BỘ CÔNG THƯƠNG
TRƯỜNG ĐH CÔNG NGHIỆP QUẢNG NINH

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

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN
TRÌNH ĐỘ ĐÀO TẠO: ĐẠI HỌC
NGÀNH/CHUYÊN NGÀNH: CÔNG NGHỆ THÔNG TIN

1. Tên học phần:

Tiếng Việt: **Đảm bảo và an toàn thông tin**

Tiếng Anh: **Information security and safety**

Mã số học phần:

Số tín chỉ học phần: 03 (lý thuyết, thực hành)

Số tiết học phần:

Lý thuyết: 30; Thực hành: 30

Tự học: 90

2. Đơn vị quản lý học phần:

2.1. Giảng viên giảng dạy:

1. ThS. Đặng Đình Đức
2. TS. Trần Văn Liêm

2.2. Bộ môn: Mạng và Công nghệ phần mềm

2.3. Khoa: Công nghệ thông tin

3. Điều kiện tiên quyết học phần

3.1. Học phần tiên quyết: Không

3.2. Học phần học trước: không

4. Mục tiêu của học phần:

Cuộc cách mạng 4.0 đã dẫn đến sự bao trùm của công nghệ thông tin vào mọi lĩnh vực. Nguy cơ mất an toàn hệ thống thông tin gia tăng. Việc đảm bảo an toàn an ninh hệ thống thông tin là yếu tố then chốt. Đảm bảo an toàn thông tin nhằm bảo vệ tài nguyên hệ thống và bảo đảm tính riêng tư. Các hệ thống máy tính lưu trữ rất nhiều thông tin và tài nguyên. Đây đều là những dữ liệu quan trọng, cần được bảo vệ hàng đầu.

4.1. Kiến thức:

4.1.1. Hiểu biết rõ cơ sở luật pháp, chính sách an ninh mạng, quản lý rủi ro, quá trình xây dựng hệ thống an toàn, vấn đề an toàn hệ thống và an ninh mạng trong thực tiễn;

4.1.2. Nắm được tổng quan về mục tiêu của an toàn và bảo mật hệ thống thông tin. Nắm rõ một số hiện trạng về tình hình an toàn và bảo mật hệ thống thông tin hiện tại;

4.1.3. Một số vấn đề cần quan tâm trong trong an toàn và bảo mật hệ thống thông tin cũng như các chính sách, tiêu chuẩn, chỉ dẫn trong an toàn bảo mật hệ thống thông tin;

4.1.4. Hiểu rõ các thành phần của một hệ mật mã, các thuật toán mã hóa cổ điển, hiện đại cũng như cung cấp những yếu tố bảo mật then chốt như xác thực, tính toàn vẹn và không thu hồi;

4.1.5. Hiểu biết các mô hình mã hóa, các kỹ thuật mã hóa hiện đại và các đánh giá liên quan đến thời gian mã hóa, thám mã.

4.1.6. Hiểu biết về cách quản lý khóa cũng như sử dụng hàm băm và chữ ký số trong việc mã hóa thông tin cũng như đánh giá độ an toàn và một số ứng dụng của mã mật

4.1.7. Hiểu các kiến thức cơ bản về truyền thông mạng, an ninh mạng, xác định các lỗ hổng bảo mật, đe dọa và xây dựng các chính sách bảo mật, các nguy cơ đối với một hệ thống thông tin cũng như các thông tin về tấn công và các giải pháp cũng như các kỹ thuật để đảm bảo an toàn hệ thống thông tin

4.2. Kỹ năng:

4.2.1. Thành thạo các phương pháp mã hóa cổ điển, hiện đại để ứng dụng trong các giao thức mạng phục vụ mục đích đảm bảo an toàn cho truyền thông tin;

4.2.2. Thành thạo kỹ năng xây dựng các giải pháp đảm bảo an ninh của các hệ thống mạng cũng như nguy cơ, các dạng tấn công và một số kỹ thuật xâm nhập hệ thống mạng;

4.2.3. Khai thác có hiệu quả và sử dụng thành thạo một số phần mềm, công cụ để ngăn chặn, phân tích và xử lý một số phần mềm độc hại tấn công vào hệ thống thông tin;

4.2.4. Thành thạo kỹ năng ứng dụng các giải pháp kỹ thuật trong các ứng dụng bảo vệ mạng máy tính.

4.2.5. Thành thạo cách quản lý khóa cũng như sử dụng hàm băm và chữ ký số trong việc mã hóa thông tin cũng như đánh giá độ an toàn và một số ứng dụng của mã mật

4.2.6. Sử dụng thành thạo một số phần mềm tiện ích và phần mềm công cụ để phục hồi, bảo vệ cho hệ thống thông tin; cũng như áp dụng một cách thích hợp các kỹ thuật căn bản đảm bảo an toàn truyền thông và an toàn hệ thống khi bị tấn công trên mạng;

4.3. Năng lực tự chủ và trách nhiệm:

4.3.1. Có ý thức và tinh thần trách nhiệm, thái độ và đạo đức đúng đắn, ý thức kỷ luật và tác phong công nghiệp để đáp ứng yêu cầu thực tế mà công việc đòi hỏi;

4.3.2. Có phương pháp làm việc khoa học, khả năng làm việc độc lập, làm việc theo nhóm, khả năng tự nghiên cứu và nâng cao chất lượng học tập;

4.3.3. Có tinh thần trách nhiệm với bản thân và tập thể, tinh thần học hỏi, ý trí vươn lên để hoàn thiện bản thân để tiếp tục học tập ở các trình độ cao hơn.

5. Chuẩn đầu ra học phần

Sau khi hoàn thành việc học học phần này, sinh viên có thể:

1. Nắm rõ cơ sở luật pháp, chính sách an ninh mạng, quản lý rủi ro, quá trình xây dựng hệ thống an toàn, vấn đề an toàn hệ thống và an ninh mạng trong thực tiễn;

2. Hiểu rõ các thành phần của một hệ mật mã, các thuật toán mã hóa cổ điển, hiện đại cũng như cung cấp những yếu tố bảo mật then chốt như xác thực, tính toàn vẹn và không thu hồi;

3. Hiểu và vận dụng được các mô hình mã hóa, các kỹ thuật mã hóa và các đánh giá liên quan đến thời gian mã hóa, thám mã.

4. Làm chủ được những điểm quan trọng trong cách quản lý khóa cũng như sử dụng hàm băm và chữ ký số trong việc mã hóa thông tin cũng như đánh giá độ an toàn và một số ứng dụng của mã mật, cũng như suy luận toán học đánh giá độ an toàn hệ thống.

5. Phân tích và ứng dụng thành thạo một số phần mềm tiện ích và các công cụ để phục hồi và bảo mật cho hệ thống thông tin khi bị tấn công trên mạng;

6. Tóm tắt nội dung học phần

Học phần trang bị cho sinh viên những kiến thức cơ bản về các khái niệm mang tính chất cơ sở của lĩnh vực an toàn hệ thống thông tin, nguyên lý hoạt động của các giải thuật mã hóa đối xứng hiện đại và sơ đồ mã hóa khối tổng quát Feistel. Các phương thức mã hóa liên hợp nhiều khối và cách thức chung quản lý các khóa bí mật. Các ứng dụng bảo mật, chữ ký số, và trao đổi khóa bí mật của mật mã khóa công khai. Các cơ chế xác thực thông báo và tác giả của thông báo. Các ứng dụng của các phương pháp mật mã, xác thực và chữ ký số trong lĩnh vực an toàn cho hệ thống thông tin.

7. Cấu trúc nội dung học phần

Đề mục	Nội dung	Số tiết			Mục tiêu
		Tổng	LT	TH/TN	
Chương 1	**Tổng quan về an toàn thông tin**	**4**	**2**	**2**	
1.1	Khái niệm về An toàn hệ thống thông tin	2	1	1	4 .1.1
1.2	Các mục tiêu an toàn				
1.3	Các mối đe dọa	2	1	1	4.1.2
1.4	Quản lý các nguy cơ mất an toàn trên HTTT				4.1.3
1.5	Các giải pháp đảm bảo ATTT				
Chương 2	**Chương 2. Mã hóa cổ điển**	**16**	**8**	**8**	
2.1	Mã Ceasar	4	2	2	4.1.4
2.2.	Mã Nhị phân				
2.3.	Mã thay thế	4	2	2	
2.4.	Mã dịch vòng				
2.5.	Mã Affine	4	2	2	
2.6.	Mã Vigenere	4	2	2	

2.7	Hệ mã Hill				
	Kiểm tra bài 1				
Chương 3	**Kỹ thuật mã hóa bí mật**	**8**	**4**	**4**	
3.1	Mã khối hiện đại	4	2	2	4.1.4 4.1.5
3.2	Chuẩn mã dữ liệu DES				
3.3	Chuẩn mã nâng cao AES	4	2	2	
3.4	Các mã đối xứng hiện đại				
3.5	Bảo mật dùng mã đối xứng				
Chương 4	**Kỹ thuật mã hóa công khai**	**12**	**6**	**6**	
4.1	Cấu trúc hệ thống mật mã bất đối xứng	4	2	2	4.1.3
4.2	Thuật toán mật mã RSA				
4.3	Thuật toán trao đổi khoá Diffie-Hellman	4	2	2	
4.4	Đánh giá kỹ thuật mật mã bất đối xứng	4	2	2	
	Kiểm tra bài 2				
Chương 5	**Quản lý khóa, hàm băm và chữ ký số**	**8**	**4**	**4**	
5.1	Quản lý khóa	4	2	2	4.1.6 4.1.7
5.2	Hàm Băm				
5.3	Chữ ký số	4	2	2	
Chương 6	**Ứng dụng bảo mật trong HTTT**	**12**	**6**	**6**	
6.1	Giao thức xác thực	4	2	2	4.1.6 4.1.7
6.2	IPSec				
6.3	SSL	4	2	2	
6.4	SET	4	2	2	
	Kiểm tra bài 3				
	Tổng cộng	**60**	**30**	**30**	

8. Phương pháp giảng dạy

- Giảng dạy lý thuyết kết hợp thảo luận theo nhóm
- Phương pháp Suy nghĩ - Chia sẻ.
- Phương pháp thực hành

9. Nhiệm vụ của sinh viên:

Sinh viên phải thực hiện các nhiệm vụ sau:

- Có mặt tối thiểu 70% số tiết học lý thuyết.
- Tham gia và hoàn thành đầy đủ các buổi thao luận, bài tập nhóm/bài tập và được đánh giá kết quả thực hiện.
- Tham dự kiểm tra giữa học kỳ.

- Chủ động chuẩn bị các nội dung và thực hiện giờ tự học theo mục 12
- Thực hiện các hoạt động khác theo yêu cầu của giảng viên.

10. Đánh giá kết quả học tập của sinh viên

10.1. Cách đánh giá

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

TT	Điểm thành phần	Quy định	Trọng số	Ghi chú
1	Điểm chuyên cần	Số tiết sinh viên tham dự học/tổng số tiết quy định. Ý thức, thái độ học tập trên lớp, ý thức chuẩn bị bài, làm bài tập … của sinh viên.	10%	Sinh viên không tham dự đủ 70% số tiết học trên lớp thì không được dự thi kết thúc học phần
2	Điểm quá trình	Bài tập lớn + Thực hành	30%	
3	Điểm thi kết thúc học phần	Vấn đáp + Thực hành	60%	

10.2. Cách tính điểm:

Điểm học phần bao gồm điểm kiểm tra thường xuyên trong quá trình học tập; điểm đánh giá nhận thức và thái độ tham gia thảo luận; điểm đánh giá phần thực hành; điểm chuyên cần; điểm thi giữa học phần; điểm tiểu luận và điểm thi kết thúc học phần thực hiện theo công thức sau:

Điểm học phần	=	Điểm chuyên cần x 0.1	+	Điểm quá trình x 0.3	+	Điểm thi kết thúc học phần x 0.6

Điểm học phần tính theo thang điểm 10 làm tròn đến một chữ số thập phân, sau đó được quy đổi sang điểm chữ và điểm số theo thang điểm 4 theo quy chế đào tạo của Nhà trường.

11. Tài liệu học tập:

- Giáo trình học tập chính:

[1]. Giáo trình Đảm bảo và an toàn thông tin - Trường Đại học Công nghiệp Quảng Ninh.

[2]. Lab thực hành Bảo đảm an toàn thông tin, Trường Đại học Công nghiệp Quảng Ninh.

- Tài liệu tham khảo:

[3] Trần Đức Sự, Nguyễn Văn Tảo, Trần Thị Lượng, Giáo trình An toàn và bảo mật dữ liệu, NXB Đại học Thái Nguyên, 2015

[4] TS. Thái Thanh Tùng, Giáo trình Mật mã học an toàn dữ liệu, NXB Thông tin và truyền thông, 2011;

[5] TS. Trần Văn Dũng, Bài giảng An toàn và bảo mật thông tin, Trường Đại học Giao thông vận tải, 2009;

[6]. Lab thực hành Đảm bảo an toàn thông tin, Trường Đại học Công nghiệp Quảng Ninh, 2017

12. Hướng dẫn tự học của học phần

Chương	Nội dung	LT (tiết)	BT (tiết)	TH (tiết)	Sinh viên cần chuẩn bị
1	1. Các mục tiêu an toàn 2. Các mối đe dọa 3. Các giải pháp đảm bảo ATTT	5	2	5	Tài liệu [1] Chương 1 Tài liệu [2] Chương 1
2	1. Mã Ceasar 2. Mã Nhị phân 3. Mã thay thế 4. Mã dịch vòng 5. Mã Affine 6. Mã Vigenere 7. Hệ mã Hill	10	2	15	Tài liệu [1] Chương 2 Tài liệu [2] Chương 2
3	1. Chuẩn mã dữ liệu DES 2. Các mã đối xứng hiện đại 3. Bảo mật dùng mã đối xứng	5	3	5	Tài liệu [1] Chương 3 Tài liệu [2] Chương 3
4	1. Thuật toán mật mã RSA 2. Thuật toán trao đổi khoá Diffie-Hellman	5	3	5	Tài liệu [1] Chương 4 Tài liệu [2] Chương 4
5	1. Quản lý khóa 2. Hàm Băm 3. Chữ ký số	5	2	5	Tài liệu [1] Chương 5 Tài liệu [2] Chương 5
6	1. IPSec 2. SSL 3. SET	5	3	5	Tài liệu [1] Chương 6 Tài liệu [2] Chương 6
	Tổng cộng	**35**	**15**	**40**	

Quảng Ninh, ngày 7 tháng 11 năm 2022

HIỆU TRƯỞNG	TRƯỞNG BỘ MÔN	GIẢNG VIÊN BIÊN SOẠN
TS. Hoàng Hùng Thắng	ThS. Đặng Đình Đức	ThS. Đặng Đình Đức