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

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN:
AN TOÀN BẢO MẬT THÔNG TIN
MÃ HỌC PHẦN : 173036

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: 0373821617 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, 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: AN TOÀN BẢO MẬT THÔNG TIN

Số tín chỉ: 3

Học kỳ: 7

Học phần: Bắt buộc

Các học phần tiên quyết: CTDL&GT, Lập trình trực quan, Lý thuyết mật mã

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:

Giới thiệu chung về vấn đề an toàn và bảo mật thông tin, các phương pháp cổ điển cũng như hiện đại để giải quyết các vấn đề đó. Giới thiệu các hệ mã hóa khóa đối xứng, công khai, chữ ký điện tử, hàm băm với các chuẩn được dùng trong thực tế hiện nay. Giới thiệu về cơ sở hạ tầng khóa công khai, các kỹ thuật xây dựng cơ sở hạ tầng khóa công khai, các ứng dụng chứng thực số và truyền dữ liệu an toàn. Giới thiệu về công nghệ Blockchain và ứng dụng của nó trong thực tế.

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; Nắm được chuẩn an toàn khi dùng các hệ mã hóa khóa đối xứng, hệ mã hóa khóa công khai, chữ ký điện tử, hàm băm trong thực tế;	C13

	1.2	Nắm vững được kiến thức cơ sở hạ tầng khóa công khai, các kỹ thuật xây dựng cơ sở hạ tầng khóa công khai, các ứng dụng chứng thực số và truyền dữ liệu an toàn	C13
	1.3	Hiểu rõ về công nghệ Blockchain và các ứng dụng của nó trong thực tế	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), một hệ chữ ký điện tử hay hàm băm để đảm bảo an toàn thông tin cho một hệ thống cụ thể	C14, C18
	2.2	Có khả năng (cài đặt mới hoặc dùng từ thư viện có sẵn) một ứng dụng chứng thực số hay một ứng dụng truyền dữ liệu an toàn cụ thể	C14, C18
	2.3	Có khả năng vận dụng công nghệ Blockchain để giải quyết các bài toán trong thực tế.	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, cẩn cù, chính xác cũng như hình thành các kỹ năng riêng cho bản thân khi giải quyết các vấn đề của môn an toàn bảo mật thông tin, 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 học của lý thuyết mật mã	1.1	C13

B	Hiểu rõ và vận dụng cài đặt được các hệ mã hóa khóa đối xứng, các hệ mã hóa khóa công khai, hệ chữ ký điện tử, hàm băm 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 ứng dụng chứng thực số và ứng dụng truyền dữ liệu an toàn	1.3, 2.2	C13, C14, C18
D	Khả năng vận dụng công nghệ Blockchain để giải quyết các bài toán trong thực tế.	3, 2.3	C13,C14,C21,C22,C23

6. Nội dung chi tiết học phần:

CHƯƠNG 1: TỔNG QUAN VỀ AN TOÀN BẢO MẬT THÔNG TIN

1.1. Giới thiệu chung về an toàn bảo mật thông tin

1.1.1. Một số vấn đề trong an toàn bảo mật thông tin

1.1.2. Phương pháp cổ điển

1.2.2. Phương pháp hiện đại

1.2.3. Một số đánh giá và hướng phát triển

1.2. Cơ sở toán học

1.2.1. Số học Modulo

1.2.2. Một số bài toán khó

1.2.3. Các công cụ cơ bản để xây dựng nên các hệ mã, chữ ký điện tử hiện đại ngày nay

1.3. Một số thuật toán cơ bản

1.4. Bài tập

CHƯƠNG 2. MÃ HÓA VÀ CHỮ KÝ ĐIỆN TỬ

2.1. Mã hóa khóa bí mật

2.1.1. Mô hình tổng quát của hệ mã hóa khóa đối xứng với chuẩn an toàn block cipher mode

2.1.2. Hệ mã A5/1 và RC4 với chuẩn an toàn block cipher mode

2.2. Mã hóa khóa công khai

2.2.1. Mô hình tổng quát của hệ mã hóa khóa công khai

2.2.2. Tấn công chọn bản rõ và tấn công chọn bản mã

2.2.3. Tấn công chọn bản mã trên hệ RSA và Elgamal

2.2.4. Hệ mã RSA-OAEP an toàn trước tấn công chọn bản mã

2.2.5. Hệ mã Cramer-Shoup an toàn trước tấn công chọn bản mã

2.3. Chữ ký điện tử

2.3.1. Mô hình tổng quát của hệ chữ ký điện tử

2.3.2. Hệ chữ ký ECDSA và so sánh với hệ chữ ký RSA, DSS

2.3.3. Một số hệ chữ ký tiên tiến khác và đánh giá

2.4. Bài tập

CHƯƠNG 3. CƠ SỞ HẠ TẦNG KHÓA CÔNG KHAI VÀ ỨNG DỤNG CHỨNG THỰC SỐ

3.1. Cơ sở hạ tầng khóa công khai

3.1.1. Giới thiệu

3.1.2. Lược đồ xây dựng chung

3.1.3. Dựa trên RSA

3.1.4. Dựa trên Elgamal, DSS

3.2. Ứng dụng chứng thực số

3.2.1. Giới thiệu ứng dụng chứng thực số

3.2.2. Xây dựng ứng dụng chứng thực số dựa trên RSA

3.2.3. Xây dựng ứng dụng chứng thực số dựa trên Elgamal, DSS

3.2.4. Giới thiệu một số hệ thống ứng dụng chứng thực số phổ biến

3.3. Bài tập

CHƯƠNG 4. CƠ SỞ HẠ TẦNG KHÓA CÔNG KHAI VÀ ỨNG DỤNG TRUYỀN DỮ LIỆU AN TOÀN

4.1. Bài toán truyền dữ liệu an toàn

4.1.1. Giới thiệu bài toán

4.1.2. Toàn vẹn thông điệp với MAC

4.1.3. Giao thức TLS

4.2. Xây dựng ứng dụng truyền dữ liệu an toàn

4.2.1. Dùng mình kỹ thuật mã hóa khóa công khai

4.2.2. Dùng hệ mã hóa lai (hybrid encryption)

4.2.3. Dùng giao thức Diffe-Hellman và hệ mã hóa đối xứng

4.3. Một số ứng dụng khác trong thực tế

4.3.1. Truyền hình trả tiền dùng mã hóa quảng bá NNL

4.3.2. Điện toán đám mây dùng mã hóa dựa trên thuộc tính

4.4. Bài tập

CHƯƠNG 5. CÔNG NGHỆ BLOCKCHAIN

5.1. Giới thiệu chung

5.1.1. Giới thiệu bài toán

5.1.2. Giới thiệu chung về công nghệ Blockchain

5.1.3. Ứng dụng

5.2. Công nghệ Blockchain

5.2.1. Các kiến thức chung của Blockchain

5.2.2. Cơ chế đồng thuận

5.2.3. Tạo Block mới và xác thực dữ liệu

5.3. Ứng dụng tiền điện tử Bitcoins và các ứng dụng khác

5.3.1. Ứng dụng Bitcoins

5.3.2. Các ứng dụng khác

5.3.3. Một số Frameworks để xây dựng ứng dụng

5.4. 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. 2004

[2]. Blockchain: Bản Chất Của Blockchain, Bitcoin, Tiền Điện Tử, Hợp Đồng Thông Minh Và Tương Lai Của Tiền Tệ. Nhà xuất bản Nhà Xuất Bản Lao Động Dịch Giả Thành Dương, 2017

+ *Học liệu tham khảo*

[1]. Blockchain – Khởi Nguồn Cho Một Nền Kinh Tế Mới. Dịch giả LeVN, nhà xuất bản Đại Học Kinh Tế Quốc Dân, 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: TỔNG QUAN VỀ AN TOÀN BẢO MẬT THÔNG TIN	**1**	**1**		**4.5**	
1.1. Giới thiệu chung về an toàn bảo mật thông tin	0,25			1	
1.2. Cơ sở toán học	0,5	1		1.5	
1.3. Một số thuật toán cơ bản	0,25			2	
CHƯƠNG 2: MÃ HÓA VÀ CHỮ KÝ ĐIỆN TỬ	**4**	**6**		**21**	
2.1. Mã hóa khóa bí mật 2.1.1. Mô hình tổng quát của hệ mã hóa khóa đối xứng với chuẩn an toàn block cipher mode 2.1.2. Hệ mã A5/1 và RC4 với chuẩn an toàn block cipher mode	1	2		10	
2.2. Mã hóa khóa công khai 2.2.1. Mô hình tổng quát của hệ mã hóa khóa công khai 2.2.2. Tấn công chọn bản rõ và tấn công chọn bản mã 2.2.3. Tấn công chọn bản mã trên hệ RSA và Elgamal 2.2.4. Hệ mã RSA-OAEP an toàn trước tấn công chọn bản mã	2	2		11	

2.2.5. Hệ mã Cramer-Shoup an toàn trước tấn công chọn bản mã					
2.3. Chữ ký điện tử 2.3.1. Mô hình tổng quát của hệ chữ ký điện tử 2.3.2. Hệ chữ ký ECDSA và so sánh với hệ chữ ký RSA, DSS 2.3.3. Một số hệ chữ ký tiên tiến khác và đánh giá	1	2			
CHƯƠNG 3: CƠ SỞ HẠ TẦNG KHÓA CÔNG KHAI VÀ ỨNG DỤNG CHỨNG THỰC SỐ	**6**	**10**		**33**	
3.1. Cơ sở hạ tầng khóa công khai 3.1.1. Giới thiệu 3.1.2. Lược đồ xây dựng chung 3.1.3. Dựa trên RSA 3.1.4. Dựa trên Elgamal, DSS	2	4		15	
3.2. Ứng dụng chứng thực số 3.2.1. Giới thiệu ứng dụng chứng thực số 3.2.2. Xây dựng ứng dụng chứng thực số dựa trên RSA 3.2.3. Xây dựng ứng dụng chứng thực số dựa trên Elgamal, DSS 3.2.4. Giới thiệu một số hệ thống ứng dụng chứng thực số phổ biến	4	6		18	
CHƯƠNG 4: CƠ SỞ HẠ TẦNG KHÓA CÔNG KHAI VÀ ỨNG DỤNG TRUYỀN DỮ LIỆU AN TOÀN	**8**	**12**		**31**	**1**
4.1. Bài toán truyền dữ liệu an toàn 4.1.1. Giới thiệu bài toán 4.1.2. Toàn vẹn thông điệp với MAC	1	2		10	

4.1.3. Giao thức TLS					
4.2. Xây dựng ứng dụng truyền dữ liệu an toàn 4.2.1. Dùng mình kỹ thuật mã hóa khóa công khai 4.2.2. Dùng hệ mã hóa lai (hybrid encryption) 4.2.3. Dùng giao thức Diffe-Hellman và hệ mã hóa đối xứng	4	5		11	
4.3. Một số ứng dụng khác trong thực tế 4.3.1. Truyền hình trả tiền dùng mã hóa quảng bá NNL 4.3.2. Điện toán đám mây dùng mã hóa dựa trên thuộc tính	3	3		10	
KT&ĐG giữa kỳ		2			
CHƯƠNG 5: CÔNG NGHỆ BLOCKCHAIN	**6**	**11**		**39.5**	
5.1. Giới thiệu chung 5.1.1. Giới thiệu bài toán 5.1.2. Giới thiệu chung về công nghệ Blockchain 5.1.3. Ứng dụng	2	3		14.5	
5.2. Công nghệ Blockchain 5.2.1. Các kiến thức chung của Blockchain 5.2.2. Cơ chế đồng thuận 5.2.3. Tạo Block mới và xác thực dữ liệu	2	4		10	
5.3. Ứng dụng tiền điện tử Bitcoins và các ứng dụng khác 5.3.1. Ứng dụng Bitcoins 5.3.2. Các ứng dụng khác 5.3.3. Một số Frameworks để xây dựng ứng	2	4		15	

dụng					
Tổng	**25**	**40**		**135**	

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	2 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 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*	- 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	Đọc tài liệu [1] (chương 1,2), và [1] học liệu tham khảo	A, B

		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.	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 - 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 [1] học liệu tham khảo, Tài liệu internet tự tìm trên google với từ khóa là tên hệ mã.	B
Tự học	4.5 giờ	- Những vấn đề về an	- Trình bày được các	Đọc tài	A, B

	Tại nhà/ thư viện/ KLF...	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 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	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 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.	liệu [1] (chương 1,2), và [1] học liệu 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	- Giới thiệu chung về mã hóa khóa công khai, tại sao lại cần hệ mã hóa khóa công	- Nắm được tại sao lại cần phải có hệ mã hóa khóa công khai. - Hiểu được ý tưởng	Đọc tài liệu [1,2] (chương 3), và [1]	B

		khai? - Ý tưởng của Diffie Hellman và lược đồ xây dựng chung. - Tấn công chọn bản rõ và tấn công chọn bản mã - Tấn công chọn bản mã trên hệ RSA và Elgamal. - Hệ mã RSA-OAEP an toàn trước tấn công chọn bản mã - Hệ mã Cramer-Shoup an toàn trước tấn công chọn bản mã	của Diffie Hellman để xây dựng lược đồ chung cho một hệ mã hóa khóa công khai. - Nắm được hai phương pháp tấn công chọn bạn rõ và chọn bản mã nói chung. - Nắm được hai phương pháp tấn công chọn bạn rõ và chọn bản mã cụ thể trên hai hệ RSA và Elgamal - Nắm được hệ mã RSA-OAEP an toàn trước tấn công chọn bản mã. - Nắm được hệ mã Cramer-Shoup an toàn trước tấn công chọn bản mã	học liệu tham khảo. Tài liệu internet tự tìm trên google với từ khóa là tên hệ mã.	
BT-TL	3 giờ Phòng học	- Thảo luận về cài đặt hệ mã RSA-OAEP - Thảo luận về cài đặt hệ mã Cramer-Shoup	Thành thạo các thuật toán để cài đặt hai hệ mã RSA-OAEP và Cramer-Shoup.	Đọc tài liệu [1,2] (chương 3), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google với từ khóa là tên hệ mã.	B
Tự học	10 giờ Tại	- Các kiến thức toán học về số học modulo,	- Nắm vững về các kiến thức toán học, thành	Đọc tài liệu [1,2]	B

	nhà/ thư viện/ KLF...	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 điểm xuất phát của mã hóa hiện đại ngày nay	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	(chương 3,4 và [1] học liệu tham khảo. Tài liệu internet	
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	- Chuẩn chữ ký điện tử DSS, ECDSA - Hệ chữ ký ECDSA và so sánh với hệ chữ ký RSA, DSS - Một số hệ chữ ký điện tử mới hiện nay và đánh giá - Giới thiệu cơ sở hạ tầng khóa công khai là gì, tại sao cần nó. - Lược đồ chung để xây dựng cơ sở hạ tầng	- Nắm được chuẩn chữ ký điện tử DSS, chữ ký ECDSA. - Nắm được ưu nhược điểm của ECDSA và RSA, DSS. - Biết được một số hệ chữ ký mới hiện nay dựa trên Parings, ưu nhược điểm của các hệ chữ ký này so với các hệ chữ ký RSA, DSS, ECDSA - Hiểu được về cơ sở	Đọc tài liệu [1,2] (chương 4), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	B

		khóa công khai	hạ tầng khóa công khai - Nắm được lược đồ chung để xây dựng cơ sở hạ tầng khóa công khai		
BT-TL	3 giờ Phòng học	- Thảo luận về chuẩn chữ ký điện tử DSS, ECDSA - Cách cài đặt cụ thể của hệ chữ ký này dựa trên các thư viện có sẵn - Thảo luận về cơ sở hạ tầng khóa công khai và cách xây dựng.	- Biết được cụ thể phương pháp cài đặt hệ chữ ký ECDSA - Nắm được một số thư viện hiện có trên thế giới giúp cài đặt hệ chữ ký này - Nắm được lược đồ chung để xây dựng cơ sở hạ tầng khóa công khai	Đọc tài liệu [1,2] (chương 4), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	B
Tự học	12 giờ Tại nhà/ thư viện/ KLF...	- Tiếp tục tìm hiểu các thư viện cài đặt hệ chữ ký ECDSA	- Nắm vững các thư viện này.	Đọc tài liệu [1,2] (chương 4), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	B
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 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 lược đồ xây dựng cơ sở hạ tầng khóa công khai dựa trên RSA, Elgamal và DSS - Giới thiệu về ứng dụng chứng thực số	- Nắm được cách xây dựng cơ sở hạ tầng khóa công khai dựa trên kỹ thuật RSA. - Nắm được cách xây dựng cơ sở hạ tầng khóa công khai dựa trên kỹ thuật Elgamal. - Nắm được cách xây dựng cơ sở hạ tầng khóa công khai dựa trên kỹ thuật DSS. - Nắm được ứng dụng chứng thực số là gì	Đọc tài liệu [1,2] (chương 5), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
BT-TL	3 giờ Phòng học	- Thảo luận về cài đặt cơ sở hạ tầng khóa công khai dựa trên RSA - Thảo luận về cài đặt cơ sở hạ tầng khóa công khai dựa trên DSS	- Thành thạo các thuật toán để cài đặt hai cách xây dựng cơ sở hạ tầng khóa công khai dựa trên RSA và DSS. - Nắm được các thư viện hỗ trợ cài đặt	Đọc tài liệu [1,2] (chương 5), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
Tự học	10 giờ Tại nhà/ thư viện/	- Thực hành cài đặt cơ sở hạ tầng khóa công khai dựa trên RSA - Thực hành cài đặt cơ sở hạ tầng khóa công	- Thành thạo các thuật toán để cài đặt hai cách xây dựng cơ sở hạ tầng khóa công khai dựa trên RSA và DSS.	Đọc tài liệu [1,2] (chương 5), và [1] học liệu	C

	KLF...	khai dựa trên DSS	- Nắm được các thư viện hỗ trợ cài đặt	tham khảo. Tài liệu internet tự tìm trên google	
Tư vấn	VPK CNTT &TT	- Giải đáp vướng mắc về cài đặt	- Nắm được các vấn đề về cài đặt	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 lược đồ xây dựng ứng dụng chứng thực số dựa trên RSA - Giới thiệu lược đồ xây dựng ứng dụng chứng thực số dựa trên DSS	- Nắm được cách xây dựng ứng dụng chứng thực số dựa trên kỹ thuật RSA. - Nắm được cách xây dựng ứng dụng chứng thực số dựa trên kỹ thuật DSS - Nắm được các thư viện hỗ trợ cài đặt	Đọc tài liệu [1,2] (chương 5), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
BT-TL	3 giờ Phòng học	- Thảo luận về cài đặt ứng dụng chứng thực số dựa trên RSA - Thảo luận về cài đặt ứng dụng chứng thực số dựa trên DSS	- Thành thạo các thuật toán để cài đặt hai cách xây dựng ứng dụng chứng thực số dựa trên RSA và DSS. - Nắm được các thư viện hỗ trợ cài đặt	Đọc tài liệu [1,2] (chương 5), và [1] học liệu tham khảo. Tài liệu internet tự	C

				tìm trên google	
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Thực hành cài đặt ứng dụng chứng thực số dựa trên RSA - Thực hành cài đặt ứng dụng chứng thực số dựa trên DSS	- Thành thạo các thuật toán để cài đặt hai cách xây dựng ứng dụng chứng thực số dựa trên RSA và DSS. - Nắm được các thư viện hỗ trợ cài đặt	Đọc tài liệu [1,2] (chương 5), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
Tư vấn	VPK CNTT &TT	- Giải đáp vướng mắc về cài đặt	- Nắm được các vấn đề về cài đặt	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	- Giới thiệu lược đồ xây dựng ứng dụng chứng thực số dựa trên RSA (tiếp) - Giới thiệu lược đồ xây dựng ứng dụng chứng thực số dựa trên DSS (tiếp)	- Nắm được cách xây dựng ứng dụng chứng thực số dựa trên kỹ thuật RSA (tiếp). - Nắm được cách xây dựng ứng dụng chứng thực số dựa trên kỹ thuật DSS (tiếp). - Nắm được các thư viện hỗ trợ cài đặt (tiếp).	Đọc tài liệu [1,2] (chương 5), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
BT-TL	3 giờ	- Thảo luận về cài đặt	- Thành thạo các thuật	Đọc tài	C

	Phòng học	ứng dụng chứng thực số dựa trên RSA - Thảo luận về cài đặt ứng dụng chứng thực số dựa trên DSS	toán để cài đặt hai cách xây dựng ứng dụng chứng thực số dựa trên RSA và DSS. - Nắm được các thư viện hỗ trợ cài đặt	liệu [1,2] (chương 5), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Thực hành cài đặt ứng dụng chứng thực số dựa trên RSA - Thực hành cài đặt ứng dụng chứng thực số dựa trên DSS	- Thành thạo các thuật toán để cài đặt hai cách xây dựng ứng dụng chứng thực số dựa trên RSA và DSS. - Nắm được các thư viện hỗ trợ cài đặt	Đọc tài liệu [1,2] (chương 5), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
Tư vấn	VPK CNTT &TT	- Giải đáp vướng mắc về cài đặt	- Nắm được các vấn đề về 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	2 giờ Phòng học	- Giới thiệu bài toán truyền dữ liệu an toàn. - Toàn vẹn thông điệp với MAC. - Giới thiệu giao thức	- Biết được bài toán truyền dữ liệu an toàn. - Nắm được phương pháp bảo đảm toàn vẹn dữ liệu dùng kỹ thuật	Đọc tài liệu [2] (chương 6), và [1] học liệu	C

		TLS - Xây dựng ứng dụng truyền dữ liệu an toàn dùng mình hệ mã hóa khóa công khai.	MAC. - Nắm được giao thức truyền dữ liệu an toàn TLS. - Nắm được phương pháp xây dựng ứng dụng truyền dữ liệu an toàn dùng mình hệ mã hóa khóa công khai.	tham khảo. Tài liệu internet tự tìm trên google	
BT-TL	3 giờ Phòng học	- Thảo luận về cài đặt phương pháp toàn vẹn dữ liệu dùng MAC - Thảo luận về cài đặt ứng dụng truyền dữ liệu an toàn dùng mình hệ mã hóa khóa công khai.	- Thành thạo các thuật toán để cài đặt phương pháp toàn vẹn dữ liệu dùng MAC. - Thành thạo các thuật toán để cài đặt ứng dụng truyền dữ liệu an toàn dùng mình hệ mã hóa khóa công khai. - Nắm được các thư viện hỗ trợ cài đặt	Đọc tài liệu [2] (chương 6), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Thực hành cài đặt phương pháp toàn vẹn dữ liệu dùng MAC - Thực hành cài đặt ứng dụng truyền dữ liệu an toàn dùng mình hệ mã hóa khóa công khai	- Thành thạo các thuật toán để cài đặt phương pháp toàn vẹn dữ liệu dùng MAC. - Thành thạo các thuật toán để cài đặt ứng dụng truyền dữ liệu an toàn dùng mình hệ mã hóa khóa công khai. - Nắm được các thư viện hỗ trợ cài đặt	Đọc tài liệu [2] (chương 6), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
Tư vấn	VPK CNTT &TT	- Giải đáp vướng mắc về cài đặt	- Nắm được các vấn đề về 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
Lý thuyết	2 giờ Phòng học	- - Xây dựng ứng dụng truyền dữ liệu an toàn dùng hệ mã hóa lai (hybrid encryption). - Xây dựng ứng dụng truyền dữ liệu an toàn dùng giao thức Diffe-Hellman và hệ mã hóa đối xứng.	- Biết được bài toán truyền dữ liệu an toàn. - Nắm được phương pháp xây dựng ứng dụng truyền dữ liệu an toàn dùng hệ mã hóa lai (hybrid encryption). - Nắm được phương pháp xây dựng ứng dụng truyền dữ liệu an toàn dùng giao thức Diffe-Hellman và hệ mã hóa đối xứng.	Đọc tài liệu [2] (chương 6), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
BT-TL	1 giờ Phòng học	- Thảo luận về cài đặt ứng dụng truyền dữ liệu an toàn dùng hệ mã hóa lai (hybrid encryption). - Thảo luận về cài đặt ứng dụng truyền dữ liệu an toàn dùng giao thức Diffe-Hellman và hệ mã hóa đối xứng.	- Thành thạo các thuật toán để cài đặt ứng dụng truyền dữ liệu an toàn dùng hệ mã hóa lai (hybrid encryption). - Thành thạo các thuật toán để cài đặt ứng dụng truyền dữ liệu an toàn dùng giao thức Diffe-Hellman và hệ mã hóa đối xứng. - Nắm được các thư viện hỗ trợ cài đặt	Đọc tài liệu [2] (chương 6), và [1] 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: ứng dụng truyền dữ liệu an toàn dùng hệ mã hóa lai + ứng dụng chứng	Nắm được về ứng dụng chứng thực số và ứng dụng truyền dữ liệu an toàn	Giấy làm bài	B,C

		thực số dựa trên RSA; ứng dụng truyền dữ liệu an toàn dùng giao thức Diffe-Hellman và hệ mã hóa đối xứng + ứng dụng chứng thực số dựa trên DSS			
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Thực hành cài đặt ứng dụng truyền dữ liệu an toàn dùng hệ mã hóa lai (hybrid encryption). - Thực hành cài đặt ứng dụng truyền dữ liệu an toàn dùng giao thức Diffe-Hellman và hệ mã hóa đối xứng.	- Thành thạo các thuật toán để cài đặt ứng dụng truyền dữ liệu an toàn dùng hệ mã hóa lai (hybrid encryption). - Thành thạo các thuật toán để cài đặt ứng dụng truyền dữ liệu an toàn dùng giao thức Diffe-Hellman và hệ mã hóa đối xứng. - Nắm được các thư viện hỗ trợ cài đặt	Đọc tài liệu [2] (chương 6), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
Tư vấn	VPK CNTT &TT	- Giải đáp vướng mắc về cài đặt	- Nắm được các vấn đề về 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	- Xây dựng ứng dụng truyền dữ liệu an toàn dùng giao thức Diffe-Hellman và hệ mã hóa đối xứng (tiếp). - Xây dựng ứng dụng	- Biết được bài toán truyền dữ liệu an toàn. - Nắm được phương pháp xây dựng ứng dụng truyền dữ liệu an toàn dùng giao thức	Đọc tài liệu [2] (chương 6), và [1] học liệu tham	C

		truyền hình trả tiền dùng mã hóa quảng bá NNL	Diffe-Hellman và hệ mã hóa đối xứng. - Nắm được phương pháp xây dựng ứng dụng truyền hình trả tiền dùng mã hóa quảng bá NNL	khảo. Tài liệu internet tự tìm trên google	
BT-TL	3 giờ Phòng học	- Thảo luận về cài đặt ứng dụng truyền hình trả tiền dùng mã hóa quảng bá NNL - Thảo luận về cài đặt ứng dụng truyền dữ liệu an toàn dùng giao thức Diffe-Hellman và hệ mã hóa đối xứng.	- Thành thạo các thuật toán để cài đặt ứng dụng truyền hình trả tiền dùng mã hóa quảng bá NNL - Thành thạo các thuật toán để cài đặt ứng dụng truyền dữ liệu an toàn dùng giao thức Diffe-Hellman và hệ mã hóa đối xứng. - Nắm được các thư viện hỗ trợ cài đặt	Đọc tài liệu [2] (chương 6), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Thực hành cài đặt ứng dụng truyền hình trả tiền dùng mã hóa quảng bá NNL. - Thực hành cài đặt ứng dụng truyền dữ liệu an toàn dùng giao thức Diffe-Hellman và hệ mã hóa đối xứng.	- Thành thạo các thuật toán để cài đặt ứng dụng truyền hình trả tiền dùng mã hóa quảng bá NNL. - Thành thạo các thuật toán để cài đặt ứng dụng truyền dữ liệu an toàn dùng giao thức Diffe-Hellman và hệ mã hóa đối xứng. - Nắm được các thư viện hỗ trợ cài đặt	Đọc tài liệu [2] (chương 6), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	C
Tư vấn	VPK CNTT &TT	- Giải đáp vướng mắc về cài đặt	- Nắm được các vấn đề về cài đặt	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	- Giới thiệu điện toán đám mây dùng mã hóa dựa trên thuộc tính. - Giới thiệu chung về công nghệ Blockchain - Giới thiệu chung về ứng dụng của công nghệ Blockchain	- Nắm được điện toán đám mây dùng mã hóa dựa trên thuộc tính. - Nắm được kiến thức chung về công nghệ Blockchain. - Nắm được các loại ứng dụng phổ biến của công nghệ Blockchain	Đọc tài liệu [2] (chương 6), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	C, D
BT-TL	3 giờ Phòng học	- Thảo luận về điện toán đám mây dùng mã hóa dựa trên thuộc tính. - Thảo luận về về công nghệ Blockchain. - Thảo luận về các loại ứng dụng của công nghệ Blockchain	- Nắm được điện toán đám mây dùng mã hóa dựa trên thuộc tính. - Nắm được kiến thức chung về công nghệ Blockchain. - Nắm được các loại ứng dụng phổ biến của công nghệ Blockchain.	Đọc tài liệu [2] (chương 6), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	C, D
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu tiếp về điện toán đám mây dùng mã hóa dựa trên thuộc tính. - Tìm hiểu tiếp về công nghệ Blockchain. - Tìm hiểu tiếp các loại	- Nắm được điện toán đám mây dùng mã hóa dựa trên thuộc tính. - Nắm được kiến thức chung về công nghệ Blockchain. - Nắm được các loại	Đọc tài liệu [2] (chương 6), và [1] học liệu tham khảo.	C,D

		ứng dụng của công nghệ Blockchain .	ứng dụng phổ biến của công nghệ Blockchain.	Tài liệu internet tự tìm trên google	
Tư vấn	VPK CNTT &TT	- Giải đáp vướng mắc	- Nắm được các vấn đề về kiến thức chung và ứng dụng của Blockchain	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	- Giới thiệu về cơ sở kỹ thuật nền tảng của Blockchain bao gồm: các giao thức mạng Gossip, node mạng, chữ ký điện tử, hàm băm, merkle tree. - Giới thiệu về cơ chế đồng thuận Byzantine	- Nắm được về cơ sở kỹ thuật nền tảng của Blockchain bao gồm: các giao thức mạng Gossip, node mạng, chữ ký điện tử, hàm băm, merkle tree - Nắm cơ chế đồng thuận Byzantine	Đọc tài liệu [2] (chương 7), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	D
BT-TL	3 giờ Phòng học	- Thảo luận về cơ sở kỹ thuật nền tảng của Blockchain bao gồm: các giao thức mạng Gossip, node mạng, chữ ký điện tử, hàm băm, merkle tree. - Thảo luận về cơ chế	- Nắm được về cơ sở kỹ thuật nền tảng của Blockchain bao gồm: các giao thức mạng Gossip, node mạng, chữ ký điện tử, hàm băm, merkle tree - Nắm cơ chế đồng	Đọc tài liệu [2] (chương 7), và [1] học liệu tham khảo. Tài liệu	D

		đồng thuận Byzantine	thuận Byzantine.	internet tự tìm trên google	
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu tiếp về cơ sở kỹ thuật nền tảng của Blockchain bao gồm: các giao thức mạng Gossip, node mạng, chữ ký điện tử, hàm băm, merkle tree.. - Tìm hiểu tiếp về cơ chế đồng thuận Byzantine.	- Nắm được về cơ sở kỹ thuật nền tảng của Blockchain bao gồm: các giao thức mạng Gossip, node mạng, chữ ký điện tử, hàm băm, merkle tree - Nắm cơ chế đồng thuận Byzantine.	Đọc tài liệu [2] (chương 7), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	D
Tư vấn	VPK CNTT &TT	- Giải đáp vướng mắc	- Nắm được các vấn đề về kiến thức chung và ứng dụng của Blockchain	Các câu hỏi cần 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	- Giới thiệu về cơ chế đồng thuận của Blockchain bằng chứng công việc (PoW). - Giới thiệu về cơ chế đồng thuận của Blockchain bằng chứng cổ phần (PoS).	- Nắm được cơ chế đồng thuận của Blockchain bằng chứng công việc (PoW). - Nắm được cơ chế đồng thuận của Blockchain bằng chứng cổ phần (PoS). - Nắm được cách tạo	Đọc tài liệu [2] (chương 7), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên	D

		- Giới thiệu về cách tạo Block mới và xác thực dữ liệu trong Blockchain	Block mới và xác thực dữ liệu trong Blockchain	google	
BT-TL	3 giờ Phòng học	- Thảo luận về cơ chế đồng thuận của Blockchain bằng chứng công việc (PoW). - Thảo luận về cơ chế đồng thuận của Blockchain bằng chứng cổ phần (PoS). - Thảo luận về cách tạo Block mới và xác thực dữ liệu trong Blockchain	- Nắm được cơ chế đồng thuận của Blockchain bằng chứng công việc (PoW). - Nắm được cơ chế đồng thuận của Blockchain bằng chứng cổ phần (PoS). - Nắm được cách tạo Block mới và xác thực dữ liệu trong Blockchain	Đọc tài liệu [2] (chương 7), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	D
Tự học	10 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu tiếp về cơ chế đồng thuận của Blockchain bằng chứng công việc (PoW). - Tìm hiểu tiếp về cơ chế đồng thuận của Blockchain bằng chứng cổ phần (PoS). - Tìm hiểu tiếp về cách tạo Block mới và xác thực dữ liệu trong Blockchain	- Nắm được cơ chế đồng thuận của Blockchain bằng chứng công việc (PoW). - Nắm được cơ chế đồng thuận của Blockchain bằng chứng cổ phần (PoS). - Nắm được cách tạo Block mới và xác thực dữ liệu trong Blockchain	Đọc tài liệu [2] (chương 7), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	D
Tư vấn	VPK	- Giải đáp vướng mắc	- Nắm được cơ chế	Các câu	

	CNTT &TT		đồng thuận của Blockchain (PoS, PoW), cách tạo Block mới và xác thực dữ liệu trong Blockchain.	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 học	- Giới thiệu về ứng dụng tiền điện tử Bitcoins. - Giới thiệu về một số loại ứng dụng khác dựa trên công nghệ Blockchain. - Giới thiệu một số frameworks để cài đặt ứng dụng dựa trên Blockchain	- Nắm được ứng dụng tiền điện tử Bitcoins. - Nắm được một số loại ứng dụng khác dựa trên công nghệ Blockchain. - Nắm được một số frameworks để cài đặt ứng dụng dựa trên Blockchain	Đọc tài liệu [2] (chương 7), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	D
BT-TL	4 giờ Phòng học	- Thảo luận về ứng dụng tiền điện tử Bitcoins. - Thảo luận về một số loại ứng dụng khác dựa trên công nghệ Blockchain. - Thảo luận về một số frameworks để cài đặt ứng dụng dựa trên Blockchain	- Nắm được ứng dụng tiền điện tử Bitcoins. - Nắm được một số loại ứng dụng khác dựa trên công nghệ Blockchain. - Nắm được một số frameworks để cài đặt ứng dụng dựa trên Blockchain	Đọc tài liệu [2] (chương 7), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	D

Tự học	15 giờ Tại nhà/ thư viện/ KLF...	- Tìm hiểu tiếp về ứng dụng tiền điện tử Bitcoins. - Tìm hiểu tiếp về một số loại ứng dụng khác dựa trên công nghệ Blockchain. - Tìm hiểu tiếp về một số frameworks để cài đặt ứng dụng dựa trên Blockchain	- Nắm được ứng dụng tiền điện tử Bitcoins. - Nắm được một số loại ứng dụng khác dựa trên công nghệ Blockchain. - Nắm được một số frameworks để cài đặt ứng dụng dựa trên Blockchain.	Đọc tài liệu [2] (chương 7), và [1] học liệu tham khảo. Tài liệu internet tự tìm trên google	D
Tư vấn	VPK CNTT &TT	- Giải đáp vướng mắc	- Nắm được ứng dụng tiền điện tử Bitcoins. - Nắm được một số loại ứng dụng khác dựa trên công nghệ Blockchain. - Nắm được một số frameworks để cài đặt ứng dụng dựa trên Blockchain .	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**