TRƯỜNG ĐH NGOẠI NGỮ - TIN HỌC TP.HCM
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 chung về học phần

- **Tên học phần : Kỹ thuật mật mã (Encryption)**
- **Mã số học phần :** 1250124
- **Số tín chỉ học phần:** 4 (3+1) tín chỉ
- Thuộc chương trình đào tạo của bậc, ngành: Bậc Đại học, ngành Công nghệ thông tin
- **Số tiết học phần:**
  - Nghe giảng lý thuyết : 39 tiết
  - Làm bài tập trên lớp : 0 tiết
  - Thảo luận : 6 tiết
  - Thực hành, thực tập (ở phòng thực hành, phòng Lab,...): 30 tiết
  - Hoạt động theo nhóm : 0 tiết
  - Thực tế: : 0 tiết
  - Tự học : 120 giờ
- **Đơn vị phụ trách học phần:** Bộ môn Mạng máy tính/ Khoa Công nghệ thông tin

2. Học phần trước: An ninh mạng

3. Mục tiêu của học phần:

- Sinh viên nắm vững được tính chất, ý nghĩa và công dụng của các nhóm thuật toán chính trong lĩnh vực kỹ thuật mật mã : mã hóa đối xứng, mã hóa bất đối xứng, chữ ký điện tử, hàm băm mật mã.
- Sinh viên có khả năng phân tích yêu cầu bảo vệ thông tin trong hệ thống phần mềm, từ đó có khả năng thiết kế giải pháp, giao thức, quy trình để bảo vệ thông tin trong hệ thống phần mềm.
- Sinh viên có khả năng phân tích, đánh giá ưu điểm và hạn chế của các giải pháp, giao thức, quy trình bảo vệ thông tin trong hệ thống phần mềm.

4. Chuẩn đầu ra:

	Nội dung	**Đáp ứng CĐR CTĐT**
Kiến thức	4.1.1.Trang bị cho sinh viên những kiến thức cơ bản về kỹ thuật mã hóa.	**K1**
	4.1.2. Sinh viên có khả năng lựa chọn các kỹ thuật phù hợp trong quá trình thiết kế giải pháp để bảo vệ thông tin. Nắm một số giải thuật cơ	**K2, K3**

	bản trong lĩnh vực mã hóa và tìm hiểu một số kỹ thuật mã hóa hiện đại.	
Kỹ năng	4.2.1. Sinh viên có khả năng phân tích, đánh giá ưu điểm và hạn chế của các giải pháp, giao thức, quy trình bảo vệ thông tin trong hệ thống phần mềm.	**S2**
	4.2.2. Sinh viên có kỹ năng thiết kế giao thức đơn giản phù hợp với tình huống, kịch bản trong quá trình phát triển hệ thống phần mềm.	**S1,S3**
Thái độ	4.3.1.Đi học đúng giờ và đọc bài trước ở nhà.	**A2**
	4.3.2. Nhìn nhận đúng vai trò môn học cho công việc tương lai. Tham gia tích cực trong nghiên cứu học tập kiến thức.	**A3**

5. Mô tả tóm tắt nội dung học phần:

Học phần này nhằm cung cấp cho các sinh viên các kiến thức liên quan đến Kỹ Thuật Mã Hóa:

- Hệ thống mật mã đối xứng
- Hệ thống mật mã bất đối xứng
- Hàm băm mật mã
- Chữ ký điện tử
- Hệ thống chứng nhận khóa công cộng
- Một số quy trình bảo vệ thông tin

6. Nội dung và lịch trình giảng dạy:

- Các học phần lý thuyết:

Buổi/ Tiết	Nội dung	Hoạt động của giảng viên	Hoạt động của sinh viên	Giáo trình Chính	Tài liệu tham khảo	Ghi chú
1	Tổng quan về kỹ thuật mật mã	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	[1] Chương 1	[2] Chương 1 [3] Trang 3-24	Giải quyết 4.1.1, 4.3
2	Các hệ thống mật mã đối xứng (cổ điển)	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	[1] Chương 2	[2] Chương 2 [3] Chương 2	Giải quyết 4.1, 4.3
3	Lý thuyết Shannon	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	[1] Chương 2	[2] Chương 2	Giải quyết 4.1, 4.3
4	Các hệ thống mã hóa đối xứng mới (DES, AES…)	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	[1] Chương 3,5	[2] Chương 2	Giải quyết 4.1, 4.3
5	Các chế độ hoạt động, các chiến lược padding	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	[1] Chương 3,5	[2] Chương 5 [3] Chương 3	Giải quyết 4.1.2, 4.3

6	Các hệ thống mật mã bất đối xứng	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	[1] Chương 8,9,10	[2] Chương 6	Giải quyết 4.1.2, 4.3
7	Chữ ký điện tử	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	[1] Chương 13	[2] Chương 7 [3] Chương 12	Giải quyết 4.1, .4.3
8	Hàm băm mật mã	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	[1] Chương 11	[2] Chương 9 [3] Chương 5	Giải quyết 4.1, 4.3
9	Chứng nhận khóa công cộng	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	[1] Chương 14	[2] Chương 10 [3] Chương 10	Giải quyết 4.1.2, .4.3
10	Secured Socket Layer	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	[1] Chương 17		Giải quyết 4.1.2, 4.3
11	Một số giao thức trong mạng không dây (WEP, WPA, WPA2…)	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	[1] Chương 18	[2] Chương 9	Giải quyết 4.1.2, 4.3
12	Một số vấn đề khác (Single	- Thuyết giảng	- Nghe giảng, ghi chú	[1] Chương 15	[2] Chương 10,14	Giải quyết

	Sign-On, Trust Negotiation, Kerberos, Blind-Signature, e-Voting, e-Cash…)	- Hướng dẫn làm việc nhóm - Cho bài tập	- Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập			4.1, 4.2, 4.3
13	Ôn Tập	- Thuyết giảng - Hướng dẫn làm việc nhóm - Cho bài tập	- Nghe giảng, ghi chú - Trả lời câu hỏi - Thảo luận nhóm theo chủ đề - Làm bài tập	Tham khảo [1]	Tham khảo[2]	Giải quyết 4.1, 4.2, 4.3
14	Trình bày kết quả của đề tài nhóm.	- Góp ý cho seminar	Trình bày kết quả làm việc nhóm	Tham khảo [1]	Tham khảo [2]	Giải quyết 4.1, 4.2, 4.3
15	Trình bày kết quả của đề tài nhóm (tiếp theo)	- Góp ý cho seminar	Trình bày kết quả làm việc nhóm	Tham khảo [1]	Tham khảo [2]	Giải quyết 4.1, 4.2, 4.3

- Các học phần thực hành:

Buổi/ Tiết	Nội dung	Hoạt động của giảng viên	Hoạt động của sinh viên	Giáo trình Chính	Tài liệu tham khảo	Ghi chú
1	Bài 1: Các hệ thống mật mã đối xứng (cổ điển)	- Review điểm chính - Hướng dẫn sinh viên thực hiện - Trả lời câu hỏi của SV	- Nghe giảng, ghi chú - Đặt câu hỏi - Làm bài tập	[1] Chương 2	[2] Chương 2 [3] Chương 2	Giải quyết mục tiêu 4.2, 4.3
2	Bài 2: Hệ thống mã hóa đối xứng DES	- Review điểm chính - Hướng dẫn sinh viên thực hiện - Trả lời câu hỏi của SV	- Nghe giảng, ghi chú - Đặt câu hỏi - Làm bài tập	[1] Chương 3	[2] Chương 2	Giải quyết mục tiêu 4.2, 4.3
3	Bài 3: Hệ thống mã hóa đối xứng AES	- Review điểm chính - Hướng dẫn sinh viên thực hiện - Trả lời câu hỏi của SV	- Nghe giảng, ghi chú - Đặt câu hỏi - Làm bài tập	[1] Chương 3	[2] Chương 2	Giải quyết mục tiêu 4.2, 4.3
4	Bài 4: Hệ thống mật mã bất đối xứng RSA	- Review điểm chính - Hướng dẫn sinh viên thực hiện - Trả lời câu hỏi của SV	- Nghe giảng, ghi chú - Đặt câu hỏi - Làm bài tập	[1] Chương 9	[2] Chương 6	Giải quyết mục tiêu 4.2, 4.3
5	Bài 5: Chữ ký điện tử	- Review điểm chính - Hướng dẫn sinh viên thực hiện - Trả lời câu hỏi của SV	- Nghe giảng, ghi chú - Đặt câu hỏi - Làm bài tập	[1] Chương 13	[2] Chương 7 [3] Chương 12	Giải quyết mục tiêu 4.2, 4.3
6	Bài 6: Hàm băm	- Review điểm chính - Hướng dẫn sinh viên thực hiện - Trả lời câu hỏi của SV	- Nghe giảng, ghi chú - Đặt câu hỏi - Làm bài tập	[1] Chương 11	[2] Chương 9 [3] Chương 5	Giải quyết mục tiêu 4.2, 4.3
7	Bài 7: Chứng nhận khóa công cộng	- Review điểm chính - Hướng dẫn sinh viên thực hiện	- Nghe giảng, ghi chú - Đặt câu hỏi - Làm bài tập	[1] Chương 14	[2] Chương 10 [3] Chương 10	Giải quyết mục tiêu 4.2, 4.3

		- Trả lời câu hỏi của SV				
8	Bài 8: Giao thức mã hóa không dây WEP	- Review điểm chính - Hướng dẫn sinh viên thực hiện - Trả lời câu hỏi của SV	- Nghe giảng, ghi chú - Đặt câu hỏi - Làm bài tập	[1] Chương 18	[2] Chương 9	Giải quyết mục tiêu 4.2, 4.3
9	Bài 9: Giao thức mã hóa không dây WPA	- Review điểm chính - Hướng dẫn sinh viên thực hiện - Trả lời câu hỏi của SV	- Nghe giảng, ghi chú - Đặt câu hỏi - Làm bài tập	[1] Chương 18	[2] Chương 9	Giải quyết mục tiêu 4.2, 4.3
10	Bài 10: Thi	Coi thi và chấm điểm	Làm bài thi			Giải quyết mục tiêu 4.2, 4.3

7. Nhiệm vụ của sinh viên:

Sinh viên phải thực hiện các nhiệm vụ như sau:

- Tham dự tối thiểu 80% số tiết học lý thuyết.
- Tham gia đầy đủ 100% giờ thực hành và có báo cáo kết quả.
- Thực hiện đầy đủ các bài tập nhóm/ bài tập và được đánh giá kết quả thực hiện.
- Tham dự thi kết thúc học phần.
- Chủ động tổ chức thực hiện giờ tự học.

8. Đánh giá kết quả học tập của sinh viên:

8.1. Cách đánh giá

Sinh viên được đánh giá tích lũy học phần như sau:

TT	Điểm thành phần		Quy định	Trọng số	Mục tiêu
1	Lý Thuyết	Điểm thi kết thúc học phần	- Tham dự đủ 80% tiết lý thuyết - Thi lý thuyết	70%	4.1, 4.2.1, 4.3
2	Thực hành	Điểm thực hành	- Tham gia 100% số giờ - Thi thực hành	30%	4.1, 4.2, 4.3

8.2. Cách tính điểm

- Điểm đánh giá thành phần và điểm thi kết thúc học phần được chấm theo thang điểm 10 (từ 0 đến 10), làm tròn đến 0.5.
- Điểm học phần là tổng điểm của tất cả các điểm đánh giá thành phần của học phần nhân với trọng số tương ứng. Điểm học phần theo thang điểm 10 làm tròn đến một chữ số thập phân.

9. Tài liệu học tập:

9.1. Giáo trình chính:

[1] **Cryptography and Network Security: Principles and Practice**, 7th edition, William Stallings, Pearson, 2017

9.2. Tài liệu tham khảo:

[2] **Mã hóa và Ứng dụng**, Dương Anh Đức, Trần Minh Triết, NXB Đại học Quốc gia, 2005

[3] **Introduction to Modern Cryptography**, Jonathan Katz and Yehuda Lindell, Chapman and Hall/CRC Press, 2015

10. Hướng dẫn sinh viên tự học:

Tuần/ Buổi	Nội dung	Lý thuyết (tiết)	Thực hành (tiết)	Nhiệm vụ của sinh viên
1	Tổng quan về kỹ thuật mật mã	3	0	Tìm hiểu trước chương 1 trong [1] Tìm hiểu trước chương 1 trong [2]
2	Các hệ thống mật mã đối xứng (cổ điển)	3	3	Tìm hiểu trước chương 2 trong [1] Tìm hiểu trước chương 2 trong [2]
3	Lý thuyết Shannon	3	0	Tìm hiểu trước chương 2 trong [1] Tìm hiểu trước chương 2 trong [2]
4	Các hệ thống mã hóa đối xứng mới (DES, AES…)	3	6	Tìm hiểu trước chương 3 trong [1] Tìm hiểu trước chương 2 trong [2]
5	Các chế độ hoạt động, các chiến lược padding	3	0	Tìm hiểu trước chương 3 trong [1]
6	Các hệ thống mật mã bất đối xứng	3	3	Tìm hiểu trước chương 8,9,10 trong [1] Tìm hiểu trước chương 6 trong [2]
7	Chữ ký điện tử	3	3	Tìm hiểu trước chương 13 trong [1] Tìm hiểu trước chương 7 trong [2]
8	Hàm băm mật mã	3	3	Tìm hiểu trước chương 11 trong [1] Tìm hiểu trước chương 9 trong [2]
9	Chứng nhận khóa công	3	3	Tìm hiểu trước chương 14 trong [1] Tìm hiểu trước chương 10 trong [2]
10	Secured Socket Layer	3	0	Tìm hiểu trước chương 17 trong [1]
11	Một số giao thức trong mạng không dây (WEP, WPA, WPA2…)	3	6	Tìm hiểu trước chương 18 trong [1]
12	Một số vấn đề khác (Single Sign-On, Trust Negotiation, Kerberos, Blind-Signature, e-Voting, e-Cash…)	3	0	Tìm hiểu các giải thuật khác trong các tài liệu [1], [2], [3]
13	Ôn tập	3	3	Tìm hiểu trước kiến thức trong cuốn [1],[2]. Các vấn đề mới trên internet.
14	Trình bày kết quả của đề tài nhóm.	3	0	Cuốn [1],[2] và internet.
15	Trình bày kết quả của đề tài	3	0	Cuốn [1],[2] và internet.

	nhóm (tiếp theo)			

Ngày… tháng…. Năm 201	*Ngày… tháng…. Năm 201*	*Ngày… tháng…. Năm 201*
Trưởng khoa	**Trưởng Bộ môn**	**Người biên soạn**
(Ký và ghi rõ họ tên)	***(Ký và ghi rõ họ tên)***	***(Ký và ghi rõ họ tên)***
	Phạm Đình Thắng	**Lý Đoàn Duy Khánh**

Ngày… tháng…. Năm 201
Ban giám hiệu