BỘ CÔNG THƯƠNG
TRƯỜNG ĐH CÔNG NGHIỆP QUẢNG NINH

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

CHƯƠNG TRÌNH CHI TIẾT HỌC PHẦN
TRÌNH ĐỘ ĐẠI HỌC
Ngành/Chuyên ngành đào tạo: Hệ thống thông tin

1. Tên học phần: Mật mã

2. Loại học phần: Lý thuyết

3. Số tín chỉ: 03 tín chỉ. Trong đó (LT: 03; TH:0)

4. Bộ môn quản lý học phần: Khoa học máy tính

5. Điều kiện tiên quyết: Không

6. Phân bổ thời gian:

- **Thời gian lên lớp:** 45 tiết
  Số tiết lý thuyết: 42 tiết
  Số tiết thực hành: 0 tiết
  Số tiết kiểm tra: 03 tiết
- **Thời gian tự học:** 90 tiết.

7. Mục tiêu của học phần:

7.1. Kiến thức

- Hiểu được khái niệm mật mã, cơ sở toán học của lý thuyết mật mã
- Hiểu các kỹ thuật mật mã khóa đối xứng và mật mã khóa công khai.
- Biết phương pháp tạo chữ ký điện tử và phương pháp quản lý khóa.

7.2. Kỹ năng

- Biết xây dựng các thuật toán mật mã khóa đối xứng và công khai
- Xây dựng chữ ký số.
- Cài đặt các thuật toán.

7.3. Thái độ

- Có ý thức kỷ luật học tập, tinh thần khám phá kiến thức có liên quan đếnphân tích thiết kế hệ thống hướng đối tượng.
- Rèn luyện tác phong làm việc khoa học, theo nhóm.
- Tôn trọng nội quy lớp học,đi học đầy đủ, lên lớp đúng giờ, chuẩn bị bài trước khi đến lớp, tham gia tích cực trong giờ học.
- Nhận thức đúng đắn về tầm quan trọng và vị trí môn học trong hệ thống các môn học CNTT.

8. Nội dung học phần

8.1. Mô tả vắn tắt

Môn học gồm 05 chương với nội dung cơ bản như sau:

- Chương 1: Giới thiệu chung về mật mã
- Chương 2: Cơ sở toán học của lý thuyết mật mã
- Chương 3: Các hệ mật mã khóa đối xứng

- Chương 4: Các hệ mật mã khóa công khai
- Chương 5: Bài toán xác nhận và chữ ký điện tử

8.2. Nội dung chi tiết học phần

Tuần	Nội dung	LT (tiết)	TH (tiết)	Tài liệu đọc trước	Nhiệm vụ của sinh viên
Tuần 1	**Chương 1: Giới thiệu chung về mật mã** 1.1. Sơ lược lịch sử phát triển của mật mã 1.2. Các hệ thống mật mã 1.3.Mật mã khóa đối xứng và mật mã có khóa công khai	3		**Tài liệu [1]** Chương 1(từ 1.1 – 1.3)	- Chuẩn bị và đọc trước nội dung bài học trong **Tài liệu [1]** Chương 1 (từ 1.4 – 1.5) - Trả lời câu hỏi trong **Tài liệu [1]**, chương 1.
Tuần 2	1.4. Các bài toán an toàn thông tin 1.5. Thám mã và tính an toàn của các hệ mật mã	3		**Tài liệu [1]** Chương 1 (từ 1.4 – 1.5)	- Chuẩn bị và đọc trước nội dung bài học trong **Tài liệu [1]** Chương 2 - Trả lời câu hỏi trong **Tài liệu [1]**, chương 1.
Tuần 3	**Chương 2: Cơ sở toán học của lý thuyết mật mã** 2.1. Lý thuyết số 2.2. Lý thuyết về độ phức tạp tính toán 2.3. Hàm một phía và hàm cửa sập một phía	3		**Tài liệu [1]** Chương 2	- Chuẩn bị và đọc trước nội dung bài học trong **Tài liệu [1]** Chương 3(từ 3.1.1 – 3.1.3) - Làm bài tập trong **Tài liệu [1]**, chương 2
Tuần 4	**Chương 3: Các hệ mật mã khóa đối xứng** 3.1. Một số hệ mật mã cổ điển 3.1.1. Mã chuyển dịch 3.1.2. Mã thay thế 3.1.3. Mã apphin	3		**Tài liệu [1]** Chương 3(từ 3.1.1 – 3.1.3)	- Chuẩn bị và đọc trước nội dung bài học trong **Tài liệu [1]** Chương 3(từ 3.1.4 – 3.1.6) - Làm bài tậptrong **Tài liệu [1]**, chương 3
Tuần 5	3.1.4. Mã Vigenere 3.1.5. Mã Hill 3.1.6. Mã hoán vị	2		**Tài liệu [1]** Chương 3(từ 3.1.4 – 3.1.6)	- Chuẩn bị và đọc trước nội dung bài học trong **Tài liệu [1]** Chương 3 mục 3.2. - Làm bài tập trong

Tuần	Nội dung	LT (tiết)	TH (tiết)	Tài liệu đọc trước	Nhiệm vụ của sinh viên
					Tài liệu [1], chương 3
	Kiểm tra bài 1	1			
Tuần 6	3.2. Thám mã đối với các hệ mật mã cổ điển 3.2.1. Thám mã đối với mã apphin 3.2.2. Thám mã đối với mã vigenere	3		**Tài liệu [1]** Chương 3 mục 3.2	- Chuẩn bị và đọc trước nội dung bài học trong **Tài liệu [1]** mục 3.3 - Làm bài tập trong **Tài liệu [1]**, chương 3
Tuần 7	3.3. Mật mã theo dòng và các dãy số giả ngẫu nhiên 3.3.1. Mật mã theo dòng 3.3.2. Mã dòng với dòng khóa sinh bởi hệ thức truy toán 3.3.3. Mã dòng với dòng khóa là dãy số giả ngẫu nhiên	3		**Tài liệu [1]** Chương 3 mục 3.3	- Chuẩn bị và đọc trước nội dung bài học trong **Tài liệu [1]** Chương 3 mục 3.4 - Làm bài tập trong **Tài liệu [1]**, chương 3
Tuần 8	3.4. Hệ mật mã chuẩn DES 3.4.1. Giới thiệu hệ mã chuẩn 3.4.2. Mô tả hệ mật mã chuẩn DES 3.4.3. Các cách dùng DES 3.4.4. Về tính an toàn và việc thám mã đối với DES	3		**Tài liệu [1]** Chương3 mục 3.4	- Chuẩn bị và đọc trước nội dung bài học trong **Tài liệu [1]** Chương 4 mục 4.1 - Làm bài tập trong **Tài liệu [1]**, chương 3
Tuần 9	**Chương 4: Các hệ mật mã khóa công khai** 4.1. Giới thiệu hệ mật khóa công khai 4.1.1. Sự ra đời của mật mã khóa công khai 4.1.2. Một số bài toán cơ bản	3		**Tài liệu [1]** Chương 4 mục 4.1	- Chuẩn bị và đọc trước nội dung bài học trong **Tài liệu [1]** Chương 4 mục 4.2 - Làm bài tập trong **Tài liệu [1]**, chương 4
Tuần 10	4.2. Hệ mật khóa công khai RSA 4.2.1. Mô tả hệ mật RSA 4.2.2. Thực hiện hệ mật mã RSA 4.2.3. Tính bảo mật của mật mã RSA	3		**Tài liệu [1]** Chương 4 mục 4.2	- Chuẩn bị và đọc trước nội dung bài học trong **Tài liệu [1]** Chương 4 mục 4.3 - Làm bài tập trong **Tài liệu [1]**, chương 4

Tuần	Nội dung	LT (tiết)	TH (tiết)	Tài liệu đọc trước	Nhiệm vụ của sinh viên
Tuần 11	4.3. Hệ mật khóa công khai Rabin 4.3.1. Mô tả hệ mật mã Rabin 4.3.2. Tính an toàn của hệ mật mã Rabin	2		**Tài liệu [1]** Chương 4 mục 4.3	- Chuẩn bị và đọc trước nội dung bài học trong **Tài liệu [1]** Chương 4 mục 4.4 - Làm bài tập trong **Tài liệu [1]**, chương 4
	Kiểm tra bài 2	1			
Tuần 12	4.4. Hệ mật khóa công khai Elgamal 4.4.1. Mô tả hệ mật mã Elgamal 4.4.2. Tính an toàn của hệ mật mã Elgamal 4.4.3. Các hệ mật mã tương tự Elgamal	3		**Tài liệu [1]** Chương 4 mục 4.4	- Chuẩn bị và đọc trước nội dung bài học trong **Tài liệu [1]** Chương 4 mục 4.5 - Làm bài tập trong **Tài liệu [1]**, chương 4
Tuần 13	4.5. Các hệ mật mã dựa trên các bài toán NP-đầy đủ 4.5.1. Nguyên tắc chung 4.5.2. Hệ mật mã Merkle-Hellman 4.5.3. Hệ mật mã McEliece	3		**Tài liệu [1]** Chương 4 mục 4.5	- Chuẩn bị và đọc trước nội dung bài học trong **Tài liệu [1]** Chương 5 mục 5.1 - Làm bài tậptrong **Tài liệu [1]**, chương 4
Tuần 14	**Chương 5: Bài toán xác nhận và chữ ký điện tử** 5.1. Bài toán xác nhận và sơ đồ chữ ký 5.1.1 Đặt vấn đề 5.1.2. Định nghĩa sơ đồ chữ ký 5.1.3. Sơ đồ chữ ký RSA	2		**Tài liệu [1]** Chương 5 mục 5.1	- Chuẩn bị và đọc trước nội dung bài học trong **Tài liệu [1]**Chương 5 mục 5.2-5.3 - Làm bài tập trong **Tài liệu [1]**, chương
	Kiểm tra bài 3	1			
Tuần 15	5.2. Sơ đồ chữ ký Elgamal và chuẩn chữ ký điện tử 5.2.1. Sơ đồ chữ ký Elgamal 5.2.2. Tính an toàn của sơ đồ chữ ký Elgamal 5.2.3. Chuẩn chữ ký số (Digital signature standard) 5.3. Một số sơ đồ chữ ký khác	3		**Tài liệu [1]** Chương 5 mục 5.2-5.3	- Làm bài tậptrong **Tài liệu [1]** - Ôn tập chuẩn bị cho bài thi kết thúc học phần.

Tuần	Nội dung	LT (tiết)	TH (tiết)	Tài liệu đọc trước	Nhiệm vụ của sinh viên
	Ôn tập				
Tổng		**45**			

9. Nhiệm vụ của sinh viên:

- Dự lớp: 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.
- Dụng cụ học tập: Bài giảng, sách tham khảo, máy tính.

10. Thang điểm và hình thức đánh giá:

- **Thang điểm:** 10 (0 – 10)
- **Hình thức đánh giá:**
  + Sinh viên không tham gia đủ 70% số tiết học trên lớp không được dự thi kết thúc học phần và nhận điểm 0.
  + Điểm thành phần để điểm lẻ đến một chữ số thập phân.
  + Điểm học phần làm tròn đến phần nguyên.

11. Tiêu chuẩn đánh giá sinh viên

TT	Điểm thành phần	Quy định	Trọng số	Ghi chú
1	Điểm thường xuyên, đánh giá nhận thức, thái độ thảo luận, chuyên cần, làm bài tập ở nhà, …	1 điểm	10%	
2	Điểm kiểm tra giữa kỳ	3 bài.	30%	Trắc nghiệm + tự luận
3	Thi kết thúc học phần	Thi tự luận	60%	Thời gian 90 phút

12. Tài liệu học tập

- Giáo trình bắt buộc:

[1] Bài giảng Mật mã, Khoa công nghệ thông tin, Trường Đại học Công nghiệp Quảng Ninh.

- Tài liệu tham khảo:

[2] Phan Đình Diệu, Lý thuyết mật mã và An toàn thông tin, 2004.

[3] Modern Cryptography theory and practice.

13. Các yêu cầu khác (nếu có) của học phần:

Quảng Ninh, ngày 02 tháng 3 năm 2020

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