HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA CÔNG NGHỆ THÔNG TIN 1
*****

ĐỀ CƯƠNG MÔN HỌC
(Phương pháp đào tạo theo tín chỉ)

TÊN HỌC PHẦN: MẬT MÃ HỌC CƠ SỞ

Mã học phần: INT1344
(3 tín chỉ)

Biên soạn
ĐỖ XUÂN CHỢ

Hà Nội - 2016

ĐỀ CƯƠNG HỌC PHẦN: MẬT MÃ HỌC CƠ SỞ

Khoa: Công nghệ thông tin 1 **Bộ môn**: An toàn thông tin

1.Thông tin về giảng viên

(Những Giảng viên có thể tham gia giảng dạy được môn học,hoặc Bộ môn có kế hoạch để Giảng viên chuẩn bị giảng dạy được môn học)

1.1. Giảng viên 1:

Họ và tên: Đỗ Xuân Chợ
Chức danh, học hàm, học vị: Tiến sỹ, Giảng viên.
Địa điểm làm việc: Bộ môn An toàn thông tin, Khoa CNTT1,
Học viện Công nghệ Bưu chính Viễn thông.
Địa chỉ liên hệ: Bộ môn An Toàn Thông Tin, Khoa CNTT1, Cơ sở đào tạo Hà Đông
Học viện Công nghệ Bưu chính Viễn thông.
Điện thoại: 0965.068.868 Email: doxuancholeti@gmail.com
Các hướng nghiên cứu chính:An toàn thông tin, xử lý thông tin, hệ thống tự động hóa thiết kế, mô hình hóa.
Thông tin về trợ giảng (nếu có): ……

1.2. Giảng viên 2:

Họ và tên: Hoàng Xuân Dậu
Chức danh, học hàm, học vị: Tiến sỹ, Giảng viên.
Địa điểm làm việc: Bộ môn An toàn thông tin, Khoa CNTT1,
Học viện Công nghệ Bưu chính Viễn thông.
Địa chỉ liên hệ: Bộ môn An toàn thông tin, Khoa CNTT1, Cơ sở đào tạo Hà Đông
Học viện Công nghệ Bưu chính Viễn thông.
Điện thoại: 0904 534 390 Email: dauhx@ptit.edu.vn
Các hướng nghiên cứu chính: An toàn thông tin, hệ thống & mạng, học máy, khai phá dữ liệu và các hệ thống nhúng.

2. Thông tin chung về môn học

- Tên môn học: Mật mã học cơ sở
- Tên tiếng Anh môn học: Fundamentals of Cryptography
- Mã môn học: INT1344
- Số tín chỉ (TC): 3
- Loại môn học: *Bắt buộc*
- **Cácmôn học tiên quyết**: không.
- **Môn học trước:** Tin học cơ sở 2; Ngôn ngữ lập trình C++
- **Môn học song hành:**
- Các yêu cầu đối với môn học (nếu có):
  + Phòng học lý thuyết: Có máy chiếu
  + Phòng thực hành: Có máy tính
- Giờ tín chỉ đối với các hoạt động:
  + Nghe giảng lý thuyết: 30 tiết
  + Bài tập lớn/ tiểu luận: 8 tiết
  + Thảo luận: 0 tiết
  + Thực hành: 6 tiết
  + Tự học: 1 tiết

Địa chỉ Khoa/Bộ môn phụ trách môn học:

- ***Địa chỉ:*** Bộ môn An Toàn Thông Tin, Khoa Công Nghệ Thông Tin, tầng 9, nhà A2, Cơ sở Đào tạo Hà Đông, Học viện Công nghệ BC-VT, Km 10 đường Nguyễn Trãi, Hà Nội.
- ***Điện thoại:*** 043.854.5604

3. Mục tiêu môn học

- ***Về kiến thức***: Trang bị cho sinh viên các kiến thức cơ bản về mật mã học bao gồm: các khái niệm toán học trong mật mã; các giải thuật mã hóa thông dụng; các hàm băm, các vấn đề quản lý khóa; một số ứng dụng của mật mã trong thực tế.

- ***Kỹ năng*:** Sau khi học xong, sinh viên nắm vững các kiến thức về các giải thuật mã hóa. Có kỹ năng lựa chọn và áp dụng các giải thuật mã hóa vào việc đảm bảo an toàn thông tin trong thực tế.

- ***Thái độ, Chuyên cần:*** Đảm bảo số giờ học trên lớp và tự học.

Mục tiêu chi tiết cho từng nội dung của môn học

Mục tiêu / Nội dung	Bậc 1	Bậc 2	Bậc 3
Chương 1: Tổng quan về mật mã học.	- Hiểu được các khái niệm, thuật ngữ, lịch sử phát triển, tiêu chí phân loại và các kiến thức liên quan về mật mã. - Biết được một số ứng dụng của mật mã học đang được áp dụng trong thực tế. - Hiểu được các khái niệm toán học cơ bản trong mật mã.		
Chương 2: Mã hóa khóa đối xứng	- Hiểu được các khái niệm cơ bản, nguyên tắc mã hóa thông tin, ưu điểm và nhược điểm của các giải thuật mã hóa khóa đối xứng.	- Biết cách cài đặt các giải thuật mã hóa khóa đối xứng bằng các ngôn ngữ lập trình.	- Có khả năng đánh giá, phân tích và lựa chọn giải thuật mã hóa khóa đối xứng phù hợp cho ứng dụng cụ thể.
Chương 3: Mã hóa khóa bất đối xứng	- Hiểu được các khái niệm cơ bản, nguyên tắc mã hóa thông tin, ưu điểm và nhược điểm của các giải thuật mã hóa khóa bất đối xứng. - Biết được các ứng dụng của mã hóa khóa bất đối xứng trong thực tế.	- Biết cách cài đặt các giải thuật mã hóa khóa bất đối xứng bằng các ngôn ngữ lập trình.	- Có khả năng đánh giá, phân tích và lựa chọn giải thuật mã hóa bất đối xứng phù hợp cho ứng dụng cụ thể.
Chương 4: Các hàm băm	- Hiểu được các khái niệm, các tính chất và các đặc trưng cơ bản của hàm băm. - Hiểu được nguyên tắc làm việc của một số hàm băm thông dụng.	- Biết cách cài đặt các hàm băm bằng ngôn ngữ lập trình.	- Có khả năng nhận biết được các lỗ hổng bảo mật trong một số ứng dụng khi áp dụng hàm băm.
Chương 5: Quản lý khoá	- Hiểu được nguyên tắc phân phối và quản lý khóa sử dụng mã hoá khóa bí mật và công khai; - Biết được được một số giao thức và quản lý khóa hiện nay.	- Phân tích được các khó khăn trong việc phân phối và quản lý khóa.	- Có khả năng đánh giá được các lỗ hổng tồn tại trong các giao thực vận chuyển khóa.

4. Tóm tắt nội dung môn học

Môn học cung cấp cho sinh viên các kiến thức cơ bản về mật mã học bao gồm: vai trò, tầm quan trọng của mật mã; một số vấn đề cơ bản về toán học ứng dụng trong mật mã; các giải thuật mã hóa đối xứng và bất đối xứng thông dụng; các hàm băm phổ biến; vấn đề quản lý, thỏa thuận và phân phối khóa trong mật mã; một số ứng dụng thực tiễn của các giải thuật mã hóa.

5. Nội dung chi tiết môn học

CHƯƠNG 1: TỔNG QUAN VỀ MẬT MÃ HỌC

1.1. Các thuật ngữ và các khái niệm cơ bản

1.2. Lịch sử phát triển

1.3. Phân loại

1.4. Vai trò

1.5. Một số ứng dụng

1.6. Một số khái niệm toán học trong mật mã

CHƯƠNG 2. MÃ HÓA KHÓA ĐỐI XỨNG

2.1. Giới thiệu về mã hóa khóa đối xứng

2.2. Các kỹ thuật mã hóa đối xứng cổ điển

2.2.1. Phương pháp thay thế

2.2.2. Phương pháp mã hóa hoán vị

2.2.3. Phương pháp mã hóa XOR

2.2.4. Phương pháp sách hoặc khóa chạy

2.3. Các kỹ thuật mã hóa đối xứng hiện đại

2.3.1. Giải thuật mã hóa DES/3DES

2.3.2. Giải thuật mã hóa AES

2.3.3. Giải thuật mã hóa A51 và RC4

2.4. Ưu điểm và nhược điểm của mã hóa đối xứng

CHƯƠNG 3. MÃ HÓA KHÓA BẤT ĐỐI XỨNG

3.1. Giới thiệu về mã hóa bất đối xứng

3.2. Giải thuật mã hóa RSA

3.3. Ưu điểm và nhược điểm của mã hóa bất đối xứng

3.4. Ứng dụng của mã hóa khóa bất đối xứng

CHƯƠNG 4. CÁC HÀM BĂM

4.1. Giới thiệu về hàm băm

4.1.1. Định nghĩa

4.1.2. Các tính chất cơ bản

4.1.3. Phân loại

4.1.4. Vai trò

4.2. Các hàm băm không khóa

4.3. Các hàm băm có khóa

4.4. Một số hàm băm thông dụng

4.4.1. Hàm băm họ MD

4.4.2. Hàm băm họ SHA

Chương 5. Quản lý khóa

5.1. Giới thiệu

5.2. Phân phối khóa bí mật

5.3. Phân phối khóa công khai

5.4. Phân phối khóa kết hợp

5.5. Thỏa thuận khóa

6. Học liệu

6.1. Học liệu bắt buộc

[1] Nguyễn Bình, Ngô Đức Thiện. *Cơ sở mật mã học*. Học Viện Công Nghệ Bưu Chính Viễn Thông, 2013. 237 trang.

6.2. Học liệu tham khảo

[2] Behrouz A. Forouzan. *Introduction to cryptography and network security*. Moscow, 2010, 784p.

[3] Nguyễn Khanh Văn. *Cơ sở an toàn thông tin*. Đại học Bách khoa Hà Nội, 2014. 230 trang.

[4] William Stallings, *Cryptography and Network Security*, Prentice Hall, 2010.

[5] Jonathan Katz and Yehuda Lindell, *Introduction to Modern Cryptography*, Chapman & Hall/ CRC, 2007.

[6] Bruce Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, Wiley, 1996.

7. Hình thức tổ chức dạy học

7.1 Lịch trình chung:

Nội dung	Hình thức tổ chức dạy môn học					Tổng cộng
	Lên lớp			Thực hành	Tự học	
	Lý thuyết	Bài tập lớn/ tiểu luận	Thảo luận			
Nội dung 1: Giới thiệu về mật mã, các khái niệm cơ bản, phân loại và lịch sử phát triển. Vai trò của mật mã học.	2					2
Nội dung 2: Các ứng dụng cơ bản của mật mã trong thực tế	2					2
Nội dung 3: Một số khái niệm toán học trong mật mã	2					2
Nội dung 4: Giới thiệu về mã hóa khóa đối xứng. Các phương pháp mã hóa cổ điển	2					2
Nội dung 5: Mã hóa DES/3DES	2					2
Nội dung 6: Mã hóa AES	2					2
Nội dung 7: A51 và RC4. Ưu điểm và nhược điểm của mã hóa đối xứng	2	2				4
Nội dung 8: Giới thiệu về mã hóa khóa bất đối xứng. Giải thuật RSA	2			2		4
Nội dung 9: Đánh giá giải thuật. Ứng dụng mã hóa bất đối xứng.	2					2
Nội dung 10: Giới thiệu về hàm	2			2		4

băm, các tính chất cơ bản của hàm băm, hàm băm không khóa, có khóa						
Nội dung 11: Hàm băm họ MD	2	2				4
Nội dung 12: Hàm băm họ SHA	2	2				4
Nội dung 13: Giới thiệu. Phân phối khóa bí mật	2	2				4
Nội dung 14: Phân phối khóa bí mật. Phân phối khóa công khai.	2			2		4
Nội dung 15: Phân phối khóa kết hợp. Thỏa thuận khóa	2				1	3
Tổng cộng	**30**	**8**	**0**	**6**	**1**	**45**

(Ghi chú: *Mỗi nội dung (Trừ Thí nghiệm, Thực hành) được bố trí để thực hiện trong thời gian là 2 tiết tín chỉ (2h tín chỉ), khi cần tính liên tục thì bố trí ở nội dung tiếp theo)*

7.2. Lịch trình tổ chức dạy học cụ thể

(được thiết kế cho từng nội dung ứng với 1 tuần học, cho đến hết môn học là 15 tuần).

Tuần 1: Nội dung 1

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Giới thiệu về mật mã, các khái niệm cơ bản, phân loại và lịch sử phát triển. - Vai trò của mật mã học.	Đọc chương 1 quyển 1, 2, 3	

Tuần 2: Nội dung 2

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Các ứng dụng cơ bản của mật mã trong thực tế.	Đọc chương 1 quyển 1, 2, 3.	

Tuần 3: Nội dung 3

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Lý thuyết thông tin. - Lý thuyết số. - Độ phức tạp tính toán.	Đọc chương 1 quyển 1, 2; Phần 1 chương 2 quyển 3.	

Tuần 4: Nội dung 4

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Giới thiệu về mã hóa khóa đối xứng. - Các phương pháp mã hóa cổ điển	Đọc chương 2 quyển 1, 2; Phần 1 chương 3 quyển 3.	

Tuần 5: Nội dung 5

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Mã hóa DES/3DES	Đọc chương 2	

			quyển 1, 2; Phần 1 chương 3 quyển 3.	

Tuần 6: Nội dung 6

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Mã hóa AES.	Đọc chương 2 quyển 1, 2; Phần 1 chương 6 quyển 3.	

Tuần 7: Nội dung 7

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- A51 và RC4. - Ưu điểm và nhược điểm của mã hóa đối xứng	Đọc chương 2 quyển 1, 2; Phần 1 chương 7 quyển 3.	
Bài tập lớn/tiểu luận	2	- Tìm hiểu và cài đặt thuật toán mã hóa dòng và ứng dụng.	Chuẩn bị tài liệu và thuyết trình về bài tập lớn	

Tuần 8: Nội dung 8

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Giới thiệu về mã hóa khóa bất đối xứng. - Giải thuật RSA.	Đọc chương 3 quyển 1, 2; Phần 2 chương 9 quyển 3.	
Thực hành	2	- Cài đặt giải thuật mã hóa DES	Đọc tài liệu hướng dẫn thực hành.	

Tuần 9: Nội dung 9

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Đánh giá giải thuật. - Ứng dụng mã hóa bất đối xứng.	Đọc chương 3 quyển 1, 2; Phần 2 chương 9 quyển 3.	

Tuần 10: Nội dung10

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Giới thiệu về hàm băm. - Các tính chất cơ bản của hàm băm. - Hàm băm không khóa, có khóa	Đọc chương 4 quyển 1, 2; Phần 2 chương 12 quyển 3..	
Thực hành	2	- Cài đặt giải thuật mã hóa AES	Đọc tài liệu hướng dẫn thực hành.	

Tuần 11: Nội dung 11

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Hàm băm họ MD	Đọc chương 4 quyển 1, 2; Phần 2 chương 12 quyển	

			3.	
Bài tập lớn/ tiểu luận	2	- Tìm hiểu các giải thuật mã hóa dựa trên đường cong Elliptic.	Chuẩn bị tài liệu và thuyết trình về bài tập lớn.	

Tuần 12: Nội dung 12

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Hàm băm họ SHA	Đọc chương 4 quyển 1, 2; Phần 2 chương 12 quyển 3.	
Bài tập lớn/tiểu luận	2	- Tìm hiểu các hình thức thám mã.	Chuẩn bị tài liệu và thuyết trình về bài tập lớn	

Tuần 13: Nội dung 13

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Giới thiệu. - Phân phối khóa bí mật.	Đọc tài liệu tham khảo quyển 2 chương 15, quyển 1 chương 5, 6, quyển 3 chương 5, quyển 4 chương 10.	
Bài tập lớn/tiểu luận	2	- Nghiên cứu ứng dụng của hàm băm trong bỏ phiếu điện tử.	Chuẩn bị tài liệu và viết báo cáo để thuyết trình về bài tập lớn	

Tuần 14: Nội dung 14

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Phân phối khóa bí mật. - Phân phối khóa công khai.	Đọc tài liệu tham khảo quyển 2 chương 15, quyển 1 chương 5, 6, quyển 3 chương 5, quyển 4 chương 10.	
Thực hành	2	- Cài đặt các hàm băm SHA-1 và MD5.	Đọc tài liệu hướng dẫn thực hành.	

Tuần 15: Nội dung 15

Hình thức tổ chức dạy học	Thời gian *(tiết TC)*	Nội dung chính	Yêu cầu đối với sinh viên	Ghi chú
Lý thuyết	2	- Phân phối khóa bí mật sử dụng hệ mật công khai. - Thỏa thuận khóa.	Đọc tài liệu tham khảo quyển 2 chương 15, quyển 1 chương 5, 6, quyển 3 chương 5, quyển 4 chương 10.	
Tự học	1			

8. Chính sách đối với môn học và các yêu cầu khác của giảng viên

- Các bài tập phải làm đúng hạn. Nếu không đúng hạn sẽ bị điểm 0.
- Thiếu một điểm thành phần (bài tập, bài kiểm tra giữa kỳ), hoặc nghỉ quá 20% tổng số giờ của môn học, không được thi hết môn.

9. Phương pháp, hình thức kiểm tra – đánh giá kết quả học tập môn học

9.1. Kiểm tra đánh giá định kỳ

Hình thức kiểm tra *(Tham khảo ví dụ dưới đây)*	**Tỷ lệ đánh giá**	**Đặc điểm đánh giá**
- Tham gia học tập trên lớp (đi học đầy đủ, tích cực thảo luận)	10 %	Cá nhân
- Các bài tập lớn/ tiểu luận và thảo luận nhóm trên lớp	20%	Cá nhân
- Hoạt động theo nhóm		
- Kiểm tra giữa kỳ	10%	Cá nhân
- Kiểm tra cuối kỳ	60%	Cá nhân

9.2. Nội dung và Tiêu chí đánh giá các loại bài tập

Các loại bài tập lớn/thảo luận	**Yêu cầu và Tiêu chí đánh giá**
- Bài tập lớn/Tiểu luận	- Yêu cầu sinh viên nắm vững và trình bày được kiến thức căn bản của môn học - Tìm tài liệu, tổng hợp kiến thức và viết báo cáo theo yêu cầu của bài tập lớn được giao cho nhóm - Phân chia công việc và cộng tác theo nhóm - Chuẩn bị slides và trình bày trước lớp
- Thảo luận	- Tìm hiểu các vấn đề theo yêu cầu của nội dung thảo luận được giao và trả lời câu hỏi trực tiếp
- Kiểm tra giữa kỳ, cuối kỳ	- Nắm vững kiến thức môn học - Trả lời đúng các câu hỏi và bài tập

Duyệt	**Chủ nhiệm bộ môn**	**Giảng viên** *(Chủ trì biên soạn đề cương)*
PGS.TS Từ Minh Phương	**TS. Hoàng Xuân Dậu**	**TS. Đỗ Xuân Chợ**