ĐỀ CƯƠNG CHI TIẾT
AN NINH BẢO MẬT THÔNG TIN
Mã học phần: 33001 – Số tín chỉ: 02

Dùng cho (các) ngành: Công nghệ Thông tin
Điều kiện tiên quyết (nếu có): Cấu trúc dữ liệu và Giải thuật,
Hình thức đào tạo: Trực tiếp
Đơn vị phụ trách: Khoa Công nghệ Thông tin

1. Mô tả chung về học phần

Học phần này giới thiệu các khái niệm cơ bản về bảo mật thông tin, các phương pháp mã hóa, giải mã và ứng dụng của chúng trong bảo mật thông tin, các cơ chế và nghi thức bảo mật: Xác thực, chữ ký số. Ngoài ra, học phần này cũng giúp sinh viên vận dụng kiến thức về bảo mật thông tin đã học để giải quyết một số bài toán bảo mật trong thực tế.

2. Các chữ viết tắt (nếu có)

3. Chuẩn đầu ra của học phần

Mã	Chuẩn đầu ra học phần
plo3.1	Mô tả và giải thích thuật toán của một số sơ đồ mã khóa, sơ đồ chữ ký số, sơ đồ phân phối và thỏa thuận khóa.
plo3.2	Vận dụng các kiến thức toán học cho An toàn thông tin, Viết chương trình mã khóa, chữ ký số.
plo3.3	Mô tả và giải thích sơ đồ phân phối khóa và sơ đồ thỏa thuận khóa.

4. Giáo trình và tài liệu học tập

[1]. Phan Đình Diệu, *Lý thuyết mật mã và an toàn bảo mật thông tin*, NXB Đại học Quốc Gia Hà Nội, 2002.
[2]. William Stallings**,** *Cryptography and Network Security: Principles and Practice,* fifth ed. Prentice Hall, 2010. www.Williamstallings.com

5. 1. Tài liệu tham khảo:

[1]. A. J. Menezes, P. van Oorschot, and S. Vanstone, *Handbook of Applied Cryptography*. CRC Press, 1996. www.cacr.math.uwaterloo.ca/hac
[2]. B. Schneier, *Applied Cryptography, Protocols, Algorithms and Source Code in C*. John Wiley and Sons, 1996.

5. Chiến lược học tập

Sinh viên cần tích cực và chủ động tham gia vào quá trình học tập; cần tham gia đầy đủ các giờ học theo quy định, không ngừng phấn đấu để duy trì sự tiến bộ liên tục trong học tập; hoàn thành nhiệm vụ học tập đúng tiến độ.

Để hoàn thành tốt học phần này, sinh viên cần:

- Tích cực thực hiện các nhiệm vụ học tập do giảng viên giao;
- Tích cực nghiên cứu các giáo trình, tài liệu tham khảo mà giảng viên yêu cầu. Chủ động nghiên cứu mở rộng các tài liệu có liên quan đến bài học.
- Chủ động và tích cực làm bài tập trước khi tham dự buổi học kế tiếp.
- Thực hành để kiểm chứng lý thuyết đã học bằng cách: Viết các chương trình theo thuật toán mà giảng viên đã trình bày trên lớp, chạy chương trình và kiểm tra kết quả. Trao đổi các vấn đề mà nhóm còn thắc mắc với giảng viên và các sinh viên khác để tìm ra câu trả lời.

6. Nội dung, kế hoạch giảng dạy và đánh giá

Nội dung và kế hoạch giảng dạy, đánh giá	Hoạt động học tập của người học				Chuẩn đầu ra
	Trên lớp	ST	Tự học	SG	
Giới thiệu học phần	- Nghe giảng viên giới thiệu về học phần - Thảo luận, đặt câu hỏi có liên quan đến môn học	1	Đọc và chuẩn bị các nội dung của phần học	2	
CHƯƠNG 1: CƠ SỞ LÝ THUYẾT MẬT MÃ 1.1. Khái niệm 1.2. Cơ sở lý thuyết 1.2.1. Số nguyên 1.2.2. Đồng dư. Các vấn đề liên quan	- Nghe giảng các nội dung về cơ sở lý thuyết mật mã - Thảo luận, đặt câu hỏi trong quá trình học - Làm bài tập	5	- Đọc tài liệu, tìm hiểu các vấn đề liên quan cần thảo luận và làm rõ các vấn đề liên quan đến cơ sở toán học cho mật mã - Làm bài tập giáo viên giao cho. - Chuẩn bị câu hỏi và nội dung thảo luận	10	plo3.2
CHƯƠNG 2: HỆ MẬT MÃ KHÓA ĐỐI XỨNG 2.1. Hệ mật mã cổ điển	- Nghe giảng về hệ mật mã khoá đối xứng - Thảo luận, đặt câu	6	- Đọc tài liệu, tìm hiểu các vấn đề liên quan đến	12	plo3.1, plo3.2

2.1.1. Mã Dịch chuyển 2.1.2. Mã Hoán vị 2.1.3. Mã Thay thế 2.1.4. Mã APPHIN 2.1.5. Mã Vigenere 2.1.6. Mã HILL 2.2. Mã hóa DES	hỏi các vấn đề liên quan đến hệ mật mã khoá đối xứng - Làm bài tập		các hệ mật mã khoá đối xứng - Làm bài tập giáo viên giao cho. - Chuẩn bị câu hỏi và nội dung thảo luận của chương 2		
CHƯƠNG 3: HỆ MẬT MÃ KHÓA CÔNG KHAI 3.1. Khái niệm 3.2. Hệ mã khóa RSA 3.3. Hệ mã khóa ElGamal. 3.4. Hệ mã khóa DSS.	- Nghe giảng về các hệ mật mã khoá công khai - Thảo luận, đặt câu hỏi các vấn đề liên quan đến các hệ mật mã khoá công khai - Làm bài tập	6	- Đọc tài liệu, tìm hiểu các vấn đề liên quan đến các hệ mật mã khoá công khai - Làm bài tập giáo viên giao cho. - Chuẩn bị câu hỏi và nội dung thảo luận cho chương 3	12	plo3.1, plo3.2
CHƯƠNG 4: CHỮ KÝ SỐ 4.1. Khái niệm. 4.2. Chữ ký số RSA, ElGamal, DSS 4.3. Chữ ký không phủ nhận được	- Nghe giảng về chữ ký số - Thảo luận, đặt câu hỏi các vấn đề liên quan đến chữ ký số - Làm bài tập	6	- Đọc tài liệu, tìm hiểu các vấn đề liên quan đến chứ ký số - Làm bài tập giáo viên giao cho. - Chuẩn bị câu hỏi và nội dung thảo luận cho chương 4	12	plo3.1,plo3.2

CHƯƠNG 5: PHÂN PHỐI KHÓA VÀ THOẢ THUẬN VỀ KHÓA 5.1. Khái niệm. 5.2. Phân phối khóa. 5.3. Thỏa thuận về khóa	- Nghe giảng các nội dung về phân phối và thoả thuận khoá - Thảo luận, đặt câu hỏi - Làm bài tập	6	- Đọc tài liệu, tìm hiểu các vấn đề liên quan phân phối và thoả thuận khoá - Làm bài tập giáo viên giao cho. - Chuẩn bị câu hỏi và nội dung thảo luận cho chương 5	12	plo3.3
Tổng số tiết/giờ học		30		60	

ST-Số tiết chuẩn SG-Số giờ

7. Đánh giá kết quả học tập

Hoạt động đánh giá của học phần gồm:

Phân loại	Phương pháp đánh giá	Tỷ trọng	Chuẩn đầu ra			
			plo3.1	plo3.2	plo3.3	plo3.4
Quá trình	ĐG1: đánh giá thường xuyên	50%	x		x	
	ĐG2: báo cáo kết quả chương trình	50%		x		
Tổng cộng:		100%				

7.1. Hoạt động đánh giá 1 - Chuẩn đầu ra: **plo3.1, plo3.3 -** Tỷ lệ: **50%** điểm học phần

- Hình thức đánh giá: Đánh giá thường xuyên trong giờ học thông qua thảo luận,
- Mô tả bài đánh giá:
    - Sinh viên sẽ được yêu cầu mô tả và giải thích các phép toán, các thuật toán mã hóa khóa đối xứng và mã hóa khóa công khai, phân phối và thoả thuận khoá
- Ma trận đánh giá:

Tiêu chí đánh giá	Khung điểm				
	A	B	C	D	F
	8,5 ÷ 10	7,0 ÷ 8,4	5,5 ÷ 6,9	4,0 ÷ 5,4	< 4,0
	A	B	C	D	F
	8,5 ÷ 10	7,0 ÷ 8,4	5,5 ÷ 6,9	4,0 ÷ 5,4	< 4,0

Tiêu chí đánh giá	Khung điểm				
	A	B	C	D	F
	8,5 ÷ 10	7,0 ÷ 8,4	5,5 ÷ 6,9	4,0 ÷ 5,4	< 4,0
	A	B	C	D	F
	8,5 ÷ 10	7,0 ÷ 8,4	5,5 ÷ 6,9	4,0 ÷ 5,4	< 4,0
TC1: Mô tả và giải thích thuật toán của một số sơ đồ mã khóa, chữ ký số, phân phối và thoả thuận khoá (100%)	Mô tả và giải thích đúng, đầy đủ thuật toán, phân tích được ưu nhược điểm của các thuật toán đạt 85%-100%	Mô tả và giải thích thuật toán, phân tích được ưu nhược điểm của các thuật toán đạt mức 70%-84%.	Mô tả và giải thích thuật toán, phân tích được ưu nhược điểm của các thuật toán đạt mức 55%-69%.	Mô tả và giải thích thuật toán, phân tích được ưu nhược điểm của các thuật toán đạt mức 40%-54%	Không mô tả và giải thích được thuật toán hoặc mô tả và giải thích thuật toán đạt mức đạt dưới 40%

Kết quả đánh giá chung: ĐG1 = TC1 * 40% + TC2 * 40% + TC3 * 20%.

7.2. Hoạt động đánh giá 2 - Chuẩn đầu ra: plo3.2- Tỷ lệ: **50%** điểm học phần

- Mô tả hình thức đánh giá: Hoạt động này được thực hiện thông qua bài báo cáo của sinh viên về kết quả thực hiện cài đặt các thuật toán của một số sơ đồ chữ ký số. Sinh viên báo cáo kết quả thực hiện cài đặt chương trình.
- Mô tả bài đánh giá:
  - Sinh viên phân tích bài toán, các kiến thức toán học cơ sở dử dụng cho chương trình
  - Phân tích dữ liệu và cấu trúc dữ liệu
  - Cài đặt chương trình
  - Đánh giá kết quả thực hiện chương trình
  - Trình bày báo cáo powerpoint
- Ma trận đánh giá:

Tiêu chí đánh giá	Khung điểm				
	A	B	C	D	F
	8,5 ÷ 10	7,0 ÷ 8,4	5,5 ÷ 6,9	4,0 ÷ 5,4	< 4,0
TC1: Cài đặt các thuật toán của một số sơ đồ mã khóa và	- Phân tích bài toán và các kiến thức có sở áp dụng	- Phân tích bài toán và các kiến thức có sở áp dụng	- Phân tích bài toán và các kiến thức có	- Phân tích bài toán và các kiến thức có	- Không phân tích được

Tiêu chí đánh giá	Khung điểm				
	A	B	C	D	F
	8,5 ÷ 10	7,0 ÷ 8,4	5,5 ÷ 6,9	4,0 ÷ 5,4	< 4,0
sơ đồ chữ ký số. (70%)	đúng 100% - Cài đặt chương trình theo bài toán phân tích - Chương trình chạy tối ưu	đúng 75% - Cài đặt chương trình theo bài toán phân tích - Chương trình chạy nhưng chưa tối ưu	sở áp dụng đúng 60% - Cài đặt chương trình theo bài toán phân tích - Chương trình chạy còn một vài lỗi nhỏ	sở áp dụng đúng 40% - Cài đặt chương trình theo bài toán phân tích - Chương trình chạy còn lỗi.	- Không cài đặt được. - Chương trình chưa chạy
TC2: Trình bày kết quả, thảo luận (30%)	Rõ ràng, mạch lạc, trả lời đúng và đầy đủ	Rõ ràng, mạch lạc, trả lời đúng và đầy đủ.	Rõ ràng, mạch lạc, trả lời đúng nhưng chưa đầy đủ.	Rõ ràng, mạch lạc.	Sơ sài, không rõ ràng mạch lạc.

Kết quả đánh giá chung: ĐG2 = TC1 * 70% + TC2 * 30%.

7.3. Cách tính kết quả học tập chung của học phần

Điểm học phần = Đánh giá 1 × 50% + Đánh giá 2 × 50%

8. Các phương tiện, trang thiết bị dạy và học

- Giảng đường, phấn, máy chiếu.
- Yêu cầu đối với sinh viên: Có tài liệu môn học

9. An toàn của sinh viên và giảng viên

- Giảng viên và sinh viên phải tuân thủ các quy định về việc sử dụng các trang thiết bị điện tại phòng học.
- Trong trường hợp phát sinh các vấn đề có thể dẫn đến mất an toàn, sinh viên cần kịp thời báo cáo với giảng viên để phối hợp giải quyết.

10. Kỷ luật, khiếu nại và hỗ trợ

- Sinh viên phải có mặt trên lớp đủ thời gian theo quy định của nhà trường
- Gian lận trong hoạt động đánh giá nào sẽ hủy kết quả đánh giá đó.
- Sinh viên chưa đạt ĐG nào vẫn tiếp tục học các phần tiếp theo và sẽ được cải thiện điểm trong quá trình học.

- Sinh viên có quyền khiếu nại trực tiếp giáo viên về kết quả đánh giá ngay sau khi kết quả được công bố kết.

Sinh viên gặp bất kỳ khó khăn gì trong quá trình học tập có thể liên hệ trực tiếp với giảng viên, Trưởng khoa/bộ môn, Văn phòng hỗ trợ sinh viên, Phòng Đào tạo, Ban Thanh tra của Nhà trường để được hướng dẫn, hỗ trợ.

Chủ tịch Hội đồng **xây dựng CTĐT ngành**	*Hải Phòng, ngày tháng năm 2022* **Người biên soạn**
	Nguyễn Thị Xuân Hương