ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN
AN TOÀN THÔNG TIN

1. Thông tin tổng quát

1.1. Thông tin về giảng viên

Giảng viên 1:

Họ và tên: Lê Văn Minh

Chức danh, học hàm, học vị: Giảng viên Chính – Tiến Sỹ

Thời gian, địa điểm làm việc: Bộ môn Hệ thống và Mạng máy tính, Viện Kỹ thuật Công nghệ - Đại học Vinh

Địa chỉ liên hệ: Viện Kỹ thuật Công nghệ - Đại học Vinh

Điện thoại: 081 753 2999 Email: minhdhvinh@gmail.com

Các hướng nghiên cứu chính: Mạng máy tính.

Giảng viên 2:

Họ và tên: Lê Quốc Anh

Chức danh, học hàm, học vị: Giảng viên – Thạc sỹ

Thời gian, địa điểm làm việc: Bộ môn Hệ thống và Mạng máy tính, Viện Kỹ thuật Công nghệ - Đại học Vinh

Địa chỉ liên hệ: Viện Kỹ thuật Công nghệ - Đại học Vinh

Điện thoại: 0975 836 576 Email: anhquoc.hut@gmail.com

Các hướng nghiên cứu chính: Khoa học máy tính, Mạng máy tính.

1.2. Thông tin về học phần

- Tên học phần (tiếng Việt): **An Toàn thông tin** (tiếng Anh): **Information Security**	
- Mã học phần: INF30033	
- Thuộc khối kiến thức/kỹ năng: Kiến thức chuyên ngành hẹp	
- Số tín chỉ:	3
+ Số tiết lý thuyết:	45
+ Số tiết bài tập:	0
+ Số tiết thực hành:	0
+ Số tiết hoạt động nhóm:	0
+ Số tiết tự học:	90
- Môn học tiên quyết:	Không
- Môn học trước:	Mạng máy tính

2. Mô tả học phần

Cung cấp những kiến thức cơ bản về bảo mật và an ninh số liệu; sự cần thiết phải bảo vệ dữ liệu và an toàn thông tin; các phương thức tấn công thâm nhập. Nghiên cứu các phương pháp mã hoá đối xứng và cơ sở hạ tầng khoá công khai, chứng thực điện tử và một số giải pháp bảo mật khác.

3. Mục tiêu học phần

Mục tiêu	Mô tả mục tiêu	CĐR của CTĐT	TĐNL
G1	*Áp dụng* được nguyên tắc xây dựng một hệ thống bảo mật thông tin vào các ứng dụng	1.4.3 2.2.2	3.0
G2	*Sử dụng* được kiến thức toán học vào trong lĩnh vực an toàn bảo mật thông tin	1.4.3 2.2.2	3.0
G3	*Áp dụng* được các cơ chế mật mã vào hệ thống xác thực thông tin	1.4.3 2.2.2 2.4.5 2.5.3	3.5
G4	*Chỉ ra* được các ứng dụng mật mã trong một số ứng dụng thực tiễn	1.4.3 2.2.2 2.4.5 2.5.3	3.5
G5	*Thể hiện* thái độ làm việc nghiêm túc và có trách nhiệm với xã hội	2.4.5 2.5.3	3.5

4. Chuẩn đầu ra học phần

Mục tiêu		Nội dung CĐR học phần	Mức độ giảng dạy (I,T,U)
G1	G1.1	*Diễn giải* được các nguyên tắc, đặc trưng của một hệ thống bảo mật	T
	G1.2	*Khái quát* được các nguy cơ rủi ro đối với một hệ thống thông tin	T
	G1.3	*Áp dụng* được các chiến lược bảo mật hệ thống	TU
G2	G2.1	*Làm sáng tỏ* được vai trò của các kỹ thuật mã hóa vào các hệ thống thông tin	T
	G2.2	*Áp dụng* được các kỹ thuật mã hóa đối xứng	TU
	G2.3	*Áp dụng* được các kỹ thuật mã hóa bất đối xứng	TU
G3	G3.1	*Giải thích* được nguyên tắc xây dựng chữ ký số và hàm băm	T
	G3.2	*Minh họa* được việc ứng dụng hàm băm và chữ ký điện tử trong thực tế	TU
	G3.3	*Diễn dãi* được nguyên tắc xây dựng giao thức bảo mật	TU

G4	G4.1	*Giải thích* được việc áp dụng mật mã trong các ứng dụng thực tiễn.	T
	G4.2	*Triển khai* được các ứng dụng bảo mật trong thực tế.	TU
G5	G5.1	*Nhận ra* được việc cập nhật kiến thức là rất quan trọng, học tập suốt đời.	U
	G5.2	*Thể hiện* được quá trình làm việc nghiêm túc có trách nhiệm với xã hội	TU

5. Đánh giá học phần

Thành phần đánh giá	Bài đánh giá	CĐR học phần	Tỷ lệ (%)
A1. Đánh giá quá trình			**50%**
A1.1. Ý thức học tập			***10%***
	A1.1.1: Đánh giá ý thức, thái độ học tập, chuyên cần	G1.1-G1-3 G4-1-G4.2	*10%*
A1.2. Hồ sơ học phần			***20%***
	A1.2.1: Đánh giá các bài tập lập trình, báo cáo theo nhóm	G2.1-G2.3	*20%*
A1.3. Đánh giá giữa kỳ			***20%***
	A1.3.1: Một bài kiểm tra trắc nghiệm *Ghi chú: Trung tâm kiểm định tổ chức thi*	G1.1-G1.3 G2.1-G2.3	*20%*
A2. Thi kết thúc học phần			**50%**
	A2.1: Bài thi tự luận cuối kỳ *Ghi chú: Tổ chức thi theo lịch của nhà trường*	G3.1-G3.3 G4.1-G4.2	
Công thức tính điểm học phần: (Gồm 4 con điểm thành phần) A1.1.1*0,1 + A1.2.1*0,2 + A1.3.1*0,2 + A2.1*0,5			

6. Nội dung và kế hoạch giảng dạy

6.1. Nội dung giảng dạy

Nội dung
Chương 1. Giới thiệu nhiệm vụ của an toàn và bảo mật thông tin. 1.1. Tổng quan về an toàn bảo mật thông tin 1.2. Bảo vệ thông tin trong quá trình truyền thông tin. 1.3. Mục tiêu và nguyên tắc chung của ATBM.

1.4. Giới thiệu chung về các mô hình mật mã. 1.5. Giới thiệu về pháp luật và chính sách an toàn thông tin 1.6. Luật quốc tế về an toàn thông tin 1.7. Luật Việt Nam về an toàn thông tin
Chương 2: Mã độc 2.1. Giới thiệu Malware 2.2. Phân loại Malware 2.3. Các kỹ thuật lây nhiễm và phá hoại trong Malware 2.4 Tổng quan các kỹ thuật phát hiện Malware
Chương 3: Hệ mã hóa cổ điển 3.1 Cơ sở toán học của lý thuyết mật mã 3.2. Hệ mã dịch vòng 3.3 Phân tích mã theo phương pháp thống kê 3.4. Hệ mã Vigenre 3.5. Hệ mã Affine 3.6. Hệ mã Hill 3.7 Hệ mã hoán vị 3.8. Đánh giá mức độ bảo mật của một phương pháp mã hóa.
Chương 4: Hệ mã hóa khóa bí mật 4.1. Mục đích của mã hóa hiện đại 4.2. Mã dòng: A5/1, RC4 4.3. Mã khối: DES, AES 4.4.Nhược điểm của mã hóa đối xứng 4.5. Các chế độ sử dụng mã khối
Chương 5: Hệ mã hóa khóa công khai 5.1. Nguyên tắc mã hóa khóa công khai 5.2. Mã hóa RSA 5.3. Hệ Mã ElGamal 5.4. Hệ mã Knapsack 5.5. Truyền khóa Diffie-Hellman 5.6. Ưu nhược điểm của mã hóa khóa công khai
Chương 6: Mã chứng thực thông điệp và hàm băm 6.1. Mã chứng thực thông điệp MAC 6.2. Hàm băm 6.3. Ứng dụng của hàm băm 6.4. Chữ ký điện tử RSA

Chương 7: Giao thức bảo mật 7.1 Phát lại thông điệp 7.2 Giao thức bảo mật 7.3 Định danh và trao đổi khóa phiên dùng mã hóa đối xứng với KDC 7.4 Định danh và trao đổi khóa phiên dùng mã hóa khóa công khai
Chương 8: Mốt số ứng dụng thực tiễn 8.1. Chứng chỉ X509 8.2. Giao thức SSL/ TSL 8.3. Giấu tin trong ảnh số 8.4. Chữ ký mù 8.5. Tiền ảo Bitcoin 8.6. Mã hóa ổ đĩa cứng Bit Locker 8.7. Tấn công SQL Injection

6.2. Kế hoạch giảng dạy

Tuần	Nội dung	Hình thức tổ chức dạy học	Chuẩn bị của sinh viên	CĐR môn học	Bài đánh giá
1.	**Chương 1. Giới thiệu nhiệm vụ của an toàn và bảo mật thông tin.** 1.1. Tổng quan về an toàn bảo mật thôngtin 1.2. Bảo vệ thông tin trong quá trình truyền thông tin. 1.3. Mục tiêu và nguyên tắc chung của ATBM. 1.4. Giới thiệu chung về các mô hình mật mã. 1.5. Giới thiệu về pháp luật và chính sách an toàn thông tin 1.6. Luật quốc tế về an toàn thông tin 1.7. Luật Việt Nam về an toàn thông tin	- Thuyết trình dựa trên slide kết hợp bảng-phấn. - Thảo luận	Đọc tài liệu [1], chương 1 Đọc tài liệu [3], chương 1	**G1.1-G1.3**	**A1.1.1** **A1.2.1** **A1.3.1**
2.	**Chương 2: Mã độc** 2.1. Giới thiệu Malware 2.2. Phân loại Malware 2.3. Các kỹ thuật lây nhiễm và phá hoại trong Malware	- Thuyết trình dựa trên slide kết hợp bảng-phấn. - Thảo luận - Hướng dẫn đọc tài liệu	Đọc tài liệu [1], chương 2 Đọc tài liệu [3], chương 2	**G1.1-G1.3** **G2.1-G2.3**	**A1.1.1** **A1.2.1** **A1.3.1**

	2.4 Tổng quan các kỹ thuật phát hiện Malware				
3.	**Chương 3: Hệ mã hóa cổ điển** 2.1 Cơ sở toán học của lý thuyết mật mã 2.2. Hệ mã Ceasar 2.3 Phân tích mã theo phương pháp thống kê	- Thuyết trình dựa trên slide kết hợp bảng-phấn. - Thảo luận - Hướng dẫn đọc tài liệu	Đọc tài liệu [1], chương 2 Đọc tài liệu [3], chương 2	**G1.1-G1.3** **G2.1-G2.3**	**A1.1.1** **A1.2.1** **A1.3.1**
4.	2.5. Hệ mã Vigenre 2.6. Hệ mã Affine	- Thuyết trình dựa trên slide kết hợp bảng-phấn. - Thảo luận - Nghiên cứu tình huống - Hướng dẫn đọc tài liệu	Đọc tài liệu [1], chương 1,2 Đọc tài liệu [3], chương 2	**G1.1-G1.3** **G2.1-G2.3**	**A1.1.1** **A1.2.1** **A1.3.1**
5.	2.7. Hệ mã Hill 2.9 Hệ mã hoán vị	- Vấn đáp gợi mở vấn đề. - Thuyết trình dựa trên slide kết hợp bảng-phấn. - Thảo luận - Hướng dẫn đọc tài liệu	Đọc tài liệu [1], chương 1,2 Đọc tài liệu [3], chương 2	**G1.1-G1.3** **G2.1-G2.3**	**A1.1.1** **A1.2.1** **A1.3.1**
6.	2.10. Đánh giá mức độ bảo mật của một phương pháp mã hóa. 2.11. Bài tập các hệ mã cổ điển	- Vấn đáp gợi mở vấn đề. - Thuyết trình dựa trên slide kết hợp bảng-phấn. - Thảo luận - Hướng dẫn đọc tài liệu - Hướng dẫn làm bài tập	Đọc tài liệu [1], chương 1,2	**G1.1-G1.3** **G2.1-G2.3**	**A1.1.1** **A1.2.1** **A1.3.1**
7.	**Chương 4: Hệ mã hóa đối xứng** 1. Mục đích của mã hóa hiện đại 2. Mã dòng: A5/1, RC4	- Vấn đáp gợi mở vấn đề. - Thuyết trình dựa trên slide kết hợp bảng-phấn. - Thảo luận - Hướng dẫn đọc tài liệu	Đọc tài liệu [1], chương 2 Đọc tài liệu [3], chương 4,5	**G2.1-G2.3** **G5.1-G5.2**	**A1.1.1** **A1.2.1** **A2.2**
8.	3. Mã khối: DES, AES	- Vấn đáp gợi mở vấn đề. - Thuyết	Đọc tài liệu [1], chương 2	**G2.1-G2.3**	**A1.1.1** **A1.2.1**

		trình dựa trên slide kết hợp bảng-phấn. - Thảo luận - Hướng dẫn làm bài tập	Đọc tài liệu [3], chương 4,5	**G5.1-G5.2**	**A2.2**
9.	4. Các chế độ sử dụng mã khối 5.Nhược điểm của mã hóa đối xứng	- Vấn đáp gợi mở vấn đề. - Thuyết trình dựa trên slide kết hợp bảng-phấn. - Thảo luận - Hướng dẫn đọc tài liệu	Đọc tài liệu [1], chương 2 Đọc tài liệu [3], chương 4,5	**G2.1-G2.3** **G5.1-G5.2**	**A1.1.1** **A1.2.1** **A2.2**
10.	**Chương 5: Hệ mã hóa khóa công khai** 1. Nguyên tắc mã hóa khóa công khai 2. Mã hóa RSA 3. Hệ Mã ElGamal	- Vấn đáp gợi mở vấn đề. - Thuyết trình dựa trên slide kết hợp bảng-phấn. - Hướng dẫn đọc tài liệu - Hướng dẫn làm bài tập	Đọc tài liệu [1], chương 3 Đọc tài liệu [2], chương 6	**G2.1-G2.4** **G5.1-G5.2**	**A1.1.1** **A1.2.1** **A2.2**
11.	4. Truyền khóa Diffie-Hellman 5. Ưu nhược điểm của mã hóa khóa công khai	- Vấn đáp gợi mở vấn đề. - Thuyết trình dựa trên slide kết hợp bảng-phấn. - Thảo luận - Hướng dẫn đọc tài liệu - Hướng dẫn làm bài tập	Đọc tài liệu [1], chương 3 Đọc tài liệu [2], chương 6	**G2.1-G2.3** **G5.1-G5.2**	**A1.1.1** **A1.2.1** **A2.1** **A2.2**
12.	**Chương 6: Mã chứng thực thông điệp và hàm băm** 1. Mã chứng thực thông điệp MAC 2. Hàm băm	- Vấn đáp gợi mở vấn đề. - Thuyết trình dựa trên slide kết hợp bảng-phấn. - Hướng dẫn đọc tài liệu - Hướng dẫn làm bài tập	Đọc tài liệu [1], chương 5 Đọc tài liệu [2], chương 9	**G3.1-G3.3** **G4.1-G4.2** **G5.1-G5.2**	**A1.1.1** **A1.2.1** **A2.2**
13.	3. Ứng dụng của hàm băm 4. Chữ ký điện tử RSA	- Vấn đáp gợi mở vấn đề. - Thuyết trình dựa trên slide kết hợp bảng-phấn.	Đọc tài liệu [1], chương 5 Đọc tài liệu [2], chương 9	**G3.1-G3.3** **G4.1-G4.2**	**A1.1.1** **A1.2.1** **A2.2**

		- Hướng dẫn đọc tài liệu - Hướng dẫn làm bài tập		**G5.1-G5.2**	
14.	**Chương 7: Giao thức bảo mật** 6.1 Phát lại thông điệp 6.2 Giao thức bảo mật 6.3 Định danh và trao đổi khóa phiên dùng mã hóa đối xứng với KDC 6.4 Định danh và trao đổi khóa phiên dùng mã hóa khóa công khai	- Vấn đáp gợi mở vấn đề. - Thuyết trình dựa trên slide kết hợp bảng-phấn. - Thảo luận - Hướng dẫn đọc tài liệu	Đọc tài liệu [1], chương 6 Đọc tài liệu [2], chương 5	**G3.1-G3.3** **G4.1-G4.2** **G5.1-G5.2**	**A1.1.1** **A1.2.1** **A2.2**
15.	**Chương 8: Mốt số ứng dụng thực tiễn** 1. Chứng chỉ X509 2. Giao thức SSL/ TSL 3. Giấu tin trong ảnh số 4. Chữ ký mù 5. Tiền ảo Bitcoin 6. Mã hóa ổ đĩa cứng Bit Locker 7. Tấn công SQL Injection	- Thuyết trình dựa trên slide kết hợp bảng-phấn. - Thảo luận - Hướng dẫn đọc tài liệu	Đọc tài liệu [1], chương 8,9,10	**G3.1-G3.3** **G4.1-G4.2** **G5.1-G5.2**	**A1.1.1** **A1.2.1** **A2.2**

7. Nguồn học liệu

Giáo trình:

[1]. Nguyễn Khanh Văn, *Cơ sở an toàn thông tin,* Đại học Bách Khoa, 2014.

Tài liệu tham khảo:

[2]. Man Young Rhee, Wilay, *Internet Security - Cryptographic Principles, Algorithms and Protocols,* 2003.

[3]. PGS.TS Thái Hồng Nhị, TS Phạm Minh Việt, An toàn thông tin , NXB khoa học và kỹ thuật 2008.

8. Quy định của học phần

- Tham gia trên 80% số giờ lên lớp;
- Tham gia đủ số tiết thực hành quy định;
- Phải làm đầy đủ các bài tập theo yêu cầu của giảng viên.

9. Phụ trách học phần

- Bộ môn Hệ thống và Mạng máy tính, Viện Kỹ thuật và Công nghệ

- Địa chỉ: Tầng 1, Nhà A0, Trường Đại học Vinh, 182 Lê Duẩn, Vinh, Nghệ An

- Email: vienktcn.htmmt@vinhuni.edu.vn