BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC MỞ TP. HỒ CHÍ MINH

ĐỀ CƯƠNG MÔN HỌC

1. THÔNG TIN VỀ MÔN HỌC

1.1 Tên môn học: AN TOÀN VÀ BẢO MẬT THÔNG TIN
Mã MH: ITEC4406
1.2 Khoa/Ban phụ trách: Công Nghệ Thông Tin
1.3 Số tín chỉ: 03(02LT, 01TH)

2. MÔ TẢ MÔN HỌC

Cung cấp những kiến thức cơ bản về an toàn và bảo mật thông tin trên hệ thống máy tính bao gồm kiến thức về mật mã và an toàn trên mạng Internet.

3. MỤC TIÊU MÔN HỌC

3.1. Mục tiêu chung

Hướng sinh viên vào một lĩnh vực khoa học mới – An toàn Thông tin và có đủ kiến thức xây dựng một hệ thống thông tin an toàn một các hiệu quả.

3.2. Mục tiêu cụ thể:

- Điều kiện tiên quyết: Mạng máy tính (hoàn chỉnh), toán logic, lập trình C/C++.
- Các yêu cầu khác: Hệ ĐH Linux và lập trình trên Linux.

4. NỘI DUNG MÔN HỌC

STT	Tên chương	Mục, tiểu mục	Số tiết				Tài liệu tự học
			TC	LT	BT	TH	
1.	Chương 1: Tầm quan trọng của BMTT trên HTTT (2 tiết)	1.1. Tại sao ? 1.2. An tòan thông tin là gì? 1.3. Tính chất của hệ thống thông tin. 1.4. Các mức ATTT. 1.5. Một số khái niệm cơ bản về ATTT.	2	2			[1]
2.	Chương 2: Các hệ mật mã (8 tiết)	2.1 Vai trò của mật mã trong BMTT. 2.1.1 Mật mã là gì. 2.1.2 Mật mã – một phần quan trọng trong ATTT. 2.1.3 Vai trò của mật mã.	13	8	0	5	[1]

STT	Tên chương	Mục, tiểu mục	Số tiết				Tài liệu tự học
			TC	LT	BT	TH	
		2.1.4 Mô hình sử dụng mật mã trên Internet. 2.2 Mật mã đối xứng. 2.2.1. Định nghĩa mật mã đối xứng.Một số hệ mật đối xứng cổ điển. 2.2.2: Mô tả hoạt động Hệ mật DES. 2.2.3 Các hệ mật đối xứng hiện đại. 2.3 Hệ mật bất đối xứng. 2.3.1. RSA (Revest – Sammer –Anderman). 2.3.2. Thuật giải Diffie-Hellman. 2.4 Hàm băm một chiều (One Way Hash function). 2.4.1. Khái niệm. 2.4.2. SHA-1 (Secure Hash Algorithm). 2.4.3. Một số hàm băm khác. 2.5 Chữ ký số (Digital signature). 2.5.1.Khái niệm về chữ ký số. 2.5.2. Thuật giải RSA trong vai trò chữ ký số. 2.5.4. Thuật giải DSA – Chuẩn chữ ký số. 2.5.5. Chuyển giao dữ liệu nhờ RSA.					
3.	Chương 3 Hạ tầng kiến trúc khóa công khai (PKI)	3.1 Khái niệm. 3.2 CA – Certificate Authorities. 3.3 RAs and LRAs. 3.3.1.Registration authority (RA). 3.3.2.Local registration	10	5		5	[1]

STT	Tên chương	Mục, tiểu mục	Số tiết				Tài liệu tự học
			TC	LT	BT	TH	
		authority (LRA). 3.4 Certificates (Chứng chỉ). 3.4.1 Nội dung của chứng chỉ - chuẩn x-509. 3.4.2 Certificate Policies. 3.4.3 Certificate Practice Statements. 3.4.4 Thu hồi / huỷ chứng chỉ (Certificate Revocation). 3.5 Mô hình uỷ quyền (Trust Models). 3.5.1 Hierarchical. 3.5.2 Bridge. 3.5.3 Mesh. 3.5.4 Hybrit.					
4.	Chương 4: Bảo mật thông tin trên internet	4.1 Hạ tầng mạng và những điểm yếu. 4.1.1 Chuẩn OSI và TCP/IP. 4.1.2 Mô hình OSI và truyền thông giữa hai máy. 4.1.3 TCP/IP model. 4.1.4 Mô hình OSI và TCP/IP. 4.1.5 Đóng gói trong TCP/IP. 4.2 Protocols and Services. 4.2.1 Ports. 4.2.2 TCP Three - Way – Handshake. 4.2.3.Application Programming Interfaces (API). 4.3 Các điểm yếu dễ bị khai thác trên mạng. 4.3.1.TCP/IP Attacks.	15	5	5	5	[1]

STT	Tên chương	Mục, tiểu mục	Số tiết				Tài liệu tự học
			TC	LT	BT	TH	
		4.3.2.Malicious Code. 4.3.3.Một số dấu hiệu nhiễm virut. 4.3.4.Hoạt động củaVirut. 4.3.5 Các loại virut. 4.3.6.Social Engineering. 4.4 Các giao thức bảo mật trên mạng Internet. 4.4.1 Bảo mật giao thức PPP (Layer 2). 4.4.2.Tunneling Protocols. 4.4.3 IPsec (Layer 3). 4.4.4 Secure Shell (SSH) (Layer 4). 4.4.5 HTTP/S – on top of SSH (Layer 4,5). 4.4.6 Bảo mật E-Mail (Layer 5). 4.5 Bảo mật Wireless network. 4.5.1 Wireless Applications Protocol (WAP). 4.5.2 Wireless Transport Layer Security (WTLS). 4.5.3 WEP/WAP. 4.5.4 Các điểm yếu trên Wireless.					
5.	Chương 5: Chính sách an toàn và bảo mật thông tin trong doanh nghiệp	5.1 Quản lý các chính sách 5.1.1 Mục đích. 5.1.2 Một số chính sách quan trọng. 5.2. Quản lý rủi ro trong HTTT. 5.3. Quản lý chất lượng ATTT và ISO 17799/27001.	5	5	0	5	[1]

Ghi chú: TC: Tổng số tiết; LT: Lý thuyết; BT: Bài tập; TH: Thực hành.

5. TÀI LIỆU THAM KHẢO

5.1. Tài liệu chính:

[1]. Chuck Easttom, *Modern Cryptography: Applied Mathematics for Encryption and Information Security*, 2016.

5.2. Tài liệu tham khảo:

[2]. Mark Stamp, Information Security: Principles and Practice,Wiley, 2011.

[3]. Mark S. Merkow, Jim Breithaupt, Information Security: Principles and Practices – 2nd Edition – Certification/Training, Pearson, 2014.

6. ĐÁNHGIÁ KẾTQUẢHỌCTẬP

STT	Điểm thành phần	Tỉ lệ %
1	Kiểm tra giữa kỳ	40%
2	Thi cuối kỳ cuối kỳ	60%
	Điểm tổng kết môn học *(Điểm kiểm tra giữa kỳ * 30% + Điểm thi cuối kỳ * 70%)*	**100%**

7. KẾ HOẠCH GIẢNG DẠY

7.1. Kế hoạch giảng dạy lớp ngày

STT	Buổi học	Nội dung	Ghi chú
1.	Buổi 1	Chương 1: Tầm quan trọng của BMTT trên HTTT Chương 2: Các hệ mật mã	
2.	Buổi 2	Chương 2:Các hệ mật mã	
3.	Buổi 3	Chương 3 :Hạ tầng kiến trúc khóa công khai (PKI)	
4.	Buổi 4	Chương 3 :Hạ tầng kiến trúc khóa công khai (PKI)	
5.	Buổi 5	Chương 4: Bảo mật thông tin trên internet	
6.	Buổi 6	Chương 5: Chính sách an toàn và bảo mật thông tin trong doanh nghiệp	
7.	Buổi 7	Chương 5: Chính sách an toàn và bảo mật thông tin trong doanh nghiệp	

7.2. Kế hoạch giảng dạy lớp tối

STT	Buổi học	Nội dung	Ghi chú
1.	Buổi 1	Chương 1(2,0 tiết) – Tầm quan trọng của BMTT trên HTTT Chương 2(1,0 tiết) – Các hệ mật mã	
2.	Buổi 2	Chương 2 (3,0 tiết) – Các hệ mật mã	
3.	Buổi 3	Chương 2 (3,0 tiết) – Các hệ mật mã	
4.	Buổi 4	Chương 2 (1,0 tiết) – Các hệ mật mã Chương 3(2,0 tiết) – Hạ tầng kiến trúc khóa công khai (PKI)	
5.	Buổi 5	Chương 3(3,0 tiết) – Hạ tầng kiến trúc khóa công khai (PKI)	
6.	Buổi 6	Chương 4 (3,0 tiết) – Bảo mật thông tin trên internet	
7.	Buổi 7	Chương 4(2,0 tiết) – Bảo mật thông tin trên internet Chương 4(1,0 tiết) – Bài tập	
8.	Buổi 8	Chương 4(3,0 tiết) – Bài tập	
9.	Buổi 9	Chương 4(1,0 tiết) – Bài tập Chương 5(2,0 tiết) – Chính sách an toàn và bảo mật thông tin trong doanh nghiệp	
10.	Buổi 10	Chương 5(3,0 tiết) – Chính sách an toàn và bảo mật thông tin trong doanh nghiệp	

KT. KHOA TRƯỞNG
PHÓ TRƯỞNG KHOA
(Ký và ghi rõ họ tên)

TS. Lê Xuân Trường