BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC DÂN LẬP HẢI PHÒNG

ISO 9001:2008

ĐỀ CƯƠNG CHI TIẾT

MÔN HỌC

AN TOÀN VÀ BẢO MẬT THÔNG TIN

Mã môn: SSI33021

Dùng cho các ngành

CÔNG NGHỆ THÔNG TIN

Bộ môn phụ trách

CÔNG NGHỆ PHẦN MỀM

THÔNG TIN VỀ CÁC GIẢNG VIÊN
CÓ THỂ THAM GIA GIẢNG DẠY MÔN HỌC

1.ThS. Lê Thụy – Giảng viên cơ hữu

- Chức danh, học hàm, học vị: Thạc sỹ .....
- Thuộc bộ môn: Công nghệ phần mềm .....
- Địa chỉ liên hệ: Khoa Công nghệ thông tin – Trường Đại học dl Hải Phòng .....
- Điện thoại: 0983322011 ..... Email: thuyle@hpu.edu.vn .....
- Các hướng nghiên cứu chính: Bảo mật, Xử lý ảnh, Hệ thống thông tin.

2. **ThS. Hồ Thị Hương Thơm** – Giảng viên cơ hữu

- Chức danh, học hàm, học vị: Thạc sỹ .....
- Thuộc bộ môn: Công nghệ phần mềm .....
- Địa chỉ liên hệ: Khoa Công nghệ thông tin – Trường Đại học DL Hải Phòng .....
- Điện thoại: 0976123446 ..... Email: thomhth@hpu.edu.vn .....
- Các hướng nghiên cứu chính: Bảo mật, Hệ thống thông tin

3. **Thông tin về trợ giảng** (nếu có):

- Họ và tên: .....
- Chức danh, học hàm, học vị: .....
- Thuộc bộ môn/lớp: .....
- Địa chỉ liên hệ: .....
- Điện thoại: ..... Email: .....
- Các hướng nghiên cứu chính: .....

THÔNG TIN VỀ MÔN HỌC

1. Thông tin chung:

- Số đơn vị học trình/ tín chỉ: 4/2
- Các môn học tiên quyết: Toán cao cấp, Phương pháp tính, Lập trình C, Cấu trúc dữ liệu và giải thuật
- Các môn học kế tiếp: .....
- Các yêu cầu đối với môn học (nếu có): .....
- Thời gian phân bổ đối với các hoạt động:
  + Nghe giảng lý thuyết: 23
  + Làm bài tập trên lớp: 3
  + Thảo luận: 2
  + Thực hành, thực tập (ở PTN, nhà máy, điền dó,...): 15
  + Hoạt động theo nhóm: 0
  + Tự học: 50
  + Kiểm tra: 2

2. Mục tiêu của môn học:

- Kiến thức: Sinh viên nắm bắt được các kỹ thuật che giấu thông tin thông qua các phương pháp mã hóa và che giấu dữ liệu, ngoài ra các kỹ thuật khác trong lĩnh vực mật mã cũng được giới thiệu, từ đó sinh viên có thể hiểu và xây dựng các ứng dụng trong lĩnh vực bảo mật.
- Kỹ năng: Giúp sinh viên có các kỹ năng về đọc và hiểu các thuật toán trong lĩnh vực mật mã.
- Thái độ: Nghiêm túc, cẩn trọng trong nghiên cứu khoa học .....

3. Tóm tắt nội dung môn học:

Nội dung môn học chia làm 5 chương, lần lượt đi vào các vấn đề từ đơn giản đến phức tạp của lĩnh vực bảo mật thông tin. Chương 1, môn học giới thiệu lại các kiến thức toán học đã được học trước đó giúp sinh viên nhớ lại các kiến thức hỗ trợ cho môn học này. Chương 2, môn học giới thiệu về lại Mã hóa khóa đối xứng, một loại mã được sử dụng từ rất lâu và cũng rất phổ biện hiện nay. Các loại dữ liệu lớn và cần có tốc độ mã hóa và giải mã nhanh thì thường sử dụng loại mã hóa này. Chương 3, môn học giới thiệu về Mã hóa khóa công khai, một loại mã hiện đại và mới được phát triển và đầu những năm 1970. Chương 4, môn học giới thiệu về Chữ ký số, một trong những kỹ thuật quan trọng trong lĩnh vực bảo mật. Chương 5, môn học giới thiệu về các phương pháp phân phối khóa và thỏa thuận về khóa, nhằm mục đích phát tán khóa bí mật tới những người được phép trọng một mạng nhiều thành viên.

4. Học liệu:

Bắt buộc :

[1] Phan Đình Diệu, *An toàn và bảo mật thông tin*, Đại học Quốc gia HN, 2002

Tham khảo :

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

[2]. A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1997.

[3]. Bruce Schneier. *Applied Cryptography. Protocols, Algorithms and Source Code in C*, John Wiley&Son,Inc, 1996.

5. Nội dung và hình thức dạy – học:

Nội dung (Ghi cụ thể theo từng chương, mục, tiểu mục)	**Hình thức dạy – học**						**Tổng** (tiết)
	Lý thuyết	**Bài tập**	**Thảo luận**	**TH, TN, điền dó**	**Tự học, tự NC**	**Kiểm tra**	
CHƯƠNG 1: CƠ SỞ LÝ THUYẾT MẬT MÃ 1.1. Khái niêm 1.2. Cơ sở lý thuyết *1.2.1. Số nguyên* *1.2.2. Đồng dư. Các vấn đề liên quan*	5	1	1	3	10		20
CHƯƠNG 2: HỆ MẬT MÃ ĐỐI XỨNG 2.1. Hệ mật mã cổ điển *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	5	1		3	10	1	20
CHƯƠNG 3: HỆ 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.	5			3	10		18
CHƯƠNG 4: CHỮ KÝ SỐ (DIGITAL SIGNATURE) 4.1. Khái niệm. 4.2. Chữ ký số RSA, ElGamal, DSS 4.3. Chữ ký không phủ nhận được	5		1	3	10		19

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	3	1		3	10	1	18
Tổng (tiết)	**23**	**3**	**2**	**15**	**50**	**2**	**95**

6.Lịch trình tổ chức dạy – học cụ thể:

Tuần	Nội dung	Chi tiết về hình thức tổ chức dạy – học	Nội dung yêu cầu sv phải chuẩn bị trước	Ghi chú
1	**CHƯƠNG 1: CƠ SỞ LÝ THUYẾT MẬT MÃ** 1.1. Khái niêm 1.2. Cơ sở lý thuyết *1.2.1. Số nguyên*	- Sinh viên nghe giảng trên lớp. - Làm các bài tập được giao. - Thực hành cài đặt thuật toán.	- Sinh viên xem lại các kiến thức toán cao cấp. - Sinh viên xem lại kỹ thuật lập trình.	
2	1.2 Cơ sở lý thuyết (tiếp) *1.2.1. Số nguyên.* *1.2.2. Đồng dư, Các vấn đề liên quan*	- Sinh viên nghe giảng trên lớp. - Lấy ví dụ minh họa thuật toán. - Cài đặt thuật toán.	- Sinh viên đọc trước các kỹ thuật sẽ tìm hiểu. - Tìm các minh họa cụ thể cho từng kỹ thuật.	
3	*1.2.2. Đồng dư, Các vấn đề liên quan. (tiếp)* **CHƯƠNG 2: HỆ MẬT MÃ ĐỐI XỨNG** 2.1. Hệ mật mã cổ điển *2.1.1. Mã Dịch chuyển* *2.1.2. Mã Hoán vị* *2.1.3. Mã Thay thế*	- Sinh viên nghe giảng trên lớp. - Lấy ví dụ minh họa thuật toán. - Cài đặt thuật toán.	- Sinh viên đọc trước các kỹ thuật sẽ tìm hiểu. - Tìm các minh họa cụ thể cho từng kỹ thuật.	
4	*2.1.4. Mã Apphin* *2.1.5. Mã Vigenere* *2.1.6. Mã Hill*	- Sinh viên nghe giảng trên lớp. - Lấy ví dụ minh họa thuật toán. - Cài đặt thuật toán.	- Sinh viên đọc trước các kỹ thuật sẽ tìm hiểu. - Tìm các minh họa cụ thể cho từng kỹ thuật.	
5	2.2. Mã hóa DES	- Sinh viên nghe giảng trên lớp.	- Sinh viên đọc trước các kỹ thuật sẽ	

	CHƯƠNG 3: HỆ MÃ KHÓA CÔNG KHAI 3.1. Khái niệm	- Lấy ví dụ minh họa thuật toán. - Cài đặt thuật toán.	tìm hiểu. - Tìm các minh họa cụ thể cho từng kỹ thuật.	
6	3.2. Hệ mã khóa RSA 3.3. Hệ mã khóa ElGamal.	- Sinh viên nghe giảng trên lớp. - Lấy ví dụ minh họa thuật toán. - Cài đặt thuật toán.	- Sinh viên đọc trước các kỹ thuật sẽ tìm hiểu. - Tìm các minh họa cụ thể cho từng kỹ thuật.	
7	3.4. Hệ mã khóa DSS. **CHƯƠNG 4: CHỮ KÝ SỐ (DIGITAL SIGNATURE)** 4.1. Khái niệm. 4.2. Chữ ký số RSA, ElGamal, DSS	- Sinh viên nghe giảng trên lớp. - Lấy ví dụ minh họa thuật toán. - Cài đặt thuật toán.	- Sinh viên đọc trước các kỹ thuật sẽ tìm hiểu. - Tìm các minh họa cụ thể cho từng kỹ thuật.	
8	4.2. Chữ ký số RSA, ElGamal, DSS (tiếp)	- Sinh viên nghe giảng trên lớp. - Lấy ví dụ minh họa thuật toán. - Cài đặt thuật toán.	- Sinh viên đọc trước các kỹ thuật sẽ tìm hiểu. - Tìm các minh họa cụ thể cho từng kỹ thuật.	
9	4.3. Chữ ký không phủ nhận được **CHƯƠNG 5: PHÂN PHỐI KHÓA VÀ THOẢ THUẬN VỀ KHÓA** 5.1. Khái niệm.	- Sinh viên nghe giảng trên lớp. - Lấy ví dụ minh họa thuật toán. - Cài đặt thuật toán.	- Sinh viên đọc trước các kỹ thuật sẽ tìm hiểu. - Tìm các minh họa cụ thể cho từng kỹ thuật.	
10	5.2. Phân phối khóa. 5.3. Thỏa thuận về khóa	- Sinh viên nghe giảng trên lớp. - Lấy ví dụ minh họa thuật toán. - Cài đặt thuật toán.	- Sinh viên đọc trước các kỹ thuật sẽ tìm hiểu. - Tìm các minh họa cụ thể cho từng kỹ thuật.	
11	Thực hành tại phòng máy	Làm việc tại phòng	Sinh viên chuẩn bị	

		máy (Mỗi sinh viên 1 máy)	kiến thức về thuật toán trước khi cài đặt chạy trên máy	
12	Thực hành tại phòng máy	Làm việc tại phòng máy (Mỗi sinh viên 1 máy)	Sinh viên chuẩn bị kiến thức về thuật toán trước khi cài đặt chạy trên máy	
13	Thực hành tại phòng máy	Làm việc tại phòng máy (Mỗi sinh viên 1 máy)	Sinh viên chuẩn bị kiến thức về thuật toán trước khi cài đặt chạy trên máy	

7.Tiêu chí đánh giá nhiệm vụ giảng viên giao cho sinh viên:

Sau khi học xong môn học, sinh viên cần có cái nhìn tổng quan về môn học, năm bắt được các khái niệm mới mà, môn học cung cấp, đồng thời đọc và hiểu sâu sắc về các thuật toán đã được tìm hiểu trong môn học.

8.Hình thức kiểm tra, đánh giá môn học:

Thông qua các bài kiểm tra các modul chương trình được sinh viên lập trình trong quá trình học, để kiểm tra khả năng nắm bắt kiến thức và mức độ hiểu bài.

Thi hết môn: Tự luận.

9.Các loại điểm kiểm tra và trọng số của từng loại điểm:

- Kiểm quá trình (tư cách): 30%
- Thi hết môn: 70%

10.Yêu cầu của giảng viên đối với môn học:

- Yêu cầu về điều kiện để tổ chức giảng dạy môn học
  - Phòng học sạch sẽ, có máy chiếu.
  - Phòng thực hành có một số phần mềm lập trình. (C, C++, VB…)
- Yêu cầu đối với sinh viên
  - Sinh viên phải tuân thủ các quy định trên lớp của nhà trường.
  - Phải thực hiện đầy đủ các nhiệm vụ được giao trong môn học.

Hải Phòng, ngày 10 tháng 06 năm 2011

Chủ nhiệm Bộ môn **Người viết đề cương chi tiết**

Ths. Vũ Anh Hùng **Ths. Lê Th ụy**