BỘ GD&ĐT
Trường đại học SPKT
Khoa: Công nghệ Thông tin……

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

Chương trình Giáo dục đại học

Ngành đào tạo: Công nghệ Thông tin trình độ đào tạo: Đại học

Chương trình đào tạo: Kỹ sư Công nghệ Thông tin

Đề cương chi tiết học phần

1. Tên học phần: Bảo mật thông tin **Mã học phần:** INSE340379

2. Tên Tiếng Anh: Information Security

3. Số tín chỉ: 4

Phân bố thời gian: 4 (3:1:8)

4. Các giảng viên phụ trách học phần

1/ GV phụ trách chính: TS. Đặng Trường Sơn

2/ Danh sách giảng viên cùng GD: ThS. Lê Thị Minh Châu

5. Điều kiện tham gia học tập học phần

Môn học trước: Tin học đại cương, Kỹ thuật lập trình, Cấu trúc dữ liệu và giải thuật

Môn học tiên quyết: Không

6. Mô tả học phần (Course description)

Học phần này cung cấp các khái niệm cơ bản về bảo mật thông tin , giới thiệu 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 cung cấp khả năng vận dụng kiến thức về bảo mật thông tin đã học để giải quyết một số bài toán bảo mật trong thực tế. Bên cạnh đó, sinh viên được làm việc trong các nhóm và thuyết trình các vấn đề nâng cao sử dụng các phương tiện trình chiếu.

7. Mục tiêu học phần(Course objective)

Mục tiêu ***(Goals)***	**Mô tả** ***(Goal description)*** *(Học phần này trang bị cho sinh viên:)*	**Chuẩn đầu ra CTĐT**
G1	Vai trò của bảo mật thông tin, các cơ chế, chính sách an toàn thông tin, các kiểu tấn công và các phương pháp phòng chống	1.2, 1.3
G2	Nguyên lý hoạt động của mật mã dòng, mật mã khối; Kiến thức về xác thực, toàn vẹn thông tin và sử dụng các thuật toán mật mã để hiện thực những chức năng này	2.1, 2.2
G3	Kỹ năng làm việc nhóm, và thuyết trình trước lớp	3.1, 3.2
G4	Kiến thức và kỹ năng vận dụng kiến thức bảo mật thông tin và mật mã để giải quyết một số bài toán an toàn thông tin trong thực tế.	4.3, 4.4, 4.5

8. Chuẩn đầu ra của học phần

Mục tiêu	Chuẩn đầu ra học phần	Mô tả *(Sau khi học xong môn học này, người học có thể:)*	Chuẩn đầu ra CDIO
G1	G1.1	Trình bày được về vai trò của bảo mật thông tin, các cơ chế, chính sách bảo mật.	1.2
	G1.2	So sánh, phân tích các kiểu tấn công và các phương pháp phòng chống	1.3
G2	G2.1	Trình bày được nguyên lý hoạt động của mật mã dòng, khối.	2.1.1
	G2.2	Mô tả được cơ chế xác thực, toàn vẹn thông tin. Xây dựng được các chức năng này, sử dụng các thuật toán mật mã.	2.1.3, 2.1.4
G3	G3.1	Làm việc hiệu quả trong một nhóm	3.1.1, 3.1.2
	G3.2	Trình bày trước lớp, sử dụng phương tiện trình chiếu	3.2.6
G4	G4.1	Xây dựng được các mô hình an toàn thông tin dựa trên kiến thức bảo mật thông tin và mật mã	4.3.1, 4.3.3, 4.4.3
	G4.2	Đánh giá và lựa chọn các công cụ bảo mật thông tin trong việc giải quyết các bài toán thực tế	4.5.5

9. Tài liệu học tập

- Sách, giáo trình chính:

+ Đặng Trường Sơn, *Giáo trình Bảo mật thông tin,* NXB Đại học quốc gia TP.HCM, 2012
+ William Stallings**,** *Cryptography and Network Security: Principles and Practice*, fifth ed. Prentice Hall, 2010. www.Williamstallings.com

- Sách (TLTK) tham khảo:

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

9. Nhiệm vụ của sinh viên

SV không thực hiện đủ chỉ một trong các nhiệm vụ sau đây sẽ bị cấm thi:

- Dự lớp: 80%

- Bài tập: 100%

10. Tỷ lệ Phần trăm các thành phần điểm và các hình thức đánh giá sinh viên : (11)

- Thang điểm: 10

- Kế hoạch kiểm tra như sau:

Hình thức KT	Nội dung	Thời điểm	Công cụ KT	Chuẩn đầu ra KT	Tỉ lệ (%)
Bài tập					**30**
BT#1	Cài đặt thuật toán Caesar mở rộng, tấn công Caesar.	Tuần 3	Bài tập nhỏ trên lớp	G1.2	10
BT#2	Cài đặt S-box của thuật toán DES	Tuần 7	Bài tập nhỏ trên lớp	G2.1	10
BT#3	Cài đặt chương trình tính khoá mở rộng trong AES	Tuần 9	Bài tập nhỏ trên lớp	G2.1	10
Bài tập lớn (Project)					**10**
BL#1	Nhóm sinh viên từ 3-5 người chọn 1 trong các bài tập Cài đặt và minh họa thuật toán DES Minh họa từng bước mã hoá và giải mã RSA Minh họa từng bước tạo và kiểm tra chữ ký số RSA Minh họa nghi thức khoá thoả thuận Diffie-Helman	Tuần 7-9	Đánh giá sản phẩm	G2.1 G2.2 G3.1 G4.1 G4.2	
Tiểu luận - Báo cáo					**10**
	Mỗi nhóm sinh viên từ 3-5 người chọn 1 trong các đề tài sau để tìm hiểu và trình bày báo cáo: Đề tài 1: Classical Encryption Techniques Đề tài 2: Block Ciphers and the Data Encryption Standard Đề tài 3: Basic Concepts in Number Theory and Finite Fields Đề tài 4: Advanced Encryption Standard Đề tài 5: Block Cipher Operation Đề tài 6: Pseudorandom Number Generation and Stream Ciphers Đề tài 7: Number Theory Đề tài 8: Public-Key Cryptography & RSA Đề tài 9: Other Public-Key Cryptosystems Đề tài 10: Cryptographic Hash Functions Đề tài 11: Message Authentication Codes Đề tài 12: Digital Signatures Đề tài 13: Key Management and Distribution Đề tài 14: User Authentication Protocols Đề tài 15: Transport-Level Security Đề tài 16: Wireless Network Security	Tuần 10-15	Tiểu luận - Báo cáo	G1.1 G3.1 G3.2	

	Đề tài 17: Electronic Mail Security Đề tài 18: IP Security				
Thi cuối kỳ					**50**
	- Nội dung bao quát tất cả các chuẩn đầu ra quan trọng của môn học. - Thời gian làm bài 60 phút.		Thi tự luận	G1.1 G1.2 G2.1 G2.2 G4.1 G4.2	

11. Nội dung chi tiết học phần

Tuần	Nội dung	Chuẩn đầu ra học phần
1	***Chương 1: NHẬP MÔN***	
	A/* Các nội dung và PPGD chính trên lớp: (4)* **Nội dung GD lý thuyết:** + Giới thiệu môn học, hướng dẫn cách học, tài liệu tham khảo. + Các khái niệm về bảo mật thông tin + Các nguy cơ và các kiểu tấn công + Các mô hình, dịch vụ, cơ chế và công cụ bảo mật + Hệ thống mã hóa, khái niệm thám mã + Khái niệm thuật toán an toàn **PPGD chính**: + Thuyết trình. + Trình chiếu PowerPoint. + Tương tác hỏi đáp với sinh viên	G1.1 G1.2
	***B/* Các nội dung cần tự học ở nhà**: *(8)* + Đọc chương 1-2: William Stallings**,** *Cryptography and Network Security*...	G1.1 G1.2
2	***Chương 2: MẬT MÃ CỔ ĐIỂN***	
	A/* Tóm tắt các ND và PPGD chính trên lớp: (4)* **Nội dung GD lý thuyết:** + Lịch sử các thuật toán mật mã cổ điển + Các kỹ thuật mã hóa + Mật mã thay thế đơn từ + Mật mã thay thế đa từ + Kỹ thuật mã hóa hoán vị, kết hợp **PPGD chính**: + Thuyết trình. + Trình chiếu PowerPoint. + Tương tác hỏi đáp với sinh viên	G1.2

	***B/* Các nội dung cần tự học ở nhà**: *(8)* + Đọc chương 2: Đặng Trường Sơn**,** *Bảo mật thông tin…*	G1.2 G2.1
3	*Thực hành chương 1, 2:* *Cài đặt thuật toán Caesar mở rộng và tấn công Caesar*	
	A/* Các nội dung và PPGD chính trên lớp: (4)* **Nội dung GD:** + Hướng dẫn cài đặt thuật toán Caesar mở rộng và tấn công Caesar. **PPGD chính**: + Thuyết trình + Làm mẫu + Tương tác hỏi đáp với sinh viên	G1.2
	***B/* Các nội dung cần tự học ở nhà**: *(8)* + Cài đặt đặt thuật toán Caesar trên máy tính + Đọc chương 3: Đặng Trường Sơn**,** *Bảo mật thông tin…*	G1.2 G2.1
4	***Chương 3: MẬT MÃ DÒNG***	
	A/* Các nội dung và PPGD chính trên lớp: (4)* **Nội dung GD lý thuyết:** + Mã hóa theo dòng + Các phương pháp tạo dòng khóa + Tạo dòng khóa tuyến tính + Tạo dòng khóa không tuyến tính **PPGD chính**: + Thuyết trình. + Trình chiếu PowerPoint. + Tương tác hỏi đáp với sinh viên	G2.1
	***B/* Các nội dung cần tự học ở nhà**: *(8)* + Đọc chương 3: William Stallings**,** *Cryptography and Network Security…*	G2.1
5	***Chương 4: MẬT MÃ KHỐI***	
	A/* Các nội dung và PPGD chính trên lớp: (4)* **Nội dung GD lý thuyết:** + Mã hóa theo khối + Mạng thay thế và hoán vị Shanon + Cấu trúc thuật toán Feistel + Hiệu ứng thác và hiệu ứng toàn vẹn + Lịch sử của DES + Tạo các khóa con **PPGD chính**: + Thuyết trình. + Trình chiếu PowerPoint. + Tương tác hỏi đáp với sinh viên	G2.1
	***B/* Các nội dung cần tự học ở nhà**: *(8)* + Đọc chương 4: Đặng Trường Sơn**,** *Bảo mật thông tin…*	G2.1

6	***Chương 4: MẬT MÃ KHỐI (Tiếp theo)***	
	A/* Các nội dung và PPGD chính trên lớp: (4)* **Nội dung GD lý thuyết:** + Hàm mở rộng E, các S-box + Giải mã và chạy thử DES + Các yêu cầu thiết kế DES + Các phương thức sử dụng DES: ECB, CBC + Sử dụng DES để tạo luồng khóa: CFB, OFB **PPGD chính**: + Thuyết trình. + Trình chiếu PowerPoint. + Tương tác hỏi đáp với sinh viên	G2.1
	***B/* Các nội dung cần tự học ở nhà**: *(8)* + Đọc chương 5: Đặng Trường Sơn**,** *Bảo mật thông tin…*	G2.1
7	*Thực hành chương 4:* *Cài đặt S-box của thuật toán DES*	
	A/* Các nội dung và PPGD chính trên lớp: (4)* **Nội dung GD:** + Hướng dẫn cài đặt S-box của thuật toán DES. **PPGD chính**: + Thuyết trình + Làm mẫu + Tương tác hỏi đáp với sinh viên	
	***B/* Các nội dung cần tự học ở nhà**: *(8)* + Cài đặt S-box của thuật toán DES trên máy tính	G2.1
8	***Chương 5: CƠ SỞ LÝ THUYẾT SỐ***	
	A/* Các nội dung và PPGD chính trên lớp: (4)* **Nội dung GD lý thuyết:** + Số nguyên tố + Phép tính modulo + Thuật toán Bình phương và nhân + ƯSCLN và TT Euclid + TT Euclid mở rộng + Định lý Euler và Fermat **PPGD chính**: + Thuyết trình. + Trình chiếu PowerPoint. + Làm mẫu. + Tương tác hỏi đáp với sinh viên	G2.2
	***B/* Các nội dung cần tự học ở nhà**: *(8)* + Đọc chương 7: William Stallings**,** *Cryptography and Network Security…*	G2.2
9	***Chương 5: CƠ SỞ LÝ THUYẾT SỐ (tiếp theo)***	

	A/* Các nội dung và PPGD chính trên lớp: (4)* **Nội dung GD lý thuyết:** + Nhóm, vành, trường + Các đa thức trong trường Galoa + Các phép toán trên đa thức + Lý thuyết phức tạp và mã hóa **PPGD chính**: + Thuyết trình. + Trình chiếu PowerPoint. + Tương tác hỏi đáp với sinh viên	G2.2
	***B/* Các nội dung cần tự học ở nhà**: *(8)* + Đọc chương 6: Đặng Trường Sơn**,** *Bảo mật thông tin…*	G2.2
10	***Chương 6: CHUẨN MẬT MÃ CAO CẤP AES***	
	A/* Các nội dung và PPGD chính trên lớp: (4)* **Nội dung GD lý thuyết:** + Giới thiệu chuẩn mã hóa cao cấp + Rijndael – AES + Các tham số của AES + Các vòng mã hóa ✓ SubBytes ✓ ShiftRows ✓ MixColumns ✓ AddRoundkey + Tạo khóa mở rộng (Key Expansion) + Chạy thử AES **PPGD chính**: + Thuyết trình. + Trình chiếu PowerPoint. + Tương tác hỏi đáp với sinh viên	G2.1
	***B/* Các nội dung cần tự học ở nhà**: *(8)* + Đọc chương 7: Đặng Trường Sơn**,** *Bảo mật thông tin…*	G2.2
11	*Thực hành chương 6:* *Cài đặt chương trình tính khoá mở rộng trong AES*	
	A/* Các nội dung và PPGD chính trên lớp: (4)* **Nội dung GD:** + Hướng dẫn cài đặt chương trình tính khoá mở rộng trong AES. **PPGD chính**: + Thuyết trình + Làm mẫu + Tương tác hỏi đáp với sinh viên	G2.1
	***B/* Các nội dung cần tự học ở nhà**: *(8)* + Cài đặt chương trình tính khoá mở rộng trong AES trên máy tính	
12	***Chương 7: MẬT MÃ KHOÁ CÔNG KHAI***	

	A/* Các nội dung và PPGD chính trên lớp: (4)* **Nội dung GD lý thuyết:** + Khái niệm mật mã khóa công khai + Thuật toán mật mã khóa công khai RSA + Thuật toán mật mã El-Gamal **PPGD chính**: + Thuyết trình. + Trình chiếu PowerPoint. + Tương tác hỏi đáp với sinh viên	G2.2
	***B/* Các nội dung cần tự học ở nhà**: *(8)* + Đọc chương 8: Đặng Trường Sơn**,** *Bảo mật thông tin…*	G2.2
13	***Chương 8: XÁC THỰC VÀ CHỮ KÍ SỐ***	
	A/* Các nội dung và PPGD chính trên lớp: (4)* **Nội dung GD lý thuyết:** + Khái niệm xác thực + Xác thực sử dụng mật mã + Các hàm băm: MD5, SHA1-3 + Chữ ký số RSA và El Gamal + DSA (Digital Signature Algorithm) **PPGD chính**: + Thuyết trình. + Trình chiếu PowerPoint. + Tương tác hỏi đáp với sinh viên	G2.2
	***B/* Các nội dung cần tự học ở nhà**: *(8)* + Đọc chương 9: Đặng Trường Sơn**,** *Bảo mật thông tin…*	G2.2
14	***Chương 9: PHÂN PHỐI KHOÁ***	
	A/* Các nội dung và PPGD chính trên lớp: (4)* **Nội dung GD lý thuyết:** + Quản lý và phân phối khóa + Phân phối khóa công khai + Phân phối khóa bí mật + Quy trình tạo khóa phiên Diffie – Hellman + CA (Certification Authority) **PPGD chính**: + Thuyết trình. + Trình chiếu PowerPoint. + Tương tác hỏi đáp với sinh viên	G2.1 G2.2
	***B/* Các nội dung cần tự học ở nhà**: *(8)* + Đọc chương 13: William Stallings**,** *Cryptography and Network Security…*	
15	***ÔN TẬP***	

	A/* Các nội dung và PPGD chính trên lớp: (3)* **Nội dung GD lý thuyết:** + Báo cáo nốt tiểu luận trên lớp + Ôn tập nội dung đã học. **PPGD chính**: + Thuyết giảng + Trình chiếu	G3.1 G3.2
	***B/* Các nội dung cần tự học ở nhà**: *(6)* + Ôn tập các nội dung đã học	

14. Đạo đức khoa học:

15. Ngày phê duyệt: ngày/tháng/năm

16. Cấp phê duyệt:

Trưởng khoa **Tổ trưởng BM** **Người biên soạn**

17. Tiến trình cập nhật ĐCCT

Lần 1: Nội Dung Cập nhật ĐCCT lần 1: ngày/tháng/năm	<người cập nhật ký và ghi rõ họ tên) Tổ trưởng Bộ môn:
Lần 2: Nội Dung Cập nhật ĐCCT lần 2: ngày/tháng/năm	<người cập nhật ký và ghi rõ họ tên) Tổ trưởng Bộ môn:
