Trường Đại học Bách Khoa - ĐHQG Tp.HCM
Khoa: Khoa Khoa học và Kỹ thuật Máy tính
Khoa/Bộ môn quản lý MH: Công nghệ Phần mềm

Tp.HCM, ngày ..... tháng ..... năm .....

Đề cương môn học Sau đại học

MẬT MÃ HỌC ỨNG DỤNG (APPLIED CRYPTOGRAPHY)

Mã số MH: CO5221

Số tín chỉ:	**Tc (LT.BT&TH.Tự Học): 3**						**ECTS: 6**			
Số tiết -Tổng:	**75**	LT:	**30**	BT:	**0**	TH:	**0**	ĐA:	BTL/TL:	**45**
Đánh giá:	Bài tập: 20% Thuyết Trình: 30% Thi cuối kì: 50%									
- Môn tiên quyết:										
- Môn học trước:										
- Môn song hành:										
- CTĐT ngành (Mã ngành):	Khoa Học Máy Tính (8480101)									
- Ghi chú khác:										

1. <u>Mục tiêu môn học:</u>

Các mục tiêu chính của môn học này là để cung cấp cho các nguyên tắc cơ bản của mật mã học hiện đại; trình bày cách xác định tính an toàn và các phương pháp chứng minh tính an toàn ở cấp độ mật mã; giải thích các thuật toán và giao thức mật mã hiện đại phổ biến được sử dụng như thế nào; và minh họa cách thức sử dụng chúng một cách đúng đắn cũng như chứng minh mức độ an toàn của chúng.

Hơn nữa, môn học chủ yếu tập trung vào việc sử dụng các hệ mật hiện đại phổ biến trong các ứng dụng thực tế hơn là các khía cạnh lý thuyết của mật mã học.

Aims:

The main objectives of this course are to give the fundamentals of modern cryptography; to present how security is defined and proven at the cryptographic level; to explain how widely-used modern cryptography algorithms and protocols work; and to demonstrate how to use them correctly and reason about their security.

Moreover, the course mainly focuses on applying popular modern cryptosystems in practical problems rather on theoretical aspects in cryptography.

2. <u>Nội dung tóm tắt môn học:</u>

Các chủ đề cơ bản sẽ được đề cập trong môn học này bao gồm mã hóa an toàn, chữ ký số và xác thực số. Môn học sẽ thảo luận chi tiết về các chủ đề này, việc hiện thực và các ứng dụng của chúng. Cụ thể hơn, môn học sẽ bao gồm các chủ đề sau

- mật mã cổ điển (ngắn gọn);

- mật mã học hiện đại và các khái niệm cơ bản về mật mã khóa đối xứng;

- các nguyên tắc thiết kế cơ bản cho hệ mã khối, như hệ mã khối DES và AES;

- một số bài toán "khó" và cơ sở về lý thuyết số cần thiết để hiểu các hệ thống mã hóa RSA, Diffie-Hellman và El Gamal. Môn học cũng đưa ra một số ví dụ về cách các giả định liên quan đến lý thuyết số được sử dụng trong mật mã học;

- lý do cần phải thiết lập các hệ mã khóa công khai và cách xây dựng các hệ mã này (bao gồm các lược đồ dựa trên RSA và hệ mã El Gamal);

- các lược đồ chữ ký số và ứng dụng;

- mô hình "máy tư vấn ngẫu nhiên" và lược đồ chữ ký số RSA-FDH.

Course outline:

The basic topics will be covered in this course include secure encryption, digital signatures, and authentication. The course will discuss on theses topics, their realizations, and applications. More precisely, the course will cover

- classical cryptography (briefly);

- modern cryptography, and the basics of private-key cryptography;

- illustrating basic design principles for block ciphers and including material on the widely-used block ciphers DES and AES;

- introducing concrete mathematical problems believed to be "hard", and providing the number-theoretic background needed to understand the RSA, Diffie-Hellman, and El Gamal cryptosystems. The course also gives the first examples of how number-theoretic assumptions are used in cryptography;

- motivating the public-key setting and discussing public-key encryption (including RSA-based schemes and El Gamal encryption);

- describing digital signature schemes and applications;

- introducing the random oracle model and the RSA-FDH signature scheme.

3. Tài liệu học tập:

[1] Boneh, Dan, and Victor Shoup. "A graduate course in applied cryptography." *Version 0.4, from http://cryptobook. net* (2017).

[2] Goldreich, Oded. *Foundations of cryptography: volume 2, basic applications*. Cambridge University Press, 2009.

[3] Katz, Jonathan, et al. *Handbook of applied cryptography*. CRC Press, 1996.

[4] Katz, Jonathan, and Yehuda Lindell. *Introduction to modern cryptography*. CRC Press, 2014.

[5] Mao, Wenbo. *Modern cryptography: theory and practice*. Prentice Hall, 2003.

[6] Stinson, Douglas R. *Cryptography: theory and practice*. CRC Press, 2005.

[7] Swenson, Christopher. *Modern cryptanalysis: techniques for advanced code breaking*. John Wiley & Sons, 2008.

4. Các hiểu biết, các kỹ năng cần đạt được sau khi học môn học:

STT	Chuẩn đầu ra môn học (CĐRMH)	Công cụ đánh giá CĐRMH	Đóng góp CĐR Chương trình (CĐRCT)		
			Ứng dụng	Nghiên cứu	
CĐRMH.1	Kiến thức nền tảng về mật mã học hiện đại	Thuyết Trình, Thi cuối kì	i, j		1.3
CĐRMH.2	Khả năng chứng minh tính an toàn khi hiện thực các hệ mã trong các hệ thống thực tế	Bài tập, Thi cuối kì	h, i		2.1, 2.3
CĐRMH.3	Khả năng áp dụng các kỹ thuật mật mã thích hợp cho vấn đề bảo mật trong công nghiệp	Bài tập, Thi cuối kì	h		2.2

Learning outcomes:

No.	Course learning outcomes (CLO)	CLO assessment	Matching with PLO		
			Coursework	Research	
L.O.1	Having knowledge of the basic concepts of modern cryptography, and the fundamentals	Projects, Final Exam	i, j		1.3
L.O.2	Ability to show how security is achieved in reallife systems	Exercises, Final Exam	h, i		2.1, 2.3
L.O.3	Ability to use appropriate cryptographic techniques in security engineering to solve reallife problem at hand	Exercises, Final Exam	h		2.2

Bảng ánh xạ chuẩn đầu ra môn học và chuẩn đầu ra chương trình ứng dụng:

	Chuẩn đầu ra của chương trình (CĐRCT)										
Chuẩn đầu ra môn học (CĐRMH)	a	b	c	d	e	f	g	h	i	j	k
CĐRMH.1									×	×	
CĐRMH.2								×	×		
CĐRMH.3								×			

Bảng ánh xạ chuẩn đầu ra môn học và chuẩn đầu ra chương trình nghiên cứu:

	Chuẩn đầu ra của chương trình (CĐRCT)										
Chuẩn đầu ra môn học (CĐRMH)	a	b	c	d	e	f	g	h	i	j	k
CĐRMH.1											
CĐRMH.2											
CĐRMH.3											

5. Hướng dẫn cách học - chi tiết cách đánh giá môn học:

Phương pháp học chủ yếu sẽ là nghe các bài giảng, tham gia thảo luận trên lớp và nghiên cứu các trường hợp điển hình.

Học viên nên có một vai trò tích cực trong môn học, cần tham dự đầy đủ các bài giảng và tham gia tích cực vào việc thảo luận, trình bày trên lớp.

Học viên sẽ phải hoàn thành các bài tập về nhà, đồ án môn học, chuyên đề, bài tập lớn và làm một bài thi cuối kỳ.

Cách đánh giá:

- Chuyên cần: 5%

- Bài tập về nhà: 20%

- Đồ án môn học: 25%

- Thi cuối kì: 50%

Learning strategies & Assessment Scheme:

The primary learning method will be attending lectures, participating in class discussions and studying case studies.

Students should have an active role in the courses, should attend all lectures, be actively involved in discussion and give presentation in class.

Students will be required to complete homework, assignments, projects, and take the final examination.

Grading:

- Class attendant: 5%

- Homeworks: 20%

- Project: 25%

- Final exam: 50%

6. Nội dung chi tiết:

Tuần/ Buổi	Chủ đề (chương)	Nội dung	Chuẩn đầu ra môn học	Tài liệu
1	Giới thiệu về mã hóa thông tin	- Khái niệm - Lịch sử về lý thuyết mã hóa - Các mô hình mật mã		[1, 2]
2-3	Các phương pháp mã hóa cổ điển	Phương pháp mã hóa đơn giản: hoán vị trong bảng chữ cái, mật mã cộng tính, mật mã nhân tính, ...		[1, 2]
4	Hướng tiếp cận Shannon	- Phân tích mã theo phương pháp thống kê - Lý thuyết về sự bí mật tuyệt đối		[3]
5-6	Hệ thống mã với khóa riêng	- Khái niệm - Block ciphers AES, DES,...		[1-3]
7	Hash functions	- Khái niệm - Secure Hash algorithm		[1-3]
8-9	Hệ thống mã với khóa công khai	- Khái niệm: đặc trưng và nguyên tắc - Một số giải thuật phổ biến: RSA, DSA, ...		[1-3]

Tuần/ Buổi	Chủ đề (chương)	Nội dung	Chuẩn đầu ra môn học	Tài liệu
10	Các vấn đề về mã hóa liên quan đến hệ thống bảo mật	- Chữ ký điện tử - Quản lý khóa trong hệ thống mật mã - Giao thức mật mã		[1-7]

7. Giảng viên tham gia giảng dạy:

CBGD chính:	TS. Trương Tuấn Anh
CBGD tham gia:	TS. Nguyễn An Khương

XÁC NHẬN
CỦA HỘI
ĐỒNG XÂY
DỰNG
CHƯƠNG
TRÌNH ĐÀO
TẠO VÀ KHOA

Tp. Hồ Chí
Minh, ngày
..... tháng
..... năm
.....
GIẢNG
VIÊN
LẬP ĐỀ
CƯƠNG

PGS.TS
Phạm
Hoàng
Anh