MI4100 MẬT MÃ VÀ ĐỘ PHỨC TẠP THUẬT TOÁN

Phiên bản: 2020.1.0

1. THÔNG TIN CHUNG

Tên học phần:	Mật mã và độ phức tạp thuật toán *(Complexity and Cryptography)*
Mã số học phần:	MI4100
Khối lượng:	3(3-1-0-6) - Lý thuyết: 45 tiết - Bài tập/BTL: 15 tiết - Thí nghiệm: 0 tiết
Học phần tiên quyết:	-
Học phần học trước:	- MI1141 Đại số - MI3010 Toán rời rạc
Học phần song hành:	

2. MÔ TẢ HỌC PHẦN

Mật mã và độ phức tạp thuật toán là học phần cơ sở, bắt buộc của chương trình đào tạo. Học phần này được thiết kế với mục đích:

- Cung cấp kiến thức nền tảng về lý thuyết độ phức tạp tính toán, lý thuyết mã và ứng dụng của các lý thuyết này trong lĩnh vực biểu diễn thông tin, mật mã, truyền thông dữ liệu.
- Giới thiệu những kết quả, thành tựu tiêu biểu của mật mã học trong việc bảo đảm an ninh, an toàn thông tin.
- Trang bị những hiểu biết liên quan đến các tiêu chuẩn, công nghệ mật mã; cách thức thiết kế, cài đặt các hệ mật và các giao thức bảo mật; phân tích, đánh giá hiệu quả hoạt động cũng như độ an toàn của các hệ mật và các sơ đồ ứng dụng mật mã.

This is a mandatory course. The course is designed with the following goals.

- To provide fundamental knowledge related to the theory of computational complexity and the theory of codes, and applications of these two theories in information representation, cryptography and data communications.
- To introduce achievements and new results in the field of cryptography that can be used to protect information systems.
- Students of this course can develop their ability to work independently or in a group for solving information security problems.

3. MỤC TIÊU VÀ CHUẨN ĐẦU RA CỦA HỌC PHẦN

Sinh viên hoàn thành học phần này có khả năng:

Mục tiêu/CĐR	Mô tả mục tiêu/Chuẩn đầu ra của học phần	CĐR được phân bổ cho HP/ Mức độ (I/T/U)
[1]	[2]	[3]
M1	**Hiểu và phân tích được các kiến thức cơ sở độ phức tạp tính toán, mã hóa và ứng dụng của mã hóa**	2.1.1;2.1.2
M1.1	Trình bày được các khái niệm về máy Turing và độ phức tạp tính toán. Xây dựng được mô hình máy Turing tính hàm cho trước.	[2.1.1;2.1.2](T)
M1.2	Trình bày được các khái niệm liên quan mật mã, mã khóa bí mật, mã khóa công khai, mã phát hiện lỗi và sửa lỗi.	[2.1.1;2.1.2](T)
M2	**Khả năng vận dụng mật mã trong an ninh thông tin**	2.1.1;2.1.2
M2.1	So sánh các loại hệ mật mã khóa bí mật, mật mã khóa công khai. Khả năng phân tích sơ đồ áp dụng trong giải quyết các bài toán thực tiễn về an ninh thông tin (chữ ký số, giao thức bảo mật,...)	[2.1.1;2.1.2](TU)
M2.2	Mô tả thuật toán mã phát hiện lỗi và mã sửa lỗi. Thực hiện tính toán mã phát hiện lỗi, mã sửa lỗi.	[2.1.1;2.1.2](TU)
M3	**Thái độ làm việc nghiêm túc, tự chủ tìm hiểu các kiến thức mới về mật mã và ứng dụng**	2.1.3;2.1.4
M3.1	Có ý thức kỷ luật học tập, tinh thần khám phá kiến thức. Bước đầu tìm hiểu khả năng áp dụng mật mã trong thực tiễn, rèn luyện kỹ năng tự đọc, tra cứu và tự nghiên cứu về an ninh bảo mật.	[2.1.3;2.1.4](I)

4. TÀI LIỆU HỌC TẬP

Giáo trình

[1] Bài giảng powerpoint

Sách tham khảo

[1] A. Binstock and J. Rex (1995), *Practical Algorithms for Programmers*, Addition-Wesley-Publishing Company

[2] J. Berstel, D. Perrin (1985), *Theory of Codes*, Academic Press. INC. New York, London

[3] D. Stinson, M. Paterson (2018), *Cryptography Theory and Practice*, Chapman and Hall/CRC

[4] A. Salomaa, *Nhập môn tin học lý thuyết - tính toán và các otomat*, (bản dịch tiếng Việt. Ng. Dịch. Nguyễn Xuân My- Phạm Trà Ân) NXB KHKT, Hà nội, 1992

[5] W. Stalling, *Cryptography and Network Security*, 4th, Prentice Hall, 2005

[6] Phạm Huy Điển and Hà Huy Khoái (2004), *Mã hóa thông tin:Cơ sở toán học và ứng dụng*, NXB Đại học Quốc gia Hà Nội, Hà Nội

5. CÁCH ĐÁNH GIÁ HỌC PHẦN

Điểm thành phần	Phương pháp đánh giá cụ thể	Mô tả	CĐR được đánh giá	Tỷ trọng
[1]	[2]	[3]	[4]	[5]
A1. Điểm quá trình (*)	**Đánh giá quá trình**			**30%**
	A1.1. Thảo luận trên lớp, bài tập	Thuyết trình Bài tập	M1.1; M1.2; M2.1; M2.2; M3.1	
	A1.2. Thi giữa kỳ	Thi trắc nghiệm/ tự luận	M1.1; M1.2; M2.1; M2.2;	
A2. Điểm cuối kỳ	**A2.1. Thi cuối kỳ**	Thi tự luận/ Vấn đáp/ Bài tập lớn	M1.1; M1.2; M2.1; M2.2; M3.1	**70%**

** Điểm quá trình sẽ được điều chỉnh bằng cách cộng thêm điểm chuyên cần, điểm tích cực học tập. Điểm chuyên cần và điểm tích cực học tập có giá trị từ –2 đến +2, theo qui định của Viện Toán ứng dụng và Tin học cùng Quy chế Đào tạo đại học hệ chính quy của Trường ĐH Bách khoa Hà Nội.*

6. KẾ HOẠCH GIẢNG DẠY

Tuần	Nội dung	CĐR học phần	Hoạt động dạy và học	Bài đánh giá
[1]	[2]	[3]	[4]	[5]
1	**Chương 1: Thuật toán và Máy Turing** 1.1 Máy Turing 1.2 Máy Turing và hàm tính được	M1.1 M2.1	Giảng bài Bài tập	A1.2; A2.1
2	1.3 Các biến thế máy Turing 1.4 Máy Turing vạn năng	M1.1 M2.1	Đọc trước tài liệu; Giảng bài Bài tập	A1.1; A1.2; A2.1
3	1.5 Độ phức tạp tính toán 1.6 Lớp P và NP	M1.1 M2.1	Đọc trước tài liệu; Giảng bài;	A1.1; A1.2; A2.1
4	**Chương 2: Tổng quan về mật mã** 2.1 Lịch sử mật mã 2.2 Một số hệ mật cổ điển	M1.2; M2.2	Đọc trước tài liệu; Giảng bài; Bài tập	A1.1; A1.2; A2.1
5	2.3 Độ mật và Thám mã 2.4 Mã Hufman	M1.2; M2.2	Đọc trước tài liệu; Giảng bài; Bài tập	A1.1; A1.2; A2.1

Tuần	Nội dung	CĐR học phần	Hoạt động dạy và học	Bài đánh giá
[1]	[2]	[3]	[4]	[5]
6	2.5 Tích các hệ mã 2.6 Mã đại số	M1.2; M2.2	Đọc trước tài liệu; Giảng bài; Thảo luận	A1.1; A2.1
7	**Chương 3: Mật mã khóa bí mật** 3.1 Mật mã khóa đối xứng 3.2 Mạng Feistel, mạng SPN	M1.2; M2.2	Đọc trước tài liệu; Giảng bài;	A1.1; A1.2; A2.1
8	3.3 Chuẩn mã hóa dữ liệu DES 3.4 Chuẩn mã hóa nâng cao AES	M1.2; M2.2	Đọc trước tài liệu; Giảng bài; Thảo luận	A1.1; A1.2; A2.1
9	**Chương 4: Mật mã khóa công khai** 4.1 Mật mã khóa công khai 4.2 Hệ mật RSA	M1.2; M2.2; M3.1	Đọc trước tài liệu; Giảng bài; Thảo luận	A1.1; A1.2; A2.1
10	4.3 Chữ ký số 4.4 Hàm băm	M1.2; M2.2	Đọc trước tài liệu; Giảng bài;	A1.1; A2.1
11	**Chương 5: Mã phát hiện lỗi và sửa lỗi** 5.1 Cơ sở Toán học 5.2 Phát hiện lỗi 5.3 CRC	M1.2; M2.2; M3.1	Đọc trước tài liệu; Giảng bài; Bài tập	A1.1; A2.1
12	5.4 Mã sửa lỗi 5.5 Khoảng cách Hamming	M1.2; M2.2	Đọc trước tài liệu; Giảng bài;	A1.1; A2.1
13	5.6 Mã sửa lỗi Hamming	M1.2; M2.2; M3.1	Đọc trước tài liệu; Giảng bài; Bài tập	A1.1; A2.1
14	5.7 Nén dữ liệu	M1.2; M2.2	Đọc trước tài liệu; Giảng bài;	A1.1; A2.1
15	***Tổng kết và ôn tập***			

7. QUY ĐỊNH CỦA HỌC PHẦN

(Các quy định của học phần nếu có)

Tuân thủ quy định học tập trong quy chế đào tạo của Trường ĐHBK Hà Nội.

8. NGÀY PHÊ DUYỆT: ……..

Chủ tịch Hội đồng **Nhóm xây dựng đề cương**

TS. Vũ Thành Nam

9. QUÁ TRÌNH CẬP NHẬT

Lần cập nhật	Nội dung điều chỉnh	Ngày tháng được phê duyệt	Áp dụng từ kỳ/khóa	Ghi chú
1	Cập nhật theo chuẩn CDIO			
2				