TRƯỜNG ĐẠI HỌC HỒNG ĐỨC
Khoa CNTT&TT
Bộ môn Khoa học máy tính

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN:
LÝ THUYẾT MẬT MÃ
MÃ HỌC PHẦN : 173043

1. Thông tin về giảng viên:

- Họ và tên: **Trịnh Viết Cường**
  Chức danh, học hàm, học vị: Giảng viên, Tiến sĩ Khoa học máy tính
  Thời gian, địa điểm làm việc: Các ngày trong tuần từ thứ 2 đến thứ 6, tại khoa CNTT&TT.
  Địa chỉ liên hệ: Khoa CNTT&TT, trường ĐHHĐ
  Điện thoại: DĐ: 0948.921.740
  Email: *trinhvietcuong@hdu.edu.vn*
- Họ và tên: **Nguyễn Đình Định**
  Chức danh, học hàm, học vị: Giảng viên, Thạc sĩ CNTT
  Thời gian, địa điểm làm việc: Các ngày trong tuần từ thứ 2 đến thứ 6, tại khoa CNTT&TT.
  Địa chỉ liên hệ: Khoa CNTT&TT, trường ĐHHĐ
  Điện thoại: DĐ: 0953.826.552
  Email: *nguyendinhdinh@hdu.edu.vn*
- Họ và tên: **Trịnh Thị Phú**
  Chức danh, học hàm, học vị: Giảng viên, Thạc sĩ CNTT
  Thời gian, địa điểm làm việc: Các ngày trong tuần từ thứ 2 đến thứ 6, tại khoa CNTT&TT.
  Địa chỉ liên hệ: Khoa CNTT&TT, trường ĐHHĐ
  Điện thoại: DĐ: 0904.470.579
  Email: *trinhthiphu@hdu.edu.vn*
- Họ và tên: **Phạm Thế Anh**
  Chức danh, học hàm, học vị: Giảng viên, PGS.Tiến sĩ Khoa học máy tính
  Thời gian, địa điểm làm việc: Các ngày trong tuần từ thứ 2 đến thứ 6, tại khoa CNTT&TT.
  Địa chỉ liên hệ: Khoa CNTT&TT, trường ĐHHĐ

Điện thoại: DĐ: 0941.070.715

Email: phamtheanh@hdu.edu.vn

2. Thông tin chung về học phần:

Tên ngành/khoá đào tạo: ĐH Công nghệ thông tin

Tên học phần: LÝ THUYẾT MẬT MÃ

Số tín chỉ: 2

Học kỳ: 4

Học phần: Bắt buộc

Các học phần tiên quyết: CTDL&GT, Toán rời rạc, Lập trình trực quan

Các môn học kế tiếp: Các môn chuyên ngành

Giờ tín chỉ đối với các hoạt động:

Lý thuyết	BT&TL	Thực hành	Tự học
18	24	0	90

Địa chỉ bộ môn phụ trách học phần: BM KHMT, khoa CNTT&TT phòng 203 nhà A2 cơ sở 3 trường ĐH Hồng Đức.

3. Nội dung học phần:

Học phần trình bày về các vấn đề an toàn và bảo mật thông tin, bao gồm các phương pháp cổ điển cũng như hiện đại để giải quyết các vấn đề đó. Cụ thể học phần giới thiệu chung về các vấn đề an toàn và bảo mật thông tin hiện nay, cơ sở toán học của lý thuyết mật mã, các hệ mã hóa cổ điển, các hệ mã hóa khóa đối xứng, công khai thông dụng hiện nay. Học phần cũng giới thiệu các hàm băm và hệ chữ ký điện tử thông dụng hiện nay, các sơ đồ xưng danh và xác nhận danh tính

4. Mục tiêu của học phần:

Mục tiêu		**Mô tả**	**Chuẩn đầu ra CTĐT**
1. Kiến thức	**1.1**	Nắm được kiến thức chung về các vấn đề an toàn và bảo mật thông tin và cơ sở toán học của lý thuyết mật mã	C13
	1.2	Nắm vững các các hệ mã hóa cổ điển, các hệ mã hóa khóa đối xứng, công khai thông dụng hiện nay	C13

	1.3	Nắm vững các hàm băm và hệ chữ ký điện tử thông dụng hiện nay, các sơ đồ xưng danh và xác nhận danh tính	C13
2. Kỹ năng	**2.1**	Có khả năng vận dụng (cài đặt mới hay dùng từ một thư viện có sẵn) một hệ mã hóa phù hợp nào đó (đối xứng hoặc công khai) để đảm bảo an toàn thông tin cho một hệ thống cụ thể	C14, C18
	2.2	Có khả năng vận dụng hàm băm (cài đặt mới hoặc dùng từ thư viện có sẵn) cho một ứng dụng cụ thể; Có khả năng vận dụng (cài đặt mới hoặc dùng từ thư viện có sẵn) chữ ký điện tử, sơ đồ xưng danh và xác nhận danh tính vào một ứng dụng cụ thể, ví dụ như ứng dụng chứng thực chữ ký số	C14, C18
	2.3	Có khả năng đánh giá mức an toàn của một hệ thống trong thực tế đang dùng kỹ thuật mã hóa, chữ ký điện tử để từ đó chọn được một giải pháp phù hợp để cài đặt	C14, C18
3. Thái độ và năng lực	**3.1**	Biết được vị trí và vai trò của môn học trong chương trình cũng như ứng dụng thực tế của môn học, trên cơ sở đó kích thích niềm say mê nghiên cứu tin học của người học và học tốt các môn học kế tiếp. Tích cực trao đổi, hợp tác và làm việc nhóm hiệu quả. Không ngừng rèn luyện, tìm tòi, học hỏi kiến thức mới từ tài liệu, mạng Internet và các thành viên trong nhóm, trong lớp.	C22, C23
	3.2	Phát huy, rèn luyện khả năng làm việc sáng tạo, độc lập, cần cù, chính xác cũng như hình thành các kỹ năng riêng cho bản thân khi giải quyết các vấn đề của môn lý thuyết mật mã, những vấn đề mô phỏng những vấn đề thực tế có thể gặp trong thực tế. Rèn luyện tư duy hệ thống và phát huy sự hợp tác nhóm của sinh viên	C22, C23
	3.3	Có năng lực trong việc áp dụng các giải pháp an toàn bảo mật thông tin cho các ứng dụng cụ thể; Có năng lực trong việc tiếp tục nghiên cứu chuyên sâu hơn nữa về lĩnh vực an toàn bảo mật thông tin	C21, C22

5. Chuẩn đầu ra của học phần

TT	Kết quả mong muốn đạt được	Mục tiêu	Chuẩn đầu ra CTĐT
A	Hiểu rõ về các vấn đề an toàn và bảo mật thông tin và cơ sở toán	1.1	C13

	học của lý thuyết mật mã		
B	Hiểu rõ và vận dụng cài đặt được các hệ mã hóa khóa đối xứng, các hệ mã hóa khóa công khai thông dụng hiện nay để tăng cường an ninh cho các hệ thống phần mềm cụ thể	1.2, 2.1	C13, C14, C18
C	Hiểu rõ và vận dụng cài đặt được các hệ chữ ký điện tử, hàm băm, sơ đồ xưng danh và xác nhận danh tính thông dụng hiện nay vào các hệ thống phần mềm cụ thể, ví dụ như ứng dụng chứng thực số	1.3, 2.2	C13, C14, C18
D	Khả năng vận dụng môn học để đánh giá và giải quyết các bài toán trong thực tế	3, 2.3	C14,C18,C21,C22,C23

6. Nội dung chi tiết học phần:

CHƯƠNG 1: GIỚI THIỆU VỀ AN TOÀN VÀ BẢO MẬT THÔNG TIN

1.1. Giới thiệu chung

1.2. Các bài toán về an toàn và bảo mật thông tin

1.2.1. Các phương pháp cổ điển

1.2.2. Các phương pháp dùng mật mã hiện đại ngày nay

1.2.3. Một số đánh giá và hướng phát triển

1.3. Tấn công chọn trước bản rõ, bản mã – CPA, CCA

1.4. Một số cơ sở toán học của lý thuyết mật mã hiện đại

1.5. Bài tập

CHƯƠNG 2. CÁC HỆ MÃ HÓA KHÓA ĐỐI XỨNG CƠ BẢN

2.1. Một số hệ mã hóa khóa đối xứng cổ điển

2.1.1. Mô hình tổng quát của hệ mã hóa khóa đối xứng

2.1.2. Mã chuyển dịch

2.1.3. Mã thay thế

2.1.4. Mã Vigenère

4.1.4. Một số hệ chữ ký điện tử mới hiện nay

4.2. Hàm băm

4.2.1. Định nghĩa

4.2.2. Giới thiệu hàm băm MD5 và họ hàm băm SHA

4.2.3. Một số ứng dụng của hàm băm

4.3. Bài toán xưng danh và xác nhận danh tính

4.4. Các sơ đồ xưng danh và xác nhận danh tính

4.5. Bài tập

7. Học liệu:

+ *Học liệu bắt buộc*

[1]. Phan Đình Diệu. Lý thuyết mật mã và An toàn thông tin. Đại học Quốc Gia Hà Nội. 2006.

+ *Học liệu tham khảo*

[2]. TS. Lê Văn Phùng. An Toàn Thông Tin. NXB Thông Tin và Truyền Thông, 2018.

8. Hình thức tổ chức dạy học

8.1. Lịch trình chung:

Nội dung	**Hình thức tổ chức dạy học môn học**				**KT đánh giá**
	LT	**BT - TL**	**TH**	**Tự học**	
CHƯƠNG 1: GIỚI THIỆU VỀ AN TOÀN VÀ BẢO MẬT THÔNG TIN	**1**	**1**		**4.5**	
1.1. Giới thiệu chung	0,25			1	
1.2. Các bài toán về an toàn và bảo mật thông tin 1.2.1. Các phương pháp cổ điển 1.2.2. Các phương pháp dùng mật mã hiện đại ngày nay 1.2.3. Một số đánh giá và hướng phát triển	0,5	1		1.5	

1.3. An toàn có chứng minh					
1.4. Một số cơ sở toán học của lý thuyết mật mã hiện đại	0,25			2	
CHƯƠNG 2: CÁC HỆ MÃ HÓA KHÓA ĐỐI XỨNG CƠ BẢN	**4**	**6**		**21**	
2.1. Một số hệ mã hóa khóa đối xứng cổ điển 2.1.1. Mô hình tổng quát của hệ mã hóa khóa đối xứng 2.1.2. Mã chuyển dịch 2.1.3. Mã thay thế 2.1.4. Mã Vigenère 2.1.5. Mã hoán vị	1	2		10	
2.2. Một số hệ mã hóa khóa đối xứng hiện đại 2.2.1. Hệ mật mã dòng A5/1 2.2.2. Hệ mật mã dòng RC4	3	4		11	
CHƯƠNG 3: CÁC HỆ MÃ HÓA KHÓA CÔNG KHAI	**6**	**10**		**33**	**1**
3.1. Giới thiệu chung 3.1.1. Tại sao lại cần hệ mã hóa khóa công khai? 3.1.2. Ý tưởng của Diffie Hellman và lược đồ xây dựng chung	1	1		5	
3.2. Một số thuật toán cơ bản 3.3. Hệ mã hóa RSA 3.3.1. Cơ sở toán học 3.3.2. Sơ đồ hệ mã RSA 3.3.3. Đánh giá an toàn và các mở rộng của RSA	2	3		10	
3.4. Hệ mã hóa Elgamal	2	3		10	

3.4.1. Cơ sở toán học 3.4.2. Sơ đồ hệ mã Elgamal 3.4.3. Đánh giá an toàn và các mở rộng của Elgamal					
3.5. Các hệ mã hóa khóa công khai hiện đại khác 3.6. Bài tập	1	1		8	
KT&ĐG giữa kỳ					1
CHƯƠNG 4: CHỮ KÝ ĐIỆN TỬ VÀ HÀM BĂM	**7**	**12**		**26**	**1**
4.1. Chữ ký điện tử 4.1.1. Giới thiệu và định nghĩa 4.1.2. Hệ chữ ký điện tử RSA 4.1.2. Hệ chữ ký điện tử Elgamal 4.1.3. Chuẩn chữ ký điện tử DSS 4.1.4. Một số hệ chữ ký điện tử mới hiện nay	5	4		6	
4.2. Một số hệ chữ ký điện tử mới hiện nay		1		10	
4.3. Hàm băm 4.3.1. Định nghĩa 4.3.2. Giới thiệu hàm băm MD5 và họ hàm băm SHA 4.3.3. Một số ứng dụng của hàm băm	0,5	0,5		4.5	
5.4. Bài toán xưng danh và xác nhận danh tính 5.5. Bài tập	1,5	2,5		5	
KT&ĐG		1			
Tổng	**18**	**24**		**90**	

8.2. Lịch trình cụ thể cho từng nội dung:

Nội dung tuần 1 (LT+BT: 5 tiết)

Hình thức tổ chức dạy học	Thời gian địa điểm	Nội dung chính	Mục tiêu cụ thể	Yêu cầu người học chuẩn bị	Chuẩn đầu ra HP
Lý thuyết	3 giờ Phòng học	- Giới thiệu chung về an toàn và bảo mật thông tin đối với một hệ thống thông tin. - Giới thiệu các bài toán về an toàn và bảo mật thông tin, các phương pháp cổ điển để giải quyết vấn đề này, các phương pháp hiện đại để giải quyết vấn đề này. - Giới thiệu về an toàn có chứng minh - Giới thiệu các cơ sở toán học cho mật mã hiện đại. Tìm hiểu về một số phương pháp lập mã của các hệ mã hóa khóa đối xứng cổ điển - Tìm hiểu một số hệ mã hóa khóa đối xứng hiện đại sử dụng phương pháp mã hóa theo dòng bít như A5/1, RC4 *- Chia nhóm sinh viên làm bài tập lớn, mỗi nhóm từ 3-5 sinh viên làm một bài tập lớn*	- Biết được thế nào là an toàn bảo mật thông tin cho một hệ thống thông tin. - Biết được các bài toán về an toàn và bảo mật thông tin, các phương pháp cổ điển để giải quyết vấn đề này, các phương pháp hiện đại để giải quyết vấn đề này. - Biết được thế nào là an toàn có chứng minh, thế nào là mô hình an toàn cho các hệ, biết được thế nào là mô hình an toàn CPA, CCA - Biết được các loại assumptions trong mật mã hiện đại ngày nay, cách tự xây dựng các asumption. - Hiểu được các phương pháp cơ bản để chống xâm nhập trái phép vào một hệ thống thông tin. Hiểu được thế nào là một hệ mã hóa khóa đối xứng. - Hiểu được các phương pháp lập mã của một số hệ mã hóa khóa đối	Đọc tài liệu [1] (chương 1,2), và [2] học liệu tham khảo	A

		với chủ đề khác nhau. Tùy thuộc số lượng sinh viên của lớp để có số lượng bài tập lớn tương ứng.	xứng cổ điển nổi tiếng như mã chuyển dịch, mã thay thế, mã Vigenère, mã hoán vị - Nắm được phương pháp lập mã và giải mã của các thuật toán A5/1 và RC4. - Nắm được tư tưởng của các hệ mật mã khóa đối xứng hiện đại sử dụng phương pháp mã hóa theo dòng bít, biết được ưu nhược điểm của phương pháp này.		
BT-TL	2 giờ Phòng học	- Tìm hiểu về một số phương pháp lập mã của các hệ mã hóa khóa đối xứng cổ điển. - Thảo luận các hệ mã hóa khóa đối xứng hiện đại sử dụng phương pháp mã hóa theo dòng bít như A5/1.	- Hiểu được thế nào là một hệ mã hóa khóa đối xứng. - Hiểu được các phương pháp lập mã của một số hệ mã hóa khóa đối xứng cổ điển nổi tiếng như mã chuyển dịch, mã thay thế, mã Vigenère, mã hoán vị - Hiểu rõ phương pháp lập mã và giải mã của các thuật toán A5/1, phân tích ưu nhược điểm của nó.	Đọc tài liệu [1] (chương 1,2), và [2] học liệu tham khảo, Tài liệu internet tự tìm trên google với từ khóa là tên hệ mã.	A
Tự học	4.5 giờ Tại nhà/ thư viện/	- Những vấn đề về an toàn bảo mật thông tin của một hệ thống thông tin, các phương pháp đảm bảo an toàn bảo mật thông tin cơ	- Trình bày được các vấn đề cơ bản về an toàn thông tin của một hệ thống thông tin. - Có khả năng tự đánh	Đọc tài liệu [1] (chương 1,2), và [2] học liệu	

	KLF...	bản. Tìm hiểu sâu hơn các phương pháp này. - Tìm hiểu sâu hơn về các phương pháp tấn công, xâm nhập trái phép vào một hệ thống thông tin hiện nay. - Tìm hiểu thêm về các hệ mã hóa khóa đối xứng cổ điển khác. - Tìm hiểu sâu hơn về vấn đề an toàn có chứng minh, các mô hình anh toàn CPA, CCA	giá sơ bộ độ an toàn của một hệ thống thông tin và chỉ ra các biện pháp khắc phục cơ bản trong trường hợp hệ thống đó chưa an toàn. - Nắm vững các hệ mật mã khóa đối xứng cổ điển, lịch sử và các phương pháp phát triển của nó. - Nắm được thế nào là vấn đề an toàn có chứng minh, nắm được các mô hình an toàn như CPA, CCA.	tham khảo, Tài liệu internet tự tìm trên google với từ khóa là tên hệ mã.	
Tư vấn	VPK CNTT &TT	- Tài liệu và phương pháp học tập môn học. - Cách tìm tài liệu trên internet	- Chuẩn bị được các tài liệu phục vụ môn học, có phương pháp học tốt về môn học.	Câu hỏi vướng mắc	

Nội dung tuần 2 (LT+BT: 5 tiết)

Hình thức tổ chức dạy học	Thời gian địa điểm	Nội dung chính	Mục tiêu cụ thể	Yêu cầu người học chuẩn bị	Chuẩn đầu ra HP
Lý thuyết	2 giờ Phòng học	- Thảo luận các hệ mã hóa khóa đối xứng hiện đại sử dụng phương pháp mã hóa theo dòng bít RC4.	- Hiểu được các kiến thức toán học cơ bản phục vụ cho việc lập mã giải mã của các hệ mã hóa hiện đại. - Hiểu được lịch sử của chuẩn mã hóa khóa đối	Đọc tài liệu [1] (chương 2,3), và [2] học liệu tham	B

			xứng. Hiểu được công dụng của chuẩn mã hóa khóa đối xứng. - Hiểu được các bước lập mã và giải mã của hệ RC4	khảo	
BT-TL	3 giờ Phòng học	- Cách lập mã giải mã của hệ A5/1 - Cách lập mã giải mã của hệ RC4. - Cách lập mã giải mã của các hệ mã hóa cổ điển.	- Thành thạo các phương pháp lập mã, giải mã của hệ A5/1. - Thành thạo các phương pháp lập mã, giải mã của hệ RC4. - Thành thạo các phương pháp lập mã, giải mã của các hệ mã hóa cổ điển.	Đọc tài liệu [1] (chương 2,3), và [2] học liệu tham khảo, tài liệu internet tự tìm trên google với từ khóa là tên hệ mã.	B
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu các hệ mật mã khóa đối xứng hiện đại sử dụng phương pháp mã hóa theo dòng bít khác, phân tích ưu nhược điểm của phương pháp này. - Tìm hiểu sâu hơn về các biến thể của A5/1, RC4 hiện nay - Tìm hiểu các ứng dụng cụ thể nổi tiếng nhất của các hệ hày	- Nắm được các hệ mật mã khóa đối xứng hiện đại sử dụng phương pháp mã hóa theo dòng bít, phân tích ưu nhược điểm của các hệ mật này. - Nắm được các biến thể của A5/1, RC4 hiện nay. - Nắm được các ứng dụng cụ thể nổi tiếng nhất của các hệ hày trong thực tế	Đọc tài liệu [1] (chương 2,3), và [2] học liệu tham khảo, tài liệu internet tự tìm trên google với từ khóa là	B

		trong thực tế		tên hệ mã.	
Tư vấn	VPK CNTT &TT	- Tài liệu và phương pháp đọc tài liệu. - Cách tìm tài liệu trên internet	- Nắm được cơ bản các bước để có thể tự đọc được tài liệu môn học. - Cách để tìm tài liệu môn học trên mạng	Câu hỏi vướng mắc	

Nội dung tuần 3 (LT+BT: 5 tiết)

Hình thức tổ chức dạy học	Thời gian địa điểm	Nội dung chính	Mục tiêu cụ thể	Yêu cầu người học chuẩn bị	Chuẩn đầu ra HP
Lý thuyết	1 giờ Phòng học	- Cách cài đặt hai hệ A5/1 và RC4 - Các thư viện hỗ trợ	.- Sinh viên hiểu được cách cài đặt hại hệ A5/1 và RC4. Sinh viên nắm được thư viện hỗ trợ cài đặt hai hệ mã hóa này: shoup.net/ntl/	Đọc tài liệu [1] (chương 3 và [2] học liệu tham khảo	B
BT-TL	4 giờ phòng học	- Thảo luận về cài đặt A5/1 và RC4	- Sinh viên biết được cách cài đặt hại hệ A5/1 và RC4. Sinh viên nắm được thư viện hỗ trợ cài đặt hai hệ mã hóa này: shoup.net/ntl/	Đọc tài liệu [1] (chương 2), và [2] học liệu tham khảo, tài liệu internet tự tìm trên google với từ khóa là tên hệ	B

				mã.	
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Cách lập mã giải mã của các hệ mã hóa cổ điển khác. - Cách lập mã giải mã của các hệ mã hóa theo dòng bít khác.	-.Thành thạo các phương pháp giải mã, lập mã của các hệ mã hóa cổ điển và các hệ mã hóa theo dòng bít.	Đọc tài liệu [1] (chương 2) và [2] học liệu tham khảo, tài liệu internet tự tìm trên google với từ khóa là tên hệ mã.	B
Tư vấn	VPK CNTT &TT	- Cách đọc tài liệu	- Biết cách đọc tài liệu hiệu quả	Câu hỏi vướng mắc	

Nội dung tuần 4 (LT+BT: 5 tiết)

Hình thức tổ chức dạy học	**Thời gian địa điểm**	**Nội dung chính**	**Mục tiêu cụ thể**	**Yêu cầu người học chuẩn bị**	**Chuẩn đầu ra HP**
Lý thuyết	2 giờ Phòng học	- Giới thiệu chung về mã hóa khóa công khai, tại sao lại cần hệ mã hóa khóa công khai? - Ý tưởng của Diffie Hellman và lược đồ xây dựng chung. - Một số thuật toán cơ bản	- Nắm được tại sao lại cần phải có hệ mã hóa khóa công khai. - Hiểu được ý tưởng của Diffie Hellman để xây dựng lược đồ chung cho một hệ mã hóa khóa công khai. - Nắm được một số thuật toán cơ bản như thuật	Đọc tài liệu [1] (chương 3), và [2] học liệu tham khảo. Tài liệu internet tự tìm	B

		- Cơ sở toán học của hệ mã hóa RSA.	toán lũy thừa nhanh, thuật toán tìm số nguyên tố, Euclid mở rộng. - Hiểu được cơ sở toán học của hệ mã hóa RSA.	trên google với từ khóa là tên hệ mã.	
BT-TL	3 giờ Phòng học	- Một số thuật toán cơ bản - Cơ sở toán học của hệ mã hóa RSA.	Thành thạo các thuật toán cơ bản như lũy thừa nhanh, tìm số nguyên tố, tìm số nghịc đảo.	Đọc tài liệu [1] (chương 4), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google với từ khóa là tên hệ mã.	B
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Các kiến thức toán học về số học modulo, nhóm, vành, trường, ma trận, độ phức tạp tính toán. - Tìm hiểu lịch sử chuẩn mã hóa khóa đối xứng. Chuẩn mã hóa khóa đối xứng DES. - Tìm hiểu về lịch sử của khóa công khai để hiểu tại sao nó lại là điểm xuất phát của mã hóa hiện đại ngày	- Nắm vững về các kiến thức toán học, thành thạo các phép biến đổi, làm tốt bài tập liên quan. - Tìm hiểu về chuẩn mã hóa khóa đối xứng DES, tại sao DES bị thay thế bởi AES. - Nắm được tầm quan trọng của mã hóa khóa công khai	Đọc tài liệu [1] (chương 3,4), và [2] học liệu tham khảo. Tài liệu internet	B

		nay			
Tư vấn	VPK CNTT &TT	- Giải đáp vướng mắc khi tìm hiểu về lịch sử chuẩn mã hóa khóa đối xứng. Chuẩn mã hóa khóa đối xứng DES, mã hóa khóa công khai	- Nắm được chuẩn mã hóa khóa đối xứng DES. Hiểu được vì sao DES bị thay thế bởi AES. Nắm được tầm quan trọng của mã hóa khóa công khai	Các câu hỏi cần giải đáp	

Nội dung tuần 5 (LT+BT: 5 tiết)

Hình thức tổ chức dạy học	**Thời gian địa điểm**	**Nội dung chính**	**Mục tiêu cụ thể**	**Yêu cầu người học chuẩn bị**	**Chuẩn đầu ra HP**
Lý thuyết	2 giờ Phòng học	- Các bước lập mã của hệ RSA. - Giới thiệu về cơ sở toán học của hệ mã hóa Elgamal. Các assumptions xuất phát từ bài toán khó logarit rời rạc. - Hệ mã hóa Elgamal.	- Nắm được các bước lập mã giải mã của hệ RSA. - Nắm được các assumptions xuất phát từ bài toán khó logarit rời rạc. - Nắm được cơ sở toán học và các bước lập mã, giải mã của hệ mã hóa Elgamal.	Đọc tài liệu [1] (chương 4), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google với từ khóa là tên hệ mã.	B
BT-TL	2 giờ Phòng học	- Phân tích, thảo luận từng bước lập mã của hệ RSA. - Đánh giá độ an toàn của hệ RSA và thảo	- Nắm vững được các bước lập mã và giải mã của RSA. - Có cái nhìn tổng quan về độ an toàn của RSA	Đọc tài liệu [1] (chương 4), và [2] học liệu	B

		luận các phương pháp phòng tránh cũng như các biến thể của hệ RSA. - Phân tích, thảo luận từng bước lập mã của hệ Elgamal. - Đánh giá độ an toàn của hệ Elgamal và thảo luận các phương pháp phòng tránh cũng như các biến thể của hệ Elgamal.	và các phương pháp biến đổi để RSA đạt an toàn cao hơn. - Nắm vững được các bước lập mã và giải mã của Elgamal. - Có cái nhìn tổng quan về độ an toàn của Elgamal và các phương pháp biến đổi để Elgamal đạt an toàn cao hơn. - Nắm được một số thư viện hỗ trợ cài đặt hai hệ này dùng trường số nguyên cũng như đường cong eliptics: openssl.org/ và shoup.net/ntl/	tham khảo. Tài liệu internet tự tìm trên google với từ khóa là tên hệ mã.	
KT&ĐG giữa kỳ	1 giờ phòng học	Kiểm tra về hoặc hệ mã hóa RSA hoặc Elgamal	Thành thạo kỹ năng lập mã, giải mã đối với các hệ RSA, Elgamal	Giấy làm bài	B
Tự học	12.5 giờ Tại nhà/ thư viện/ KLF...	- Ôn luyện lại các bước lập mã của hệ AES - Tìm hiểu các biến thể của hệ AES hiện nay, trả lời câu hỏi tại sao lại phải có các biến thể này? - Tìm hiểu về các vấn đề an toàn của hệ RSA - Các giải thuật để tấn công RSA hiện nay, và cách chọn tham số của hệ để nó đạt được	- Thành thạo các bước lập mã của hệ mã AES. - Hiểu được các loại biến thể hiện nay của hệ AES, và lý do tại sao lại sinh ra các biến thể này - Biết được một số loại tấn công hiện nay trên hệ RSA - Biết được cách thiết lập tham số cho hệ RSA để nó đảm bảo được an toàn.	Đọc tài liệu [1] (chương 4), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google với từ khóa là	B

		an toàn - Các thư viện cài đặt RSA	- Nắm được việc cài đặt RSA	tên hệ mã.	
Tư vấn	VPK CNTT &TT	- Tìm hiểu về các các biến thể của hệ AES hiện nay - Tìm hiểu về các tấn công trên hệ RSA, cách thiết lập tham số an toàn	- Hiểu được các loại biến thể hiện nay của hệ AES - Hiểu được các tấn công trên RSA và cách thiết lập tham số an toàn - Nắm được các thư viện hỗ trợ cài đặt shoup.net/ntl/	Các câu hỏi cần giải đáp	

Nội dung tuần 6 (LT+BT: 5 tiết)

Hình thức tổ chức dạy học	**Thời gian địa điểm**	**Nội dung chính**	**Mục tiêu cụ thể**	**Yêu cầu người học chuẩn bị**	**Chuẩn đầu ra HP**
Lý thuyết	3 giờ phòng học	- Giới thiệu và định nghĩa chữ ký điện tử. - Hệ chữ ký điện tử RSA - Hệ chữ ký điện tử Elgamal	- Hiểu được thế nào là một chữ ký điện tử, vai trò của nó trong thực tế. - Nắm được các bước thiết lập một chữ ký điện tử theo sơ đồ RSA. Độ an toàn khi ký bằng sơ đồ này. - Nắm được các bước thiết lập một chữ ký điện tử theo sơ đồ Elgamal. Độ an toàn khi ký bằng sơ đồ này.	Đọc tài liệu [1] (chương 5), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google với từ khóa là tên hệ chữ ký.	C

BT-TL	2 giờ Phòng học	- Tìm hiểu các hệ mã hóa khóa công khai mới nhất hiện nay như hệ mã hóa khóa công khai Cramer-shoup, ….	- Biết được tổng quan các hệ mã hóa khóa công khai mới nhất hiện nay. Ưu nhược điểm của một số hệ quan trọng nhất, xu hướng phát triển trong tương lai.	Đọc tài liệu [1] (chương 5), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google với từ khóa là tên hệ mã.	C
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu về các vấn đề an toàn của hệ mã Elgamal - Các giải thuật để tấn công hệ mã Elgamal hiện nay, và cách chọn tham số của hệ để nó đạt được an toàn - Các thư viện cài đặt hệ mã Elgamal	- Nắm được một số loại tấn công hiện nay trên hệ Elgamal - Nắm được cách thiết lập tham số cho hệ Elgamal để nó đảm bảo được an toàn. - Nắm được các thư viện hỗ trợ cài đặt Elgamal: openssl.org/; shoup.net/ntl/; wolfssl.com/wolfSSL	Đọc tài liệu [1] (chương 5) và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google với từ khóa là tên hệ mã.	C
Tư vấn	VPK CNTT &TT	- Một số vấn đề vướng mắc khi tìm hiểu các thư viện cài đặt.	- Hiểu rõ về các thư viện cài đặt.	Các câu hỏi cần giải đáp	

Nội dung tuần 7 (LT+BT: 5 tiết)

Hình thức tổ chức dạy học	Thời gian địa điểm	Nội dung chính	Mục tiêu cụ thể	Yêu cầu người học chuẩn bị	Chuẩn đầu ra HP
Lý thuyết	3 giờ Phòng học	- Chuẩn chữ ký điện tử DSS - Hàm băm - Bài toán xưng danh và xác nhận danh tính	- Nắm được chuẩn chữ ký điện tử DSS, hiểu được DSS được phát triển tử Elgamal như thế nào. - Hiểu được thế nào là hàm băm, có những loại hàm băm nào, ứng dụng của hàm băm trong thực tế. - Nắm được sơ đồ xưng danh Schnor.	Đọc tài liệu [1] (chương 5) và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google với từ khóa là tên hệ chữ ký, sơ đồ xưng danh	C
BT-TL	2 giờ Phòng học	- Thảo luận về giải thuật chữ ký tổng quát RSA - Cách cài đặt cụ thể của hệ chữ ký này dựa trên trường số nguyên.	- Biết được cụ thể phương pháp cài đặt hệ chữ ký RSA dựa trên trường số nguyên - Nắm được một số thư viện hiện có trên thế giới giúp cài đặt hệ chữ ký này: shoup.net/ntl/;	Đọc tài liệu [1] (chương 5), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	C

				với từ khóa là tên hệ chữ ký.	
Tự học	12 giờ Tại nhà/ thư viện/ KLF...	- Tiếp tục tìm hiểu các thư viện cài đặt hệ chữ ký RSA, Elgamal	- Nắm vững các thư viện này: openssl.org/; shoup.net/ntl/; wolfssl.com/wolfSSL	Đọc tài liệu [1] (chương 5), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google với từ khóa là tên hệ chữ ký.	C
Tư vấn	VPK CNTT &TT	- Các vấn đề vướng mắc khi cài đặt	- Thành thạo việc dùng thư viện cài đặt	Các câu hỏi cần giải đáp	

Nội dung tuần 8 (LT+BT+KTĐG: 5 tiết)

Hình thức tổ chức dạy học	Thời gian địa điểm	Nội dung chính	Mục tiêu cụ thể	Yêu cầu người học chuẩn bị	Chuẩn đầu ra HP
BT-TL	4 giờ Phòng học	- Thảo luận về giải thuật chữ ký tổng quát Elgamal - Các cài đặt cụ thể của hệ chữ ký này dựa trên trường số	- Biết được cụ thể phương pháp cài đặt hệ mã RSA dựa trên trường số nguyên - Nắm được một số thư viện hiện có trên thế	Đọc tài liệu [1] (chương 5), và [2] học liệu tham	C

		nguyên và đường cong eliptics	giới giúp cài đặt hệ mã hóa này	khảo. Tài liệu internet tự tìm trên google với từ khóa là tên hệ chữ ký.	
KT&ĐG	1 giờ phòng học	Kiểm tra về hoặc hệ chữ ký RSA, hoặc Elgamal, hoặc DSS	Thành thạo kỹ năng tạo chữ ký, kiểm tra chữ ký với các hệ chữ ký RSA, Elgamal, DSS	Giấy làm bài	C
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu các thư viện cài đặt hệ chữ ký RSA, Elgamal	- Biết được tổng quan về độ an toàn của Elgamal và các phương pháp biến đổi để Elgamal đạt an toàn cao hơn - Nắm vững các thư viện này.	Đọc tài liệu [1] (chương 5), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google với từ khóa là tên hệ chữ ký.	C
Tư vấn	VPK CNTT &TT	- Các vấn đề vướng mắc khi cài đặt	- Thành thạo việc dùng thư viện cài đặt	Các câu hỏi cần giải đáp	

Nội dung tuần 9 (LT+BT: 5 tiết)

Hình thức tổ chức dạy học	Thời gian địa điểm	Nội dung chính	Mục tiêu cụ thể	Yêu cầu người học chuẩn bị	Chuẩn đầu ra HP
Lý thuyết	2 giờ phòng học	- Một số hệ chữ ký điện tử mới hiện nay - Các sơ đồ xưng danh	- Biết được một số hệ chữ ký mới hiện nay dựa trên Parings như Boneh-Boyen, dựa trên đường cong elliptic như ECDSA, ưu nhược điểm của các hệ chữ ký này so với các hệ chữ ký RSA, Elgamal - Nắm được sơ đồ xưng danh Schnnor, Okamoto	Đọc tài liệu [1] (chương 6) và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google với từ khóa là ECDSA, Boneh-Boyen Signature	C
BT-TL & KTĐG	3 giờ phòng học	. - Ứng dụng của các sơ đồ xưng danh trong các hệ khác cũng như trong thực tế. - Một số hệ chữ ký điện tử mới hiện nay - Bảo vệ bài tập lớn	- Nắm được về vấn đề sơ đồ xưng danh. - Nắm được ứng dụng của loại sơ đồ này - Nắm được xu hướng phát triển của loại sơ đồ này hiện nay. - Biết được một số hệ chữ ký mới hiện nay, ưu nhược điểm của chúng so với các hệ chữ ký RSA, Elgamal, DSS - Một số thư viện hỗ trợ cài đặt loại sơ đồ	Đọc tài liệu [1] (chương 6) và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google với từ khóa là tên sơ đồ xưng	C, D

			này	danh.	
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu sâu hơn về các hệ mã hóa, chữ ký khóa công khai mới nhất hiện nay như hệ mã hóa, chữ ký khóa công khai dựa trên định danh Identity-based Encryption, Signature, Cramer-shoup. - Tìm hiểu sâu hơn về các sơ đồ xưng danh	- Hiểu được các hệ này có ưu nhược điểm gì, so sánh với các hệ RSA và Elgamal thông thường. - Hiểu được sơ đồ xưng danh có những ứng dụng gì trong thực tế	Đọc tài liệu [1] (chương 6) và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google với từ khóa là tên hệ mã, tên hệ chữ ký, tên sơ đồ xưng danh.	C
Tư vấn	VPK CNTT &TT	- Các vấn đề vướng mắc khi tìm hiểu về các hệ mã hóa, chữ ký khóa công khai mới nhất hiện nay, sơ đồ xưng danh	- Nắm vững các hệ mã hóa, chữ ký khóa công khai mới nhất hiện nay. Ưu nhược điểm của một số hệ quan trọng nhất, xu hướng phát triển trong tương lai. - Nắm vững hai sơ đồ xưng danh thông dụng hiện nay là Schnnor và Okamoto	Các câu hỏi cần giải đáp	

9. Chính sách đối với phần học

Yêu cầu đối với người học:

- Người học phải đầy đủ tư liệu để tự nghiên cứu và chuẩn bị bài trước khi đến lớp tối thiểu là bài giảng của giảng viên.

- Hiện diện trên lớp theo quy định (không nghỉ quá 20% tổng số giờ TC).

- Người học phải tham gia đầy đủ các bài kiểm tra - đánh giá định kỳ trong quá trình học, làm bài tập lớn, và bài kiểm tra kết thúc học phần.

10. Phương pháp, hình thức kiểm tra - đánh giá kết quả học tập học phần

10.1. Tiêu chí kiểm tra, đánh giá

Với các bài tập lớn: các nhóm phải thực hiện phân công thành viên thực hiện bài tập lớn một cách khoa học, hiệu quả, thực hiện đúng và đầy đủ các yêu cầu của các bài tập lớn là chương trình cài đặt phải chạy được, giao diện đẹp, đầy đủ chức năng của một hệ mã hóa/chữ ký điện tử/sơ đồ xưng danh. Mỗi nhóm phải nộp báo cáo quyển đi kèm với chương trình cài đặt.

Với bài kiểm tra: sinh viên phải theo dõi bài trên lớp, hiểu và vận dụng kiến thức, kỹ năng được trang bị từ bài giảng để làm các bài tập thực hành

10.2. Kiểm tra- đánh giá thường xuyên:.

- Trong các buổi học thường xuyên đánh giá quá trình học tập, tự học của người học.
- Chia sinh viên trong lớp thành các nhóm từ 3-5 sinh viên một nhóm, mỗi nhóm làm một bài tập lớn khác nhau. Báo cáo nhóm (bài tập lớn) trong thời gian 5-10 phút/báo cáo. Điểm trung bình của bài tập lớn và bài kiểm tra quá trình có trọng số 0,3.

10.3. Kiểm tra – đánh giá giữa kỳ:

- Kiểm tra - đánh giá giữa kì: 1 bài thi viết 50 phút

- Điểm của bài kiểm tra giữa kỳ có trọng số 0,2

10.4. Kiểm tra – đánh giá cuối kì:

- Hình thức: Thi viết 90 phút. Thời gian: phòng Đào tạo xếp. Địa điểm: khoa CNTT&TT. Trọng số: 0,5

11. Các yêu cầu khác:

- Bố trí lịch học, thời gian học theo đúng lịch trình cụ thể.

Ngày Khoa duyệt		Ngày xây dựng ĐCCT
Ngày tháng năm 2019		*Ngày tháng năm 2019*
TRƯỞNG KHOA	P.TRƯỞNG BỘ MÔN	GIẢNG VIÊN
Phạm Thế Anh	**Trịnh Thị Phú**	**Trịnh Viết Cường**