IT4025 MẬT MÃ ỨNG DỤNG

Phiên bản: 2019.1.0

1. THÔNG TIN CHUNG

Tên học phần: Mật mã ứng dụng
(Applied Cryptography)

Mã số học phần: IT4025

Khối lượng: 3(3-1-0-6)
- Lý thuyết: 45 tiết
- BTL: 15 tiết
- Thí nghiệm: 0 tiết

Học phần tiên quyết: - Không có

Học phần học trước: - IT4010 - Nhập môn An toàn Thông tin

Học phần song hành: - Không có

2. MÔ TẢ HỌC PHẦN

Mật mã là công cụ không thể thiếu để bảo vệ an toàn thông tin trong các hệ thống máy tính. Môn học Mật Mã Ứng Dụng dụng giúp sinh viên hiểu các thành phần cơ bản của mật mã và sử dụng chúng một cách đúng đắn.

Về nội dung, môn học giới thiệu kiến thức cơ bản về mật mã hiện đại: mã đối xứng, mã công khai, hàm băm, sơ đồ mã hóa có xác thực, chữ ký điện tử và các giao thức mật mã. Ngoài ra, các phương pháp tấn công và phương pháp chứng minh tính an toàn của một số sơ đồ mật mã cụ thể cũng được trình bày chi tiết.

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	**Nắm vững ý nghĩa, tầm quan trọng và mục đích cụ thể của An Toàn Thông Tin (ATTT) trong đời sống**	1.2.4, 1.3.1
M1.1	Hiểu các mục tiêu cơ bản của ATTT	1.2.4(IT) 1.3.1 (I)
M1.2	Hiểu các yêu cầu ATTT trong đời sống	1.2.4(TU) 1.3.1 (I)
M2	**Hiểu về cách sử dụng công cụ mật mã trong việc xây dựng giải pháp ATTT trong thực tế**	1.2.4,1.3.1, 2.1.1-4, 2.5.3-4, 2.5.3-4
M2.1	Phân tích các phương pháp tấn công đe dọa đến an toàn hệ thống thông tin	1.2.4(TU) 1.3.1 (I)

Mục tiêu/CĐR	Mô tả mục tiêu/Chuẩn đầu ra của học phần	CĐR được phân bổ cho HP/ Mức độ (I/T/U)
		[2.1.1,2.1.2](T) [2.1.3,2.1.4](I)
M2.2	Hiểu về cách sử dụng đúng đắn công cụ mật mã trong ATTT	1.2.4(TU) 1.3.1 (I) [2.1.1,2.1.2](T) [2.1.3,2.1.4](I) 2.5.3-4 (I)
M3	**Hiểu các thành phần mật mã cơ bản**	1.1.2,1.1.4,1.2.1,1.2.2 1.2.4,1.3.1,1.4.1,2.1.1-4, 2.4.2-4, 3.3.3, 3.3.3
M3.1	Hiểu về các công cụ mật mã cơ sở: mật mã đối xứng, mật mã công khai, mã hóa có xác thực, chữ ký điện tử, cơ sở hạ tầng khóa công khai.	1.1.2 (IU);1.1.4(U); 1.2.1(IU);1.2.4(TU) 3.3.3 (U)
M3.2	Hiểu về các giao thức mật mã	1.2.4(TU),3.3.3 (U) [1.3.1,1.4.1](I) [2.1.1,2.1.2](T) [2.1.3,2.1.4](I), 3.3.3 (U)

4. TÀI LIỆU HỌC TẬP

Giáo trình

[1] Jonathan Katz, Yehuda Lindell (2014). *Introduction to Modern Cryptography*. Second Edition. Chapman &Hall/CRC.

Sách tham khảo

[1] Serge Vaudenay (2006). *A Classical Introduction to Cryptography: Applications for Communications Security*. Springer.

[2] Mihir Bellare, Phillip Rogaway (2014). *Introduction to Modern Cryptography* (Course notes).

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**			**40%**
	A1.1. Bài tập về nhà	Tự luận	M2, M3	10%
	A1.2. Bài tập nhóm	Làm việc	M1÷M3	30%

		nhóm, lập trình, viết báo cáo		
A2. Điểm cuối kỳ	**A2.1. Thi cuối kỳ**	Thi viết	M1,M2,M3	**60%**

** - Giáo viên có thể lựa chọn chấm điểm Bài tập về nhà hoặc không. Nếu không có Bài tập về nhà, điểm Bài tập lớn sẽ có tỷ trọng là 40%.*

- Điểm quá trình có thể được điều chỉnh bằng cách cộng thêm điểm chuyên cần. Điểm chuyên cần có giá trị từ –2 đến +1, theo 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: Giới thiệu chung 1.1 Mật mã là gì? 1.2 Mật mã khóa đối xứng 1.3 Lịch sử mật mã và thám mã 1.4 Các nguyên lý của mật mã hiện đại	M1, M3	Giảng bài; Chữa bài tập.	A1.1, A2.1
2	Chương 2: Mã hóa bí mật tuyệt đối 2.1 Định nghĩa 2.2 One-Time Pad 2.3 Hạn chế của mã hóa bí mật tuyệt đối 2.4 Định lý của Shannon	M1,M3	Đọc trước tài liệu; Giảng bài; Chữa bài tập.	A1.1, A1.2, A2.1
3	Chương 3: Mã hóa khóa bí mật (đối xứng) 3.1 An toàn theo độ phức tạp tính toán 3.2 Định nghĩa về sơ đồ mã hóa an toàn 3.3 Xây dựng các sơ đồ mã hóa an toàn	M3	Đọc trước tài liệu; Giảng bài; Chữa bài tập.	A1.1, A2.1
4	3.4 Một số định nghĩa về an toàn 3.5 Xây dựng sơ đồ mã hóa an toàn trước tấn công chọn bản rõ 3.6 Các mode sử dụng 3.7 Phương pháp tấn công chọn bản mã	M1, M2, M3	Đọc trước tài liệu; Giảng bài; Chữa bài tập.	A1.1, A1.2, A2.1
5	Chương 4: Mã xác thực thông điệp 4.1 Toàn vẹn thông điệp 4.2 Định nghĩa về Mã xác thực thông điệp 4.3 Xây dựng mã xác thực thông điệp 4.4 CBC-MAC	M1, M3	Đọc trước tài liệu; Giảng bài; Chữa bài tập.	A1.1, A2.1
6	4.5 Mã hóa có xác thực 4.6 Mã xác thực thông điệp theo lý thuyết thông tin	M1, M2, M3	Đọc trước tài liệu; Giảng bài;	A1.1, A1.2,

Tuần	Nội dung	CĐR học phần	Hoạt động dạy và học	Bài đánh giá
[1]	[2]	[3]	[4]	[5]
			Chữa bài tập.	A2.1
7	Chương 5: Hàm băm và ứng dụng 5.1 Định nghĩa 5.2 Sơ đồ Merkle-Damgard 5.3 Mã xác thực dùng hàm băm 5.4 Phương pháp tổng quát để tấn công hàm băm 5.5. Mô hình truy vấn ngẫu nhiên (Random-Orable Model) 5.6 Một số ứng dụng	M1, M3	Đọc trước tài liệu; Giảng bài; Chữa bài tập.	A1.1, A1.2, A2.1
8	Chương 6: Xây dựng thực tế các thành phần khóa đối xứng 6.1 Mã dòng (LFSR, RC4) 6.2 Mã khối (DES, 3DES, AES) 6.3 Hàm băm (MD5, SHA-{0,1, 2}, SHA-3)	M1, M2	Đọc trước tài liệu; Giảng bài; Chữa bài tập.	A1.1, A1.2, A2.1
9	Ôn tập & thi giữa kỳ Review for Midterm exam	M1, M2,M3	Chữa bài tập & thi	A1.1, A2.1
10	Chương 7: Lý thuyết số và các bài toán khó 8.1 Cơ sở lý thuyết nhóm 8.2 Số nguyên tố, phân tích thừa số và RSA 8.3 Các giả sử mật mã trong nhóm vòng 8.4 Một số ứng dụng mật mã	M3	Đọc trước tài liệu; Giảng bài; Chữa bài tập.	A1.1, A1.2, A2.1
11	Chương 8: Bài toán quản lý khóa và mật mã khóa công khai 10.1 Phân phối khóa và quản lý khóa 10.2 Giải pháp đơn giản: Trung tâm phân phối khóa 10.3 Trao đổi khóa và giao thức Diffie-Hellman 10.4 Cuộc cách mạng Khóa Công Khai	M2, M3	Đọc trước tài liệu; Giảng bài; Chữa bài tập.	A1.1, A2.1
12	Chương 9: Mã hóa công khai 11.1 Tổng quan về mã hóa công khai 11.2 Định nghĩa 11.3 Mã hóa lai (Hybrid Encryption) và lược đồ KEM/DEM	M1,M2, M3	Đọc trước tài liệu; Giảng bài; Chữa bài tập.	A1.1, A1.2, A2.1
13	11.4 Mã hóa dựa trên bài toán	M3	Đọc trước tài	A1.1,

Tuần	Nội dung	CĐR học phần	Hoạt động dạy và học	Bài đánh giá
[1]	[2]	[3]	[4]	[5]
	CDH/DDH 11.5 Mã hóa RSA		liệu; Giảng bài; Chữa bài tập.	A2.1
14	Chương 10: Chữ ký điện tử 12.1 Tổng quan về chữ ký điện tử 12.2 Định nghĩa 12.3 Lược đồ Băm-và-Ký 12.4 Lược đồ ký RSA 12.5 Các lược đồ ký từ bài toán Logarit rời rạc	M2, M3	Đọc trước tài liệu; Giảng bài; Chữa bài tập.	A1.1, A2.1
15	Ôn tập	M1,M2, M3	Chữa bài tập.	A2.1

7. QUY ĐỊNH CỦA HỌC PHẦN

8. NGÀY PHÊ DUYỆT: ……..

Chủ tịch Hội đồng

Nhóm xây dựng đề cương
Trần Vĩnh Đức và
Nguyễn Linh Giang

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	……			
2	……			