối liên hệ giữa CLOvà PLO

PLO	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
CLO 1	I			R	I	R	R			
CLO 2	I	R	R	R	I		R	R	R	
CLO 3	I	M	R	M	I	R	R	R	R	
CLO 4	I	M	R	M	I	R	R	R	R	
CLO 5									M	R
Tổng hợp học phần	I	M	R	M	I	R	R	R	M	R

5. Đánh giá

a. Phương pháp, hình thức kiểm tra - đánh giá

Bảng 3. Phương pháp, hình thức kiểm tra - đánh giá kết quả học tập của SV

Thành phần đánh giá	**Trọng số**	**Bài đánh giá**	**Trọng số con**	**Rubric (đánh dấu X nếu có)**	**Lquan đến CĐR nào ở bảng 4.1**	***Hướng dẫn phương pháp đánh giá***
(1)	(2)	(3)	(4)	(5)	(6)	*(7)*
A1. Chuyên cần, thái độ (CCTĐ)	5%			X	CLO5	Theo Rubric 1
A2. Kiểm tra thường xuyên (KTTX)	35%	A2.1: Các khái niệm khái niệm cơ bản về lý thuyết mật mã và an toàn thông tin. Các hệ mật cổ điển và chuẩn mã dữ liệu DES.	50%		CLO1 CLO2 CLO4	Chấm theo đáp án/hướng dẫn chấm
		A2.2: Hệ mật mã khóa công khai và chữ ký số.	50%		CLO3 CLO4	
A3. Đánh giá cuối kỳ	60%	Bài ktra cuối kỳ: Thi viết/Báo cáo tiểu luận		X	CLO1 CLO2 CLO3 CLO4 CLO5	Chấm theo đáp án (viết) hoặc Rubric 6 (tiểu luận)

Ghi chú: Tùy theo yêu cầu, đặc điểm của từng học phần, bộ môn có thể điều chỉnh thành phần và trọng số, trọng số con của các thành phần đánh giá. Tuy nhiên, phải đảm bảo đánh giá cuối kỳ không dưới 50%.

b. Yêu cầu đối với học phần

Sinh viên phải tham dự >=70% số buổi của HP. Nếu nghỉ >30% số buổi sẽ không được dự thi kết thúc HP.

6. Kế hoạch và nội dung giảng dạy

Bảng 4. Kế hoạch và nội dung giảng dạytheo tuần

Tuần/ Buổi (4 tiết/b)	**Các nội dung cơ bản của bài học (chương)**	**Số tiết (LT/TH/ BT/TL)**	**CĐR của bài học (chương)/chủ đề**	**Lquan đến CĐR nào ở bảng 1**	**PP giảng dạy , tài liệu và cở sở vật chất, thiết bị cần thiết để đạt CĐR**	**Hoạt động học của SV(*)**	**Tên bài đánh giá**
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	Chương 1 Tổng quan về an toàn và bảo mật thông tin 1.1. Vấn đề an toàn và bảo mật thông tin trên mạng máy tính 1.2. Các chiến lược an toàn hệ thống 1.3. Các mức bảo vệ trên mạng 1.4. Mật mã học 1.5. Cơ sở toán học của lý thuyết mật mã	**3** 2/0/1/0	1. Hiểu các khái niệm, các vấn đề cơ bản của lý thuyết mật mã và an toàn dữ liệu.	CLO1	- Thuyết giảng, Hướng dẫn làm việc nhóm, Cho bài tập - Bài giảng của giảng viên - Sử dụng bảng phấn	- Nghe giảng, ghi chú - Trả lời câu hỏi - Làm bài tập	A2.1
2	Chương 2 Các phương pháp mã hóa cổ điển 2.1. Các thuật ngữ 2.2. Định nghĩa 2.3. Những yêu cầu đối với hệ mật mã 2.4. Các phương pháp mã hoá cổ điển 2.4.1. Mật mã dịch chuyển 2.4.2. Mật mã thay thế	**3** 2/0/1/0	2.1. Hiểu và vận dụng được các phương pháp mã hóa cổ điển.	CLO2 CLO4	- Thuyết giảng, Hướng dẫn làm việc nhóm, Cho bài tập - Bài giảng của giảng viên - Sử dụng bảng phấn	- Nghe giảng, ghi chú - Trả lời câu hỏi - Làm bài tập	A2.1

3	Chương 2 Các phương pháp mã hóa cổ điển 2.4. Các phương pháp mã hoá cổ điển 2.4.3. Mật mã Affine 2.4.4. Mật mã Vigenere 2.4.5. Mật mã hoán vị 2.4.6. Mật mã dòng	**3** 2/0/1/0	2.2. Hiểu và vận dụng được các phương pháp mã hóa cổ điển.	CLO2 CLO4	- Thuyết giảng, Hướng dẫn làm việc nhóm, Cho bài tập - Bài giảng của giảng viên - Sử dụng bảng phấn	- Nghe giảng, ghi chú - Trả lời câu hỏi - Làm bài tập	A2.1
4	Chương 3 Chuẩn mã dữ liệu – DES 3.1. Giới thiệu chung về DES 3.2. Mô tả DES	**3** 2/0/1/0	3.1. Hiểu chuẩn mã dữ liệu DES	CLO2 CLO4	- Thuyết giảng, Hướng dẫn làm việc nhóm, Cho bài tập - Bài giảng của giảng viên - Sử dụng bảng phấn	- Nghe giảng, ghi chú - Trả lời câu hỏi - Làm bài tập	A2.1
5	Chương 3 Chuẩn mã dữ liệu – DES 3.3. Giải mã DES 3.4. Ứng dụng của DES	**3** 2/0/1/0	3.2. Hiểu chuẩn mã dữ liệu DES	CLO2 CLO4	- Thuyết giảng, Hướng dẫn làm việc nhóm, Cho bài tập - Bài giảng của giảng viên - Sử dụng bảng phấn	- Nghe giảng, ghi chú - Trả lời câu hỏi - Làm bài tập	A2.1

6	Chương 4 Mật mã khóa công khai 4.3. Hệ mật RSA 4.4. Hệ mật Elgamal	**3** 2/0/1/0	4.1. Hiểu các hệ mật mã khóa công khai.	CLO3 CLO4	- Thuyết giảng, Hướng dẫn làm việc nhóm, Cho bài tập - Bài giảng của giảng viên - Sử dụng bảng phấn	- Nghe giảng, ghi chú - Trả lời câu hỏi - Làm bài tập	A2.2
7	Chương 4 Mật mã khóa công khai 4.1. Giới thiệu về hệ mật mã khóa công khai 4.2. Các thuật toán cho bài toán Logarit rời rạc	**3** 2/0/1/0	4.2. Hiểu các hệ mật mã khóa công khai.	CLO3 CLO4	- Thuyết giảng, Hướng dẫn làm việc nhóm, Cho bài tập - Bài giảng của giảng viên - Sử dụng bảng phấn	- Nghe giảng, ghi chú - Trả lời câu hỏi - Làm bài tập	A2.2
8	Chương 5 Chữ ký số 5.1. Khái niệm chữ ký số 5.2. Phân loại các sơ đồ chữ ký số	**3** 2/0/1/0	5.1. Hiểu về chữ ký số và ứng dụng trong thực tế.	CLO3 CLO4	- Thuyết giảng, Hướng dẫn làm việc nhóm, Cho bài tập - Bài giảng của giảng viên - Sử dụng bảng phấn	- Nghe giảng, ghi chú - Trả lời câu hỏi - Làm bài tập	A2.2

9	Chương 5 Chữ ký số 5.3. Sơ đồ chữ ký RSA 5.4. Sơ đồ chữ ký Elgamal	**3** 2/0/1/0	5.2. Hiểu về chữ ký số và ứng dụng trong thực tế.	CLO3 CLO4	- Thuyết giảng, Hướng dẫn làm việc nhóm, Cho bài tập - Bài giảng của giảng viên - Sử dụng bảng phấn	- Nghe giảng, ghi chú - Trả lời câu hỏi - Làm bài tập	A2.2
10	Chương 5 Chữ ký số 5.5. Chuẩn chứ ký số DSS 5.6. Tấn công chữ ký số	**3** 2/0/1/0	5.3. Hiểu về chữ ký số và ứng dụng trong thực tế.	CLO3 CLO4	- Thuyết giảng, Hướng dẫn làm việc nhóm, Cho bài tập - Bài giảng của giảng viên - Sử dụng bảng phấn	- Nghe giảng, ghi chú - Trả lời câu hỏi - Làm bài tập	A2.2
Theo lịch thi	Kiểm tra cuối kì						A3

(*) Ghi chú:

- (3) Số tiết (LT/TH/BT/TL): Xác định số tiết lý thuyết, thực hành, thực tập của từng chương

- (6) PP giảng dạy đạt CĐR: Nêu tên các PP giảng dạy sử dụng trong từng chương để đạt CĐR

- (7) Hoạt động học của SV: Xác định các nội dung SV cần chuẩn bị tại nhà (đọc tài liệu nào, từ trang thứ mấy, làm việc nhóm để giải quyết bài tập, làm dự án …….); Hoạt động tại lớp (thảo luận nhóm, làm bài tập,…).

7. Học liệu

Bảng 5. 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
	Giáo trình chính			
1	Nguyễn Bình	2004	Giáo trình mật mã học	Bưu điện
2	Thái Hồng Nhị	2004	An Toàn Thông Tin Mạng Máy Tính	Khoa học kỹ thuật
	Sách, giáo trình tham khảo			
3	Dương Anh Đức, Trần Minh Triết	2005	Mã hóa và Ứng dụng	Đại học Quốc gia
4	Jonathan Katz and Yehuda Lindell	2015	Introduction to Modern Cryptography	Chapman and Hall/CRC Press, 2015

8.Cơ sở vật chất phục vụ giảng dạy

Bảng 6. Cơ sở vật chất phục vụ giảng dạy

TT	Tên giảng đường, PTN, xưởng, cơ sở TH	Danh mục trang thiết bị, phần mềm chínhphục vụ TN,TH		Phục vụ cho nội dung Bài học/Chương
		Tên thiết bị, dụng cụ, phần mềm,…	Số lượng	
1	Giảng đường A	Projector, máy tính cá nhân	1	Chương 1, 2, 3, 4, 5

9. Rubric đánh giá

Theo Phụ lục 1

Quảng Bình, ngày tháng 5 năm 2021

Trưởng khoa	Trưởng bộ môn	Người biên soạn
TS. Phạm Xuân Hậu	TS. Trần Văn Cường	ThS. Nguyễn Nương Quỳnh