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: *Mật mã*

Tiếng Anh: *Cipher*

Mã số học phần: 02DHKHMT113

Số tín chỉ học phần: 03 tín chỉ (LT: 03, TH: 0)

Số tiết học phần:

Lý thuyết: 45

Tự học: 105

2. Đơn vị quản lý học phần

2.1. Giảng viên giảng dạy: ThS. Phạm Thúy Hằng

2.2. Bộ môn: Khoa học máy tính

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

Trang bị cho sinh viên nắm vững được tính chất, ý nghĩa và công dụng của các nhóm thuật toán trong lĩnh vực mã hóa: Mã hóa đối xứng, mã hoá bất đối xứng, chữ ký điện tử, hàm băm mật mã, phân phối khóa. 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, quy trình để bảo vệ thông tin trong hệ thống phần mềm.

4.1. Kiến thức:

4.1.1. Trang bị cho sinh viên những kiến thức cơ bản về vấn đề an toàn và bảo mật thông tin;

4.1.2. Nắm vững các hệ mã hóa cổ điển, các hệ mã hóa đối xứng, bất đối xứng;

4.1.3. Nắm vững các hàm băm và hệ chữ ký điện tử thông dụng hiện nay, vấn đề phân phối và thỏa thuận khóa.

4.2. Kỹ năng:

4.2.1. Có khả năng vận dụng (cài đặt mới hay dùng từ một thư viện có sẵn) cho một ứng dụng cụ thể;

4.2.2. Có khả năng vận dụng chữ ký điện tử vào một ứng dụng cụ thể;

4.2.3. Có khả năng đánh giá mức an toàn của một hệ thống trong thực tế đang dùng kỹ thuật mã hóa, chữ ký điện tử để tù đó chọn được một giải pháp phù hợp để cài đặt.

4.3. Thái độ:

4.3.1. Học tập tích cực, nghiêm túc;

4.3.2. Rèn luyện tác phong làm việc khoa học, chuẩn xác;

4.3.3. Có ý thức kỷ luật, tôn trọng nội quy lớp học.

5. Chuẩn đầu ra học phần

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

1. Hiểu rõ về các vấn đề an toàn và bảo mật thông tin;
2. Hiểu rõ và vận dụng cài đặt được các hệ mã khóa đối xứng, khóa công khai thông dụng hiện nay để tăng cường an ninh cho các hệ thống phần mềm cụ thể;
3. Hiểu rõ và cài đặt được các chữ ký điện tử, hàm băm, vấn đề phân phối khóa và thỏa thuận khóa;
4. Khả năng vận dụng môn học để đánh giá và giải quyết các bài toán trong thực tế.

6. Tóm tắt nội dung học phần

Học phần trình bày kiến thức tổng quan về mật mã, cơ sở toán học của lý thuyết mật mã. Giới thiệu các hệ mật mã khóa đối xứng, các hệ mật mã khóa công khai, bài toán xác nhận và chữ ký điện tử.

7. Cấu trúc nội dung học phần

Đề mục	Nội dung	Số tiết			Mục tiêu
		Tổng	Lý thuyết	Thực hành	
Chương 1	**Giới thiệu chung về mật mã**	**3**	**3**	**0**	4.1.1, 4.1.2, 4.2.1, 4.2.2, 4.3.1, 4.3.2, 4.3.3
1.1	Sơ lược về lịch sử về mật mã	0.5	0.5		
1.2	Các hệ thống mật mã.	1	1		
1.3	Mật mã khóa đối xứng, mật mã khóa công khai	1	1		
1.4	Các bài toán an toàn thông tin. Thám mã và tính an toàn của các hệ mật mã	0.5	0.5		
Chương 2	**Các hệ mật mã khóa đối xứng**	**19**	**19**	**0**	4.1.1, 4.1.2, 4.2.1, 4.2.2, 4.3.1, 4.3.2, 4.3.3
2.1	Một số hệ mật khóa cổ điển	1	1		
2.2.	Mã chuyển dịch	1.5	1.5		
2.3.	Mã thay thế	1.5	1.5		
2.4.	Mã apphin	1.5	1.5		
2.5.	Mã Vigene`re	1.5	1.5		
2.6	Mã Hill	1.5	1.5		
2.7	Mã hoán vị	1.5	1.5		

Đề mục	Nội dung	Số tiết			Mục tiêu
		Tổng	Lý thuyết	Thực hành	
2.8	Thám mã đối với mã apphin	1.5	1.5		
2.9	Thám mã đối với mã Vigene`re	1.5	1.5		
2.10	Thám mã đối với mã Hill	1.5	1.5		
2.11	Mật mã theo dòng	1.5	1.5		
2.12	Hệ mật mã chuẩn DES	1.5	1.5		
2.13	Vấn đề an toàn và việc thám mã đôi với DES	1.5	1.5		
Chương 3	**Các hệ mật khoá công khai**	**13**	**13**	**0**	
3.1	Giới thiệu mở đầu	3	3		4.1.1,
3.2	Hệ mật khóa công khai RSA	2	2		4.1.3,
3.3	Hệ mật khóa công khai Rabin	2	2		4.2.1,
3.4	Hệ mật khóa công khai ElGamal	2	2		4.2.3,
3.5	Các hệ mật mã dựa trên các bài toán NP-đầy đủ	2	2		4.3.1, 4.3.2, 4.3.3
3.6	Hệ mật đường cong Eliptic	2	2		
Chương 4	**Bài toán xác nhận và chữ ký điện tử**	**5**	**5**	**0**	4.1.1, 4.1.3,
4.1	Bài toán xác nhận và sơ đồ chữ ký	1	1		4.2.1,
4.2	Sơ đồ chữ ký ElGamal và chuẩn chữ ký điện tử	2	2		4.2.3, 4.3.1,
4.3	Hàm băm và chữ ký	2	2		4.3.2, 4.3.3
Chương 5	**Vấn đề phân phối khóa và thỏa thuận khóa**	5	5		4.1.1,
5.1	Quản trị khóa trong các mạng truyền tin	0.5	0.5		4.1.3, 4.2.1,
5.2	Sơ đồ phân phối khóa Blom	1.5	1.5		4.2.3,
5.3	Giao thức trao đổi khóa Diffie-Hellman	1.5	1.5		4.3.1, 4.3.2, 4.3.3
5.4	Hệ phân phối khóa Kerberos	1.5	1.5		

8. Phương pháp giảng dạy

- Giảng dạy lý thuyết kết hợp hướng dẫn giải trực quan các ví dụ minh họa, bài tập mẫu;
- Đưa ra các bài tập để sinh viên thảo luận tìm phương pháp giải quyết thích hợp;
- Giao bài tập về nhà và có kiểm tra trong buổi học tiếp theo.

9. Nhiệm vụ của sinh viên

Sinh viên phải thực hiện các nhiệm vụ sau:

- Có mặt tối thiểu 70% số giờ học trên lớp có sự hướng dẫn của giảng viên.
- Làm bài tập đầy đủ và đọc tài liệu giảng viên yêu cầu.
- Làm bài kiểm tra giữa kỳ và thi kết thúc học phần.
- Chủ động chuẩn bị dụng cụ học tập: Bài giảng, sách tham khảo, máy tính cá nhân.

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: 5% - Ý thức, thái độ học tập trên lớp, ý thức chuẩn bị bài, làm bài tập …: 5%	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	- Hình thức kiểm tra: Thực hành trên máy tính. - Số lượng bài kiểm tra: 03	30%	
3	Điểm thi kết thúc học phần	Thi tự luận (90 phút)	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 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:

11.1. Tài liệu chính:

[1] ThS. Phạm Thúy Hằng, *Giáo trình Mật mã*, Trường Đại học Công nghiệp Quảng Ninh, Nhà xuất bản Công thương, 2022.

11.2. Tài liệu tham khảo:

[2] Phan Đình Diệu, *Lý thuyết mật mã và an toàn thông tin,* NXB Đại học Quốc Gia Hà Nội.

[3] Douglas R. Stinson. Cryptography. Theory and Practice, CRC Press,1995

[4] TS. Thái Thanh Tùng, *Giáo trình mật mã học và an toàn thông tin,* NXB thông tin và truyền thông.

12. Hướng dẫn tự học của học phần

Chương	Nội dung	LT (tiết)	BT (tiết)	Sinh viên cần chuẩn bị
1	Giới thiệu chung về mật mã	5	5	Tài liệu [1]: Chương 1
2	Các hệ mật mã khóa đối xứng	20	20	Tài liệu [1]: Chương 2
3	Các hệ mật khoá công khai	15	20	Tài liệu [1]: Chương 3
4	Bài toán xác nhận và chữ ký điện tử	5	5	Tài liệu [1]: Chương 4
5	Vấn đề phân phối khóa và thỏa thuận khóa	5	5	Tài liệu [1]: Chương 5

Quảng Ninh, ngày 28 tháng 11 năm 2022

HIỆU TRƯỞNG	P. TRƯỞNG BỘ MÔN	GIẢNG VIÊN BIÊN SOẠN
TS. Hoàng Hùng Thắng	ThS. Đoàn Thùy Dương	ThS. Phạm Thúy Hằng