TRƯỜNG ĐẠI HỌC VĂN HIẾN
KHOA CÔNG NGHỆ THÔNG TIN

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

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN

1. Thông tin về học phần

- Tên học phần: MẬT MÃ HỌC (CRYPTOGRAPHY)
- Mã học phần: INT489
- Số tín chỉ: 02 (2/0/4)
- Bậc đào tạo: Đại học
- Loại học phần: Bắt buộc
- Học phần tiên quyết/ Học phần trước: …
- Đơn vị phụ trách: Khoa Công nghệ thông tin
- Số giờ tín chỉ: 30, trong đó:
- Lý thuyết: 30 (1 tín chỉ LT = 15 tiết)
- Thực hành: 00 (1 tín chỉ TH = 30 tiết)
- Thực tập: 00 (1 tín chỉ TT = 60 giờ TT tại cơ sở)
- Đồ án/ Khóa luận 00 (1 tín chỉ ĐA/KL = 45 giờ làm ĐA/KL)

2. Thông tin về giảng viên

Giảng viên 1:

- Họ và tên: .....
- Chức danh, học vị: .....
- Thời gian làm việc: Giờ hành chính (8:00 -16:00)
- Địa điểm làm việc: Khoa ….. - Trường Đại học …..
- Điện thoại: .....
- Email: .....

Giảng viên 2:

- Họ và tên: .....
- Chức danh, học vị: .....
- Thời gian làm việc: Giờ hành chính (8:00 -16:00)
- Địa điểm làm việc: Khoa ….. - Trường Đại học …..
- Điện thoại: .....
- Email: .....

3. Tóm tắt nội dung học phần

Học phần gồm 04 chương, cung cấp cho người học kiến thức tổng quát về mật mã, nhằm giúp người học hiểu và biết ứng dụng khi triển khai thực tế. Người học được giới thiệu cơ bản về mật mã học và một số thuật toán mã hoá quan trọng trong mật mã cổ điển và mật mã hiện đại. Ngoài ra, học phần giới thiệu các dịch vụ an toàn thông tin.

4. Mục tiêu của học phần

Học phần có những mục tiêu:

- Cung cấp cho người học những kiến thức chung về lý thuyết thông tin trong các hệ mật.

- Cung cấp cho người học những kiến thức cơ bản về mật mã, đặc biệt là mật mã học hiện đại. Giúp cho sinh viên hiểu rõ được một số thuật toán mã hoá quan trọng trong mật mã cổ điển và mật mã hiện đại, một số vấn đề quan trọng trong các dịch vụ an toàn thông tin như xác thực và đảm bảo tính toàn vẹn.

- Trang bị kiến thức về một số thủ tục ứng dụng trong thực tế như chữ ký số, trao đổi và phân phối khoá. Cũng như có khả năng phân biệt khi nào cần dùng các hệ mật khóa bí mật hay các hệ mật khóa công khai để mã hóa dữ liệu lúc triển khai ứng dụng thực tế.

- Phát triển kỹ năng phân tích, lập luận, và thuyết trình hiệu quả.

5. Chuẩn đầu ra của học phần:

Mã CĐR	**Nội dung chuẩn đầu ra** (Bắt đầu bằng động từ theo thang Bloom)
Kiến thức	
CLO1	
CLO	
CLO	
CLO	
Kỹ năng	
CLO	
CLO	
CLO	
CLO	
Mức độ tự chủ và trách nhiệm	
CLO	
CLO	

Ma trận liên kết giữa Chuẩn đầu ra chương trình đào tạo và Chuẩn đầu ra học phần

Chuẩn đầu ra	**PLO1**	**PLO...**	**PLO...**	**PLO...**	**PLO...**	**PLO...**	**PLO...**
CLO1	X	X					
CLO2	X						
CLO3			X				
CLO4				X			
CLO5					X	X	X

***Ghi chú: PLOs** (ProgrammeLearningOutcomes): Chuẩn đầu ra cấp CTĐT*

***CLOs**(Course LearningOutcomes): Chuẩn đầu ra học phần*

6. Nội dung chi tiết của học phần

6.1. Lý thuyết

Chương	Nội dung	Đáp ứng CLOs
Chương 1	**Lý thuyết thông tin trong các hệ mật**	**CLO2, CLO5**
1.1	Sơ đồ khối chức năng của hệ thống thông tin số	
1.2	Các chỉ tiêu chất lượng cơ bản của một hệ thống thông tin số	
1.3	Độ mật hoàn thiện	
1.4	Entrophy và tính chất của entrophy	
1.5	Khóa giả và khoảng giải mã duy nhất	
1.6	Phân tích mật mã và độ phức tạp tính toán	
Chương 2	**Các hệ mật khóa bí mật**	
2.1	Các hệ mật thay thế đơn giản	
2.2	Các hệ mật thay thế đa biểu	
2.3	Các hệ mật thay thế không hoàn toàn	
2.4	Các hệ mật chuyển vị	
2.5	Các hệ mật tích	
2.6	Chuẩn mã dữ liệu (DES)	
2.7	Chuẩn mã dữ liệu tiên tiến (AES)	
2.8	Ưu nhược điểm của các hệ mật khóa bí mật	
Chương 3	**Các hệ mật khóa công khai**	
3.1	Khái niệm về hệ mật khóa công khai	
3.2	Số học Modulo	
3.3	Bài toán phân tích thừa số và các hệ mật có liên quan	
3.4	Bài toán logarit rời rạc và các hệ mật có liên quan	
3.5	Bài toán xếp balô và hệ mật Merkle – Hellman	
3.6	Bài toán mã sửa sai và hệ mật Mc Elice	
3.7	Hệ mật trên đường cong Eliptic	
3.8	Ưu nhược điểm của các hệ mật khóa công khai	
Chương 4	**Hàm băm, xác thực và chữ ký số**	
4.1	Các vấn đề về xác thực	
4.2	Hàm băm	
4.3	Chữ ký số	
4.4	Các chữ ký số có nén	
4.5	Chuẩn chữ ký số	

6.2. Thực hành

	Nội dung	Đáp ứng CLOs
6.2.1.	**Bài tập cá nhân**	
	Người học làm bài tập trong từng chương.	
6.2.2.	**Bài tập nhóm**	
	- Người học tạo nhóm tìm lời giải cho các bài tập do giảng giảng viên đặt ra. - Các nhóm báo cáo kết quả làm việc trước lớp.	-

7. Phân bổ thời gian theo tiết và điều kiện thực hiện:

Chương	Tên chương	Số tiết tín chỉ					Ghi chú
		Lý thuyết	Bài tập	Thực hành	Tự học	Tổng	
1	Lý thuyết thông tin trong các hệ mật	05	0	0	10	15	
2	Các hệ mật khóa bí mật	10	0	0	20	30	
3	Các hệ mật khóa công khai	10	0	0	20	30	
4	Hàm băm, xác thực và chữ ký số	05	0	0	10	15	
Tổng		**30**	**0**	**0**	**60**	**90**	

CÁC CHỦ ĐỀ THẢO LUẬN VÀ TIỂU LUẬN

1. .....
2. .....
3. .....

8. Phương pháp giảng dạy:

Giảng viên giảng dạy với sự kết hợp của một số phương pháp sau:

Gợi ý:

- Thuyết trình
- Phát vấn
- Hỏi lại hoặc vấn đáp
- Đọc và tóm lược nội dung tài liệu
- Động não nhanh (bài tập tư duy cá nhân)
- Giao bài đọc về nhà
- Hướng dẫn tự học
- Thảo luận nhóm
- ...

Ma trận liên kết giữa Chuẩn đầu ra với phương pháp giảng dạy

Phương pháp giảng dạy	CLO1	CLO2	CLO3	CLO4	CLO5	CLO6	CLO7	CLO8	CLO9	CLO10	CLO11	CLO12
	X	X								X		
	X									X		
			X							X		
				X						X	X	
					X	X	X	X	X	X	X	X
					X	X	X	X	X	X	X	X
					X	X	X	X	X	X	X	X

9. Phương pháp học tập

Sinh viên học tập với sự kết hợp của một số phương pháp sau:

Gợi ý:

- Thuyết trình
- Làm việc nhóm
- Tự học, tự nghiên cứu
- ….

Ma trận liên kết giữa Chuẩn đầu ra với phương pháp học tập

Phương pháp học tập	CLO1	CLO2	CLO3	CLO4	CLO5	CLO6	CLO7	CLO8	CLO9	CLO10	CLO11	CLO12
	X	X								X		
	X									X		
			X							X		
				X						X	X	

10. Nhiệm vụ của sinh viên

Gợi ý:

- Chủ động tổ chức thực hiện giờ tự học.
- Tham gia đầy đủ các giờ lên lớp và giờ thuyết trình (sinh viên chỉ được vắng mặt tối đa 20% thời gian lên lớp của học phần).
- Đọc tài liệu tham khảo bắt buộc và bổ trợ do giảng viên giới thiệu.
- Hoàn thành đầy đủ các bài tập cá nhân, bài tập nhóm.
- Tham gia kỳ thi kết thúc học phần.
- ....

11. Thang điểm đánh giá: Điểm đánh giá quá trình và điểm thi kết thúc học phần được chấm theo thang điểm 10 (từ 0 đến 10), làm tròn đến 1 chữ số thập phân.

12. Phương pháp kiểm tra, đánh giá kết quả học tập

Sinh viên được đánh giá kết quả học tập trên cơ sở hai điểm thành phần như sau:

1. *Điểm đánh giá quá trình: trọng số 40% bao gồm:*

a. Điểm chuyên cần: …., trọng số …%

b. Điểm kiểm tra thường xuyên: …., trọng số …%

c. ….

2. *Điểm thi kết thúc học phần: trọng số 60%*

Hình thức thi: Tự luận.

Ma trận quan hệ giữa Chuẩn đầu ra và phương pháp kiểm tra, đánh giá

Hình thức đánh giá	**CLO1**	**CLO2**	**CLO3**	**CLO4**	**CLO5**	**CLO6**	**CLO7**	**CLO8**	**CLO9**	**CLO10**	**CLO11**	**CLO12**
Tiểu luận	X	X	X	X	X	X	X	X	X	X	X	X
Thuyết trình	X		X		X	X	X	X	X	X	X	X
Trắc nghiệm	X	X	X	X	X	X	X	X	X	X	X	X
Dự lớp									X			
...												

13. Tài liệu phục vụ cho học phần (các tài liệu xuất bản trong 05 năm trở lại đây và cung cấp được cho Trung tâm Học liệu nơi đặt tài liệu)

13.1. Tài liệu chính

- Jean-Philippe Aumasson, Serious Cryptography: A Practical Introduction to Modern Encryption, No Starch Press, 2017.

13.2. Tài liệu tham khảo

- Douglas R. Stinson, Maura B. Paterson, Cryptography: Theory and Practice, CRC Press, 2018.
- William Easttom, Modern Cryptography, Springer, 2021.

TP.Hồ Chí Minh, ngày … tháng … năm ……

Hiệu trưởng **Duyệt**	**Trưởng Bộ môn** (Ký và ghi rõ họ tên)	**Giảng viên biên soạn** (Ký và ghi rõ họ tên)