TRƯỜNG ĐẠI HỌC HỒNG ĐỨC **Khoa CNTT&TT** **Bộ môn Khoa học máy tính**	**ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN:** **TÍNH TOÁN AN TOÀN** **MÃ HỌC PHẦN : 173044**

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: khoa CNTT&TT.	Các ngày trong tuần từ thứ 2 đến thứ 6, tại
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: TÍNH TOÁN AN TOÀN

Số tín chỉ: 3

Học kỳ: 7

Học phần: Tự chọn

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
25	40	0	135

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 cung cấp cho học viên những kiến thức cơ bản và mới nhất về các lĩnh vực: kỹ thuật mã hóa để đảm bảo an toàn cho các giao dịch từ smartphone, cũng như kỹ thuật mã hóa dùng để đảm bảo an toàn dữ liệu, xử lý dữ liệu trên điện toán đám mây. Cụ thể các kỹ thuật như attribute-based encryption, homomorphic encryption, garbled circuit, functional encryption

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	Tổng quan về mật mã hiện đại ngày nay. Nắm vững, có cái nhìn tổng quan về các kỹ thuật mã hóa dùng cho di động, xu hướng phát triển của nó trong tương lai	C13
	1.3	Nắm vững, có cái nhìn một cách tổng quan các kỹ thuật mã hóa mới nhất dùng cho điện toán đám mây hiện nay như kỹ thuật attribute-based encryption, homomorphic encryption, garbled circuit, functional encryption. Xu hướng phát triển của nó trong tương lai. Hiểu rõ về mức độ an toàn và một số loại tấn công thông dụng trên các hệ mã hóa này	C13
2. Kỹ năng	**2.1**	Có khả năng đánh giá các kỹ thuật mã hóa dùng trong di động, điện toán đám mây, Có khả năng vận dụng (cài đặt mới hoặc dùng từ thư viện có sẵn) được nó vào trong thực tế	C14, C18
	2.2	Biết vận dụng kiến thức đã học để chọn lựa, thiết kế một kỹ thuật mã hóa phù hợp với yêu cầu bài toán trong thực tế, cụ thể là cho các ứng dụng dùng điện toán đám mây hay trên nền tảng di động. Có khả năng hiểu biết để cài đặt cụ thể kỹ thuật đó dựa trên các thư viện mở có sẵn	C14, C18
	2.3	Có khả năng đánh giá mức an toàn cho một hệ thống trong thực tế để từ đó chọn được, đưa ra tư vấn về một hệ mã hóa 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	C22,

		cù, chính xác cũng như hình thành các kỹ năng riêng cho bản thân khi giải quyết các vấn đề của môn tính toán an toàn, 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	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 tính toán an toàn	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 học của lý thuyết mật mã	1.1	C13
B	Hiểu rõ và vận dụng cài đặt được các hệ attribute-based encryption, functional encryption 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 homomorphic encryption, garbled circuit, thông dụng hiện nay vào các hệ thống phần mềm cụ thể	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: TỔNG QUAN VỀ LÝ THUYẾT MẬT MÃ

1.1. Giới thiệu về lý thuyết mật mã

1.2. Cơ sở toán học của lý thuyết mật mã

1.2.1. Dựa trên số nguyên

1.2.2. Dựa trên đường cong Elliptic

1.3. Một số hệ mã cổ điển, khóa bí mật, khóa công khai

1.4. Chữ ký điện tử

CHƯƠNG 2: ĐIỆN TOÁN ĐÁM MÂY VÀ MÃ HÓA THUỘC TÍNH

2.1. Điện toán đám mây

2.1.1. Giới thiệu

2.1.2. Các loại kỹ thuật mã hóa được dùng cho điện toán đám mây

2.2. Mã hóa dựa trên thuộc tính (Attribute-based Encryption)

2.2.1. Giới thiệu

2.2.2. Các loại access policies và efficiency

2.2.3. Linear secret sharing matrix

2.3. Hệ mã hóa dựa trên thuộc tính của Waters

2.3.1. Construction

2.3.2. Đánh giá

2.3.3. Cải tiến của hệ mã hóa dựa trên thuộc tính của Waters.

2.3.4. Đánh giá và hướng phát triển

CHƯƠNG 3: ĐIỆN TOÁN ĐÁM MÂY VÀ KỸ THUẬT HOMOMORPHIC ENCRYPTION

3.1. Giới thiệu về Homomorphic Encryption

3.1.1. Giới thiệu tổng quan

3.1.2. Các công cụ xây dựng và xu hướng phát triển

3.2. Additive Homomorphic Encryption

3.2.1. Giới thiệu

3.2.2. Construction

3.2.3. Đánh giá

3.3. Multiplicative Homomorphic Encryption

3.3.1. Giới thiệu

3.3.2. Construction

3.3.3. Đánh giá

CHƯƠNG 4: AN TOÀN TÍNH TOÁN

4.1. Garbled Circuit

4.1.1. Tại sao cần Garbled Circuit?

4.1.2. Ứng dụng

4.1.3. Xu hướng phát triển

4.2. Yao’s Circuit

4.2.1. Giới thiệu

4.2.2. Protocol và Security

4.2.3. Đánh giá và các ứng dụng sang primitives khác

4.3. Các cải tiến của Yao’s Circuit

4.3.1. Free XOR

4.3.2. Two halfs make a whole

4.3.3. Đánh giá và xu hướng phát triển

CHƯƠNG 5: OUTSOURCING COMPUTATION

5.1. Tại sao cần Outsourcing Computation

5.1.1. Giới thiệu và ứng dụng

5.1.2. Đánh giá và xu hướng phát triển

5.2. Randomize Encoding

5.2.1. Giới thiệu

5.2.2. A simple construction

5.2.2. Full construction

5.3. Functional Encryption

5.3.1. Giới thiệu

5.3.2. Hệ GVW12

5.3.3. Đánh giá và xu hướng phát triển

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 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	2 giờ Phòng	- Giới thiệu chung về an toàn và bảo mật thông tin đối với một hệ thống	- Biết được thế nào là an toàn bảo mật thông tin cho một hệ thống	Đọc tài liệu [1] (chương	A, B

	học	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 một số hệ mã hóa khóa đối xứng hiện đại sử dụng phương pháp mã hóa theo dòng bít như A5/1, RC4 với chuẩn mã hóa Block Cipher Mode - *Chia nhóm sinh viên làm bài tập lớn, mỗi nhóm từ 3-5 sinh viên làm một bài tập lớn với chủ đề khác nhau. Tùy thuộc số lượng sinh viên của lớp để có số lượng bài tập lớn tương ứng*.	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. - Nắm được phương pháp lập mã và giải mã của các thuật toán A5/1 và RC4 theo chuẩn mã hóa Block Cipher Mode	1,2), và [2] học liệu tham khảo	

			- 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	3 giờ Phòng học	- Thảo luận các hệ mã hóa khóa đối xứng hiện đại sử dụng phương pháp mã hóa theo dòng bít như A5/1, RC4 theo chuẩn Block cipher Mode	- Hiểu được thế nào là một hệ mã hóa khóa đối xứng. - Hiểu rõ phương pháp lập mã và giải mã của các thuật toán A5/1, RC4 theo chuẩn Block cipher Mode, 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.	B
Tự học	4.5 giờ Tại nhà/ thư viện/ KLF...	- 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 bản. Tìm hiểu sâu hơn các phương pháp này. - Tìm hiểu sâu hơn về các phương pháp tấn công, xâm nhập trái	- Trình bày được các vấn đề cơ bản về an toàn thông tin của một hệ thống thông tin. - Có khả năng tự đánh 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	Đọc tài liệu [1] (chương 1,2), và [2] học liệu tham khảo, Tài liệu internet tự tìm trên	A, B

		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	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.	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	- Giới thiệu điện toán đám mây. - Các loại kỹ thuật mã hóa được dùng cho điện toán đám mây - Giới thiệu mã hóa dựa trên thuộc tính (Attribute-based Encryption). - Các loại access policies và efficiency	- Nắm được thế nào là điện toán đám mây. - Nắm được tổng quan các loại kỹ thuật mã hóa có thể được áp dụng cho điện toán đám mây hiện nay. - Nắm được thế nào là mã hóa dựa trên thuộc tính. - Nắm được thế nào là	Đọc tài liệu [1] (chương 3), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google với từ	B

		- Linear secret sharing matrix	access policy trong mã hóa thuộc tính, đánh giá được chức năng, tính hiệu quả của từng loại. - Nắm được thế nào là Linear secret sharing, ứng dụng của nó trong xây dựng access policy.	khóa là tên hệ mã.	
BT-TL	3 giờ Phòng học	- Bài tập về cách tạo khóa, lập mã, giải mã của các hệ mã hóa khóa công khai RSA, Elgamal. - Bài tập về cách tạo khóa, chữ ký, kiểm tra chữ ký của các hệ chữ ký điện tử RSA,Elgamal, DSS.	- Thành thạo các cách tạo khóa, lập mã, giải mã của các hệ mã hóa khóa công khai RSA, Elgamal. Các hệ chữ ký điện tử RSA,Elgamal, DSS	Đọc tài liệu [1] (chương 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...	- 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 công khai PKCS#. - Tìm hiểu về lịch sử của khóa công khai để hiểu tại sao nó lại là	- 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 công khai PKCS#. - 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

		điểm xuất phát của mã hóa hiện đại ngày nay			
Tư vấn	VPK CNTT &TT	- Giải đáp vướng mắc khi tìm hiểu về lịch sử chuẩn mã hóa khóa công khai PKCS#	- Nắm được chuẩn mã hóa khóa công khai PKCS#	Các câu hỏi cần giải đáp	

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	2 giờ Phòng học	- Hệ mã hóa dựa trên thuộc tính của Waters	- Nắm được các bước tạo khóa, lập mã, giải mã của hệ. - Nắm được mức độ an toàn của hệ trước các mô hình tấn công. - Đánh giá được tính hiệu quả của hệ khi cài đặt trong thực tế.	Đọc tài liệu [1] (chương 4), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	B
BT-TL	3 giờ Phòng học	- Bài tập về cách tạo khóa, chữ ký, kiểm tra chữ ký của các hệ chữ ký điện tử RSA,Elgamal, DSS (tiếp). - Thảo luận về các loại access policy. - Thảo luận về Linear secret sharing	- Biết được cụ thể phương pháp cài đặt hệ chữ ký ECDSA - Thành thạo các cách tạo khóa, lập mã, giải mã của các hệ chữ ký điện tử RSA,Elgamal, DSS, BLS, Boneh-Boyen. - Nắm được các loại access policy hiện có	Đọc tài liệu [1] (chương 4), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	B

			trong thực tế - Nắm được kỹ thuật Linear secret sharing		
Tự học	12 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu các hệ mật mã khóa công khai hiện đại sử dụng công cụ Pairings. Các hệ chữ ký điện tử hiện đại sử dụng công cụ Pairings. - Tìm hiểu về các loại access policy hiện có trong thực tế. - Tìm hiểu về những ứng dụng của Linear secret sharing, đặc biệt trong xây dựng access policy	- Nắm được ưu nhược điểm của công cụ Pairings. - Nắm được các application nào nên dùng loại access policy nào. - Nắm được những ứng dụng của kỹ thuật Linear secret sharing, đặc biệt trong xây dựng access policy	Đọc tài liệu [1] (chương 4), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	B
Tư vấn	VPK CNTT &TT	- Cách vấn đề xoay quanh access policy	- Nắm sâu hơn về access policy, ứng dụng trong thực tế.	Các câu hỏi cần giải đáp	

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	- Cải tiến của hệ mã hóa dựa trên thuộc tính của Waters. - Đánh giá và hướng phát triển của mã hóa dựa trên thuộc tính	- Nắm vững một số cải tiến của hệ mã hóa dựa trên thuộc tính của Waters. - Nắm được các hướng phát triển của hệ mã	Đọc tài liệu [1] (chương 5), và [2] học liệu tham	C

			hóa dựa trên thuộc tính, các loại kỹ thuật dùng để xây dựng hệ mã hóa dựa trên thuộc tính, nhưng thách thức cần phải vượt qua.	khảo. Tài liệu internet tự tìm trên google	
BT-TL	3 giờ Phòng học	- Thảo luận về hệ mã hóa dựa trên thuộc tính của Waters. - Thảo luận về các cải tiến của hệ mã hóa dựa trên thuộc tính của Waters	- Hiểu được những ưu nhược điểm của hệ mã hóa dựa trên thuộc tính của Waters. - Hiểu được các cải tiến đã khắc phục các nhược điểm này như thế nào, còn những nhược điểm gì cần phải khắc phục tiếp.	Đọc tài liệu [1] (chương 5), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu các kiến thức về mã hóa dựa trên thuộc tính. Các hệ mã hóa dựa trên thuộc tính khác hiện có, so sánh ưu nhược điểm của các hệ đó với hệ mã hóa dựa trên thuộc tính của Waters. - Tìm hiểu các cải tiến của hệ mã hóa dựa trên thuộc tính của Waters, đánh giá xem các cải tiến này đã tối ưu chưa, đã khắc phục được hết nhược điểm chưa, có phát sinh thêm nhược điểm gì mới trong quá	- Nắm vững về các loại hệ mã hóa dựa trên thuộc tính - Có khả năng đánh giá tốt các mặt ưu nhược điểm của một hệ mã hóa dựa trên thuộc tính, để từ đó có khả năng lựa chọn một hệ mã hóa dựa trên thuộc tính phù hợp với một ứng dụng cụ thể trong thực tế.	Đọc tài liệu [1] (chương 5), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	C

		trình khắc phục nhược điểm cũ không.			
Tư vấn	VPK CNTT &TT	- Giải đáp vướng mắc khi tìm hiểu về hệ mã hóa thuộc tính của Waters, các cải tiến của nó.	- Nắm được các kiến thức về mã hóa thuộc tính.	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	- Giới thiệu về Homomorphic Encryption - Các công cụ xây dựng và xu hướng phát triển. -Multiplicative Homomorphic Encryption	- Nắm được kiến thức tổng quan về Homomorphic Encryption. - Nắm được tổng quan mộ số công cụ dùng để xây dựng các hệ Homomorphic Encryption, xu hướng phát triển hiện nay, tình hình áp dụng trong thực tế. - Nắm được các bước tạo khóa, lập mã, giải mã của một hệ Multiplicative Encryption.	Đọc tài liệu [1] (chương 5), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
BT-TL	3 giờ Phòng	- Thảo luận về Homomorphic	- Nắm vững về Homomorphic Encryption, các loại	Đọc tài liệu [1] (chương	C

	học	Encryption. - Tìm hiểu về các ứng dụng cụ thể của Homomorphic Encryption trong thực tế	công cụ, khó khăn hiện tại. - Biết được các loại ứng dụng của Homomorphic Encryption trong thực tế, tầm quan trọng của nó.	5), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu các vấn đề về Homomorphic Encryption - Tìm hiểu về các ứng dụng cụ thể của Homomorphic Encryption trong thực tế	-Nắm vững về Homomorphic Encryption, các loại công cụ, khó khăn hiện tại. - Biết được các loại ứng dụng của Homomorphic Encryption trong thực tế, tầm quan trọng của nó	Đọc tài liệu [1] (chương 5), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
Tư vấn	VPK CNTT &TT	- Các vấn đề về Homomorphic Encryption	- Hiểu được ưu nhược điểm của Homomorphic Encryption, các ứng dụng trong thực tế của nó, cách xây dựng hệ Multiplicative HE	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	2 giờ Phòng học	Additive Homomorphic Encryption: - Giới thiệu - Construction - Đánh giá	- Nắm được thế nào là một hệ Additive Homomorphic Encryption. Ứng dụng của nó trong thực tế. - Nắm được các bước tạo khóa, lập mã, giải mã của một hệ Additive Encryption. - Nắm được các ưu nhược điểm của hệ này. Ứng dụng trong thực tế.	Đọc tài liệu [1] (chương 5), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
BT-TL	3 giờ Phòng học	- Ôn luyện lại các bước tạo khóa, lập mã, giải mã của một hệ Additive Encryption. - Tìm hiểu tiếp các ưu nhược điểm của hệ này. Ứng dụng trong thực tế	- Thành thạo các bước tạo khóa, lập mã, giải mã của một hệ Additive Encryption. - Nắm vững các ưu nhược điểm của hệ này. Ứng dụng trong thực tế	Đọc tài liệu [1] (chương 5), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu hệ Multiplicative Homomorphic Encryption. Ứng dụng của nó trong thực tế. - Tìm hiểu hệ Additive Homomorphic Encryption. Ứng dụng của nó trong thực tế.	- Nắm được các loại hệ Multiplicative Homomorphic Encryption và Additive Homomorphic Encryption. Ứng dụng của chúng trong thực tế.	Đọc tài liệu [1] (chương 5), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên	C

				google	
Tư vấn	VPK CNTT &TT	- Một số vấn đề vướng mắc về Multiplicative Homomorphic Encryption và Additive Homomorphic Encryption.	- Nắm được các loại hệ Multiplicative Homomorphic Encryption và Additive Homomorphic Encryption. Ứng dụng của chúng trong thực tế.	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	2 giờ Phòng học	Garbled Circuit: - Tại sao cần Garbled Circuit? - Ứng dụng và xu hướng phát triển. - Giới thiệu Yao's Circuit.	- Nắm được thế nào là Garbled Circuit, tại sao lại cần nó, ứng dụng thực tế của nó. Xu hướng phát triển thực tế của nó. - Nắm được tổng quan về Yao's Circuit.	Đọc tài liệu [1] (chương 6), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
BT-TL	3 giờ Phòng học	- Phân tích, thảo luận về Garbled Circuit. - Tìm hiểu về ứng dụng và xu hướng phát triển của Garbled	- Nắm được thế nào là Garbled Circuit, tại sao lại cần nó, ứng dụng thực tế của nó. Xu hướng phát triển thực	Đọc tài liệu [1] (chương 6), và [2] học liệu tham	C

		Circuit. - Thảo luận về Yao's Circuit.	tế của nó. - Nắm được tổng quan về Yao's Circuit.	khảo. Tài liệu internet tự tìm trên google	
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu về Garbled Circuit. - Tìm hiểu về Yao's Circuit.	- Nắm vững về Garbled Circuit và Yao's Circuit.	Đọc tài liệu [1] (chương 6), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
Tư vấn	VPK CNTT &TT	- Các vấn đề vướng mắc khi tìm hiểu về Garbled Circuit và Yao's Circuit	- Nắm vững về Garbled Circuit và Yao's Circuit	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
Lý thuyết	2 giờ Phòng học	- Các bước xây dựng Encoded Input và Truth tables của Protocol của Yao's Circuit - Đánh giá Security của Yao's Circuit	- Nắm được các bước xây dựng Encoded Input và Truth tables của Protocol của Yao's Circuit. - Nắm được Security của Yao's Circuit.	Đọc tài liệu [1] (chương 6), và [2] học liệu tham khảo.	C

		- Đánh giá Yao's Circuit và các ứng dụng sang primitives khác	- Đánh giá được ưu nhược điểm của Yao's Circuit và biết được các hệ khác mà có sử dụng Yao's Circuit như là một thành phần.	Tài liệu internet tự tìm trên google	
BT-TL	1 giờ Phòng học	- Phân tích, thảo luận các bước xây dựng Encoded Input và Truth tables của Protocol của Yao's Circuit - Phân tích, thảo luận Security của Yao's Circuit.	- Nắm được các bước xây dựng Encoded Input và Truth tables của Protocol của Yao's Circuit. - Nắm được Security của Yao's Circuit. - Đánh giá được ưu nhược điểm của Yao's Circuit và biết được các hệ khác mà có sử dụng Yao's Circuit như là một thành phần.	Đọc tài liệu [1] (chương 6), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
KT&ĐG giữa kỳ	2 giờ Phòng học	Kiểm tra về một trong các nội dung: Cách các bước tạo khóa, lập mã, giải mã của một hệ Additive Encryption; mã hóa dựa trên thuộc tính	Đánh giá kỹ năng các bước tạo khóa, lập mã, giải mã của một hệ Additive Encryption; Đánh giá mức độ nắm được kiến thức về mã hóa dựa trên thuộc tính	Giấy làm bài	B,C
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu tiếp về ưu nhược điểm của Yao's Circuit, các thách thức mà cần phải khắc phục. - Tìm hiểu ứng dụng	- Nắm vững ưu nhược điểm của Yao's Circuit và biết được các hệ khác mà có sử dụng Yao's Circuit như là một thành phần	Đọc tài liệu [1] (chương 6), và [2] học liệu tham khảo.	C

		của Yao's Circuit.		Tài liệu internet tự tìm trên google	
Tư vấn	VPK CNTT &TT	- Các vấn đề vướng mắc khi tìm hiểu về ưu nhược điểm của Yao's Circuit, các thách thức mà cần phải khắc phục	- Nắm vững ưu nhược điểm của Yao's Circuit và biết được các hệ khác mà có sử dụng Yao's Circuit như là một thành phần	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	- Các bước xây dựng Encoded Input và Truth tables của Protocol của hệ Free Xor - Đánh giá Security của hệ Free Xor - Đánh giá hệ Free Xor và các ứng dụng sang primitives khác.	- Nắm được các bước xây dựng Encoded Input và Truth tables của Protocol của hệ Free Xor. - Nắm được Security của hệ Free Xor. - Đánh giá được ưu nhược điểm của hệ Free Xor và biết được các hệ khác mà có sử dụng hệ Free Xor như là một thành phần	Đọc tài liệu [1] (chương 6), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
BT-TL	3 giờ Phòng học	- Phân tích, thảo luận các bước xây dựng Encoded Input và Truth tables của	- Nắm được các bước xây dựng Encoded Input và Truth tables của Protocol của hệ	Đọc tài liệu [1] (chương 6), và [2]	C

		Protocol của hệ Free Xor - Phân tích, thảo luận Security của hệ Free Xor.	Free Xor. - Nắm được Security của hệ Free Xor. - Đánh giá được ưu nhược điểm của hệ Free Xor và biết được các hệ khác mà có sử dụng hệ Free Xor như là một thành phần	học liệu tham khảo. Tài liệu internet tự tìm trên google	
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu tiếp về ưu nhược điểm của hệ Free Xor, các thách thức mà cần phải khắc phục. - Tìm hiểu ứng dụng của hệ Free Xor.	- Nắm vững ưu nhược điểm của hệ Free Xor và biết được các hệ khác mà có sử dụng hệ Free Xor như là một thành phần	Đọc tài liệu [1] (chương 6), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
Tư vấn	VPK CNTT &TT	- Các vấn đề vướng mắc khi tìm hiểu về ưu nhược điểm của hệ Free Xor, các thách thức	- Nắm vững ưu nhược điểm của hệ Free Xor và biết được các hệ khác mà có sử dụng hệ Free Xor như là một thành phần	Các câu hỏi cần giải đáp	

Nội dung tuần 10 (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 xây dựng Encoded Input và Truth tables của Protocol của hệ Two halfs make a whole - Đánh giá Security của hệ Two halfs make a whole - Đánh giá hệ Two halfs make a whole và các ứng dụng sang primitives khác. - Đánh giá và xu hướng phát triển	- Nắm được các bước xây dựng Encoded Input và Truth tables của Protocol của hệ Two halfs make a whole. - Nắm được Security của hệ Two halfs make a whole. - Đánh giá được ưu nhược điểm của hệ Two halfs make a whole và biết được các hệ khác mà có sử dụng hệ Two halfs make a whole như là một thành phần - Nắm được xu hướng phát triển của kỹ thuật dựa trên Two halfs make a whole	Đọc tài liệu [1] (chương 6), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	C, D
BT-TL	3 giờ Phòng học	- Phân tích, thảo luận các bước xây dựng Encoded Input và Truth tables của Protocol của hệ Two halfs make a whole - Phân tích, thảo luận Security của hệ Two halfs make a whole	- Nắm được các bước xây dựng Encoded Input và Truth tables của Protocol của hệ Two halfs make a whole. - Nắm được Security của hệ Two halfs make a whole. - Đánh giá được ưu nhược điểm của hệ Two halfs make a whole và biết được các	Đọc tài liệu [1] (chương 6), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	C, D

			hệ khác mà có sử dụng hệ Two halfs make a whole như là một thành phần		
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu tiếp về ưu nhược điểm của hệ Two halfs make a whole, các thách thức mà cần phải khắc phục. - Tìm hiểu ứng dụng của hệ Two halfs make a whole.	- Nắm vững ưu nhược điểm của hệ Two halfs make a whole và biết được các hệ khác mà có sử dụng hệ Two halfs make a whole như là một thành phần.	Đọc tài liệu [1] (chương 6), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	C,D
Tư vấn	VPK CNTT &TT	- Các vấn đề vướng mắc khi tìm hiểu về ưu nhược điểm của hệ Two halfs make a whole các thách thức	- Nắm vững ưu nhược điểm của hệ Two halfs make a whole và biết được các hệ khác mà có sử dụng hệ Two halfs make a whole như là một thành phần	Các câu hỏi cần giải đáp	

Nội dung tuần 11 (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	Outsourcing Computation: - Giới thiệu và ứng dụng - Đánh giá và xu	- Nắm được tổng quan về Outsourcing Computation. Ứng dụng của nó trong thực tế.	Đọc tài liệu [1] (chương 7), và [2] học liệu	D

		hướng phát triển Randomize Encoding: -Giới thiệu	- Đánh giá được xu thế phát triển của nó, những khó khăn mà nó cần phải khắc phục. - Nắm được tổng quan về Randomize Encoding. Ứng dụng của nó trong thực tế	tham khảo. Tài liệu internet tự tìm trên google	
BT-TL	3 giờ Phòng học	- Thảo luận về Outsourcing Computation - Thảo luận về Randomize Encoding	- Nắm được tổng quan về Outsourcing Computation. Ứng dụng của nó trong thực tế. - Đánh giá được xu thế phát triển của nó, những khó khăn mà nó cần phải khắc phục. - Nắm được tổng quan về Randomize Encoding. Ứng dụng của nó trong thực tế.	Đọc tài liệu [1] (chương 7), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	D
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu về ứng dụng của Outsourcing Computation trong thực tế	- Hiểu biết sâu hơn về Outsourcing Computation. .	Đọc tài liệu [1] (chương 7), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	D
Tư vấn	VPK CNTT	- Các vấn đề vướng mắc khi tìm hiểu về	- Hiểu biết sâu hơn về Outsourcing	Các câu hỏi cần	

	&TT	vấn đề Outsourcing Computation và Randomize Encoding	Computation và Randomize Encoding	giải đáp	

Nội dung tuần 12 (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	Randomize Encoding: - A simple construction - Full construction	- Nắm được các bước xây dựng Encoded Input và Truth tables của simple construction và full construction. - Nắm được Security của simple construction và full construction.. - Đánh giá được ưu nhược điểm của simple construction và full construction và biết được các hệ khác mà có sử dụng simple construction và full construction như là một thành phần	Đọc tài liệu [1] (chương 7), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	D
BT-TL	3 giờ Phòng học	- Phân tích, thảo luận các bước xây dựng Encoded Input và Truth tables của Protocol của simple construction và full construction - Phân	- Nắm được các bước xây dựng Encoded Input và Truth tables của simple construction và full construction. - Nắm được Security của simple construction	Đọc tài liệu [1] (chương 7), và [2] học liệu tham khảo.	D

		tích, thảo luận Security của simple construction và full construction	và full construction.. - Đánh giá được ưu nhược điểm của simple construction và full construction và biết được các hệ khác mà có sử dụng simple construction và full construction như là một thành phần	Tài liệu internet tự tìm trên google	
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu về các hệ randomize encoding khác. Ứng dụng trong thực tế của chúng	- Nắm được các loại hệ randomize encoding. Ứng dụng của chúng trong thực tế	Đọc tài liệu [1] (chương 7), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	D
Tư vấn	VPK CNTT &TT	- Các vấn đề vướng mắc khi tìm hiểu về randomize encoding.	- Nắm vững về randomize encoding.	Các câu hỏi cần giải đáp	

Nội dung tuần 13 (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	Functional Encryption: - Giới thiệu - Hệ GVW12	- Nắm được tổng quan về Functional Encryption, những khó	Đọc tài liệu [1] (chương	D

	học		khăn và thách thức hiện nay khi xây dựng Functional Encryption. - Nắm được các bước tạo khóa, lập mã, giải mã của hệ GVW12. Đánh giá được tính hiệu quả và độ an toàn của hệ này. So sánh được với các hệ mã hóa khác.	7), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	
BT-TL	4 giờ Phòng học	Thảo luận về Functional Encryption Thảo luận về kỹ thuật xây dựng hệ mã hóa GVW12.	Nắm được tại sao Functional Encryption lại là một primitive quan trọng hiện nay. Nắm chắc các bước tạo khóa, lập mã, giải mã của hệ mã hóa GVW12. Đánh giá được tính hiệu quả và độ an toàn của hệ này. So sánh được với các hệ mã hóa khác.	Đọc tài liệu [1] (chương 7), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	D
Tự học	15 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu sâu hơn về Functional Encryption. - Tìm hiểu sâu hơn về hệ mã hóa GVW12 và các mở rộng của nó.	Nắm được tại sao Functional Encryption lại là một primitive quan trọng hiện nay. Nắm chắc các bước tạo khóa, lập mã, giải mã của hệ mã hóa GVW12. Đánh giá được tính hiệu quả và độ an toàn của hệ này. So sánh được với các	Đọc tài liệu [1] (chương 7), và [2] học liệu tham khảo. Tài liệu internet tự tìm trên google	D

			hệ mã hóa khác.		
Tư vấn	VPK CNTT &TT	- Giải đáp các vấn đề về Functional Encryption	- Nắm được các vấn đề xoay quang Functional Encryption.	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. 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 có trọng số 0,3.
- 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/ứng dụng chứng thực số /ứng dụng truyền dữ liệu an toàn/tìm hiểu về các frameworks để xây dựng ứng dụng dựa trên Blockchain. 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 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

10.3. Kiểm tra – đánh giá cuối kì:

- Hình thức: Thi viết 120 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**