TRƯỜNG ĐẠI HỌC GIAO THÔNG VẬN TẢI
Bộ Môn: Khoa học máy tính
Chuẩn đầu ra môn học:
1. Hiểu và so sánh được những kiến thức cơ bản về an toàn và bảo mật thông tin bao gồm lý thuyết mã hóa, lý thuyết số, xác thực, chữ ký điện tử, phân phối khóa.

KỊCH BẢN DẠY HỌC B-LEARNING

Số tiết học trực tiếp 45p (1)	Số tiết học trực tuyến 45p (2)	Tên phân đoạn học liệu (Chương bài), số tiết (3)	Mục tiêu buổi học (4)	Loại hình học liệu (5)	Thời lượng phân đoạn (số trang, số slide, số phút video, audio..)	Phương pháp và phương tiện dạy học (6)	Đánh giá (7)	Ghi chú (8)
3	0	Chương 1. Mở đầu 1.1. Giới thiệu tổng quan môn học	Hướng dẫn cho sinh viên tổng quát về môn học, cách học và cách giảng viên đánh giá để sinh viên có phương pháp tiếp thu kiến thức thích hợp. Giới thiệu một số khái niệm cơ bản	*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát.	A.1.1 A1.2 A.2	
		1.2 Một số khái niệm cơ bản		*+ Slide* *+ Bài giảng dạng PDF*				
6	0	Chương 2. Mã hóa cổ điển 2.1. Các khái niệm về mã hóa	Hiểu và phân biệt được mã thế và mã hoán vị. Hiểu rõ các phương pháp mã hóa thế và hoán vị cổ điển. Có khả năng viết chương trình máy tính Biết cách áp dụng vào ứng dụng cụ thể	*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát; - Hướng dẫn bài tập	A1 A2	
		2.2. Mã thế				- Giảng viên thuyết giảng;		
		Mã Caesar		*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát; - Hướng dẫn bài tập		
		Mã cặp - playfair		*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát; - Hướng dẫn bài tập		
		2.3. Mã hoán vị và mã hoán vị cải tiến		*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát; - Hướng dẫn bài tập		
0	3	[Tự học] Mã đơn bảng chữ & Mã đa bảng chữ		*- Slide* *- Bài giảng dạng PDF* *- Câu hỏi ôn tập dạng Quiz* *- Video*		-Sinh viên xem bài giảng video tương ứng , đọc thêm tài liệu gửi kèm. - Làm câu hỏi trắc nghiệm		
		[Tự học] Mã Hill		*- Slide* *- Bài giảng dạng PDF* *- Câu hỏi ôn tập dạng Quiz* *- Video*		-Sinh viên xem bài giảng video tương ứng , đọc thêm tài liệu gửi kèm. - Làm câu hỏi trắc nghiệm		
9	0	Chương 3. Lý thuyết số 3.1 Giới thiệu Modulo	Nắm được các kiến thức cơ bản của Lý thuyết số học Modulo Có khả năng viết chương trình Biết áp dụng vào các bài toán cụ thể	*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát; - Hướng dẫn bài tập	A1 A2	
		3.2 Các phép toán modulo		*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát; - Hướng dẫn bài tập		
		3.4 Giải phương trình và hệ phương trình đồng dư		*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát; - Hướng dẫn bài tập		

		3.5 Tính lũy thừa modulo		*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát; - Hướng dẫn bài tập		
0	3	[Tự học] 3.3 Tính nghịch đảo modulo		*- Slide* *- Bài giảng dạng PDF* *- Câu hỏi ôn tập dạng Quiz* *- Video*		-Sinh viên xem bài giảng video tương ứng , đọc thêm tài liệu gửi kèm. - Làm câu hỏi trắc nghiệm		
		[Tự học] 3.6 Căn nguyên thủy và Logarit rời rạc		*- Slide* *- Bài giảng dạng PDF* *- Câu hỏi ôn tập dạng Quiz* *- Video*		-Sinh viên xem bài giảng video tương ứng , đọc thêm tài liệu gửi kèm. - Làm câu hỏi trắc nghiệm		
6	0	Chương 4. Mã khối hiện đại 4.1 Giới thiệu tổng quan	Hiểu được các phương pháp mã hiện đại gồm DES, AES, và mã dòng Có khả năng lập trình các phương pháp mã hóa Biết ứng dụng vào bài toán cụ thể	*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng;	A1 A2	
		4.4. Chuẩn mã hóa dữ liệu nâng cao (AES) (LT 1 + BT 2 + thH 1)		*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát; - Hướng dẫn bài tập		
0	3	[Tự học] 4.2 Chuẩn mã hóa dữ liệu (DES)		*- Slide* *- Bài giảng dạng PDF* *- Câu hỏi ôn tập dạng Quiz* *- Video*	2	-Sinh viên xem bài giảng video tương ứng , đọc thêm tài liệu gửi kèm. - Làm câu hỏi trắc nghiệm		
		[Tự học] 4.3 Trường hữu hạn GF 2^8		*- Slide* *- Bài giảng dạng PDF* *- Câu hỏi ôn tập dạng Quiz* *- Video*	2	-Sinh viên xem bài giảng video tương ứng , đọc thêm tài liệu gửi kèm. - Làm câu hỏi trắc nghiệm		
		[Tự học] 4.5. Mã dòng hiện đại		*- Slide* *- Bài giảng dạng PDF* *- Câu hỏi ôn tập dạng Quiz* *- Video*		-Sinh viên xem bài giảng video tương ứng , đọc thêm tài liệu gửi kèm. - Làm câu hỏi trắc nghiệm		
6	0	Chương 5. Mã công khai 5.1 Giới thiệu tổng quan	Hiểu được các phương pháp mã công khai như RSA, Elgamal, Diffie-Hellman Có khả năng lập trình các phương pháp mã hóa Biết ứng dụng vào bài toán cụ thể	*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát; - Hướng dẫn bài tập	A1 A2	
		5.2 Mã công khai RSA		*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát; - Hướng dẫn bài tập		
		5.4 Trao đổi khóa Diffie-Hellman		*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát; - Hướng dẫn bài tập		
0	3	[Tự học] 5.3 Mã công khai Elgamal		*- Slide* *- Bài giảng dạng PDF* *- Câu hỏi ôn tập dạng Quiz* *- Video*		-Sinh viên xem bài giảng video tương ứng , đọc thêm tài liệu gửi kèm. - Làm câu hỏi trắc nghiệm		
		[Tự học] 6.2 Mã xác thực thông điệp		- Slide - Bài giảng dạng PDF - Câu hỏi ôn tập dạng Quiz - Video		-Sinh viên xem bài giảng video tương ứng , đọc thêm tài liệu gửi kèm. - Làm câu hỏi trắc nghiệm		
		[Tự học] 6.3 Hàm băm						
		[Tự học] 6.4 SHA						
3	0	Chương 6. Xác thực thông điệp 6.1 Giới thiệu về xác thực thông điệp	Hiểu về xác thực thông điệp, các phương pháp xác thực.	*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát;	A1 A2	
		6.5 Chữ ký điện tử DSA		*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát; - Hướng dẫn bài tập		
		Chương 7. Một số ứng dụng bảo mật trên mạng 7.1 Giới thiệu một số ứng dụng bảo mật trên mạng	Hiểu về một số ứng dụng bảo mật trên mạng,	*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát;	A1.1 A1.2	
		7.5 An toàn thư điện tử & thanh toán điện tử		*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát;		
		Chương 8. An ninh hệ thống 8.1 Giới thiệu mô hình an ninh hệ thống	Hiểu về một số mô hình an hình an ninh hệ thống	*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát;	A1.1 A1.2	
		8.5 Hệ thống thông tin an toàn		*+ Slide* *+ Bài giảng dạng PDF*		- Giảng viên thuyết giảng; - Câu hỏi tổng quát;		

0	3	[Tự học] 7.2 Trao đổi khóa		- Slide - Bài giảng dạng PDF - Câu hỏi ôn tập dạng Quiz - Video		-Sinh viên xem bài giảng video tương ứng , đọc thêm tài liệu gửi kèm. - Làm câu hỏi trắc nghiệm		
		[Tự học] 7.3. Xác thực người sử dụng Kerberos						
		[Tự học] 7.4 Một số giao thức an ninh						
		[Tự học] 8.2 Kẻ xâm nhập		- Slide - Bài giảng dạng PDF - Câu hỏi ôn tập dạng Quiz - Video		-Sinh viên xem bài giảng video tương ứng , đọc thêm tài liệu gửi kèm. - Làm câu hỏi trắc nghiệm		
		[Tự học] 8.3 Phần mềm có hại						
		[Tự học] 8.4 Bức tường lửa						
3		Ôn tập	Tổng kết lý thuyết	*+ Slide* *+ Bài giảng dạng PDF*			A1.1	
		Nghiệm thu bài thực hành	Đánh giá kết quả thực hành				A1.4	
36	15							