HỌC VIỆN KỸ THUẬT QUÂN SỰ
KHOA: CÔNG NGHỆ THÔNG TIN

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập – Tự do – Hạnh phúc

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN
MÃ HÓA - CRYPTOGRAPHY

1. Thông tin về giáo viên

TT	Họ tên giảng viên	Học hàm	Học vị	Đơn vị công tác
1	Nguyễn Hiếu Minh	Tiến sỹ	Phó giáo sư	BM An ninh mạng

Thời gian, địa điểm làm việc: Bộ môn An ninh mạng, Nhà A1, Phòng 1305.
Địa chỉ liên hệ: Nhà 48, Tập thể Thông tin, Trần Cung, Từ Liêm, Hà Nội.
Điện thoại, email: 0989.193571, hieuminhmta@ymail.com.
Các hướng nghiên cứu chính: Mạng máy tính, An ninh mạng, Mật mã.

2. Thông tin chung về học phần

- Tên học phần: Mã hóa.
- Mã học phần:
- Số tín chỉ: 3TC, Số tiết (LT, BT, TL, TH) – (30, 15, 6, 9).
- Học phần (Bắt buộc hay Lựa chọn): Bắt buộc.
- Các học phần tiên quyết: Lập trình cơ bản, Các môn toán.
- Các học phần kế tiếp: An ninh mạng.
- Các yêu cầu đối với học phần (nếu có): Môn học được xây dựng dành cho các sinh viên hệ chính quy quân sự và dân sự hệ đại học.
- Giờ tín chỉ đối với các hoạt động:
  - Nghe giảng lý thuyết: 30 tiết
  - Làm bài tập trên lớp: 15 tiết
  - Thảo luận: 6 tiết
  - Thực hành, thực tập (ở PTN, nhà máy, thực tập...): 9 tiết
  - Hoạt động theo nhóm: 20 tiết
  - Tự học: 60 tiết
- Địa chỉ Khoa/ Bộ môn phụ trách môn học: Khoa Công nghệ Thông tin, Bộ môn An ninh mạng.

3. Mục tiêu của học phần

- Kiến thức: Có kiến thức cơ bản về các kỹ thuật an toàn thông tin, các thuật toán mật mã và các vấn đề liên quan.

- Kỹ năng: Có khả năng đọc hiểu các kiến thức mở rộng của môn học mã hóa thông tin, có khả năng xây dựng và phân tích các chương trình thực hiện các mô hình và thuật toán mật mã.
- Thái độ, chuyên cần: Rèn luyện được thái độ nghiêm túc và có khả năng đọc hiểu và nghiên cứu chuyên sâu trong lĩnh vực mật mã mã và an toàn thông tin.

4. Tóm tắt nội dung học phần

Hướng tới các kiến thức cơ bản và nâng cao trong lĩnh vực lý thuyết mật mã và các phương thức sử dụng các phương pháp mật mã khóa bí mật và công khai để giải quyết các nhiệm vụ bảo vệ an toàn thông tin trong các mạng máy tính và mạng viễn thông.

5. Nội dung chi tiết học phần

Chương, mục, tiểu mục	Nội dung	Số tiết	Giáo trình, Tài liệu tham khảo (Ghi TT của TL ở mục 6)	Ghi chú
I	Các khái niệm cơ bản về mật mã 1. Lịch sử phát triển của mật mã 2. An toàn thông tin và mật mã 3. Các dịch vụ an ninh mạng 4. Các kỹ thuật mật mã cổ điển 5. Thám mã các hệ mật cổ điển	6	1, 2, 3, 5, 6	
II	Cơ sở toán học cho mật mã 1. Lý thuyết Shannon 2. Lý thuyết thông tin 3. Cơ bản về đại số trừu tượng 4. Lý thuyết số	3	1, 3, 5, 6	
III	Các thuật toán mật mã khóa đối xứng 1. Mật mã khối và chuẩn mã hóa dữ liệu (DES) 2. Chuẩn mã hóa dữ liệu nâng cao (AES) 3. Các thuật toán mật mã khối: RC6, MARS, Twofish, SERPENT 4. Mật mã dòng và thuật toán RC4 5. Thám mã vi sai và tuyến tính các thuật toán mật mã khóa đối xứng	6	2, 3, 6	

IV	Các thuật toán mật mã khóa công khai 1. Mật mã khóa công khai và hệ mật RSA 2. Vấn đề logarit rời rạc và hệ mật Elgamal 3. Mật mã trên vành Elliptic 4. Các phương pháp tấn công các hệ mật khóa công khai	6	2, 3, 4, 6	
V	Hàm băm và chữ ký số 1. Mã xác thực bản tin (MAC) 2. Các hàm băm mật mã: MDx, SHAx 3. Lược đồ chữ ký số RSA 4. Lược đồ chữ ký số Elgamal và chuẩn chữ ký số DSS 5. Chuẩn chữ ký số ECDSS 6. Một số đánh giá về các sơ đồ chữ ký số	3	2, 3, 5	
VI	Quản lý khóa trong mật mã 1. Quản lý khóa cho các hệ mật khóa đối xứng 2. Quản lý khóa cho các hệ mật khóa công khai 3. Hạ tầng khóa công khai PKI	3	1, 2, 3, 6	
VII	Các ứng dụng mật mã trong an ninh mạng 1. Các ứng dụng xác thực 2. An toàn thư điện tử 3. An toàn Web	3	2, 3, 4, 5, 6	
	Tổng	30		

6. Giáo trình, tài liệu tham khảo

TT	Tên tài liệu	Tình trạng tài liệu			
		Có trên thư viện	Giáo viên hoặc Khoa có, cho mượn để TV pho tô hoặc có File Điện tử	Đề nghị mua mới	Đề nghị biên soạn mới
1	William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall, 2005.		File điện tử		
2	Wenbo Mao, "Modern Cryptography: Theory and Practice", Prentice Hall, 2004.		File điện tử		

3	Bruce Schneier, "Applied cryptography: protocols, algorithms, and source code in C", John Wiley & Sons, Inc., 1995.		File điện tử		
4	Douglas Stinson, "Cryptography: Theory and Practice", CRC Press, CRC Press LLC ISBN: 0849385210, Pub Date: 03/17/95.		File điện tử		
5	Peter Thorsteinson, G. Gnana Arun Ganesh, ".NET Security and Cryptography", Prentice Hall PTR, 2003.		File điện tử		
6	Hans Delfs, Helmut Knebl, "Introduction to Cryptography, Principles and Applications", Springer-Verlag Berlin Heidelberg 2007.		File điện tử		

7. Hình thức tổ chức dạy học

7.1. Lịch trình chung: (Ghi tổng số giờ cho mỗi cột)

Nội dung	Hình thức tổ chức dạy học môn học					Tổng
	Lên lớp			Thực hành, thí nghiệm, thực tập...	Tự học, tự nghiên cứu	
	Lý thuyết	Bài tập	Thảo luận			
Chương I	6	2	1		8	17
Chương II	3	2	1	3	8	17
Chương III	6	2	1	3	8	20
Chương IV	6	2	1	3	8	20
Chương V	3	2	1		8	14
Chương VI	3	2	1		8	14
Chương VII	3	3			12	18

7.2. Lịch trình tổ chức dạy học cụ thể

<u>Bài giảng 1</u>: Các khái niệm cơ bản về mật mã

Chương I Mục 1 + 2 + 3

Tiết thứ: 1 - 4 Tuần thứ: 1

- Mục đích, yêu cầu:

- Nắm sơ lược về Học phần, các chính sách riêng của giáo viên, địa chỉ giáo viên, bầu lớp trưởng Học phần.
- Nắm được khái niệm về lịch sử phát triển của mật mã, tổng quan về mật mã;
- Nắm được vai trò của mật mã trong lĩnh vực an toàn thông tin;

- Hình thức tổ chức dạy học: Lý thuyết, thảo luận, tự học, tự nghiên cứu

- ***Thời gian*****:** Lý thuyết, thảo luận: 4t; Tự học, tự nghiên cứu: 4t
- ***Địa điểm*****:** Giảng đường do P2 phân công.
- ***Nội dung chính*****:**

1. Mục đích yêu cầu của môn học

2. Các nội dung chính của môn học

3. Lịch sử phát triển của mật mã

4. An toàn thông tin và mật mã

5. Các dịch vụ an ninh mạng

- Yêu cầu SV chuẩn bị**:**

Đọc trước TL[1]: chương 1.

Tự đọc: Ví dụ cuối chương 1.

<u>Bài giảng 2</u>: Các khái niệm cơ bản về mật mã

Chương I Mục 4 + 5

Tiết thứ: 5 - 8 Tuần thứ: 2

- ***Mục đích, yêu cầu***:
  - Nắm được kiến thức về một số hệ mật cổ điển;
  - Nắm được kiến thức về một số phương pháp thám mã hệ mật cổ điển;
  - Xây dựng được chương trình (demo) một số hệ mật cổ điển.
- ***Hình thức tổ chức dạy học***: Lý thuyết, bài tập, tự học, tự nghiên cứu
- ***Thời gian*****:** Lý thuyết, bài tập: 4t; Tự học, tự nghiên cứu: 4t
- ***Địa điểm*****:** Giảng đường do P2 phân công.
- ***Nội dung chính*****:**

1. Một số hệ mật cổ điển.

2. Thám mã một số hệ mật cổ điển.

3. Xây dựng chương trình demo.

- Yêu cầu SV chuẩn bị**:**

Đọc trước TL[1]: chương 2. Đọc trước TL[4]: chương 1.

Tự đọc: Ví dụ cuối chương 1 của TL [4].

<u>Bài tập về nhà cho Chương I</u>: Cuối chương 1 của TL [4].

Bài giảng 3: Cơ sở toán học cho mật mã

Chương II Mục 1 + 2 + 3 + 4

Tiết thứ: 9 - 12 Tuần thứ: 3

- ***Mục đích, yêu cầu***:
  - Nắm được kiến thức về Lý thuyết Shannon;
  - Nắm được kiến thức về Lý thuyết thông tin;
  - Nắm được kiến thức về Cơ bản về đại số trừu tượng;
  - Nắm được kiến thức về Lý thuyết số;
  - Xây dựng chương trình demo.
- ***Hình thức tổ chức dạy học***: Lý thuyết, bài tập, tự học, tự nghiên cứu
- ***Thời gian*****:** Lý thuyết, bài tập: 4t; Tự học, tự nghiên cứu: 4t
- ***Địa điểm*****:** Giảng đường do P2 phân công.
- ***Nội dung chính*****:**
  1. Lý thuyết Shannon
  2. Lý thuyết thông tin
  3. Cơ bản về đại số trừu tượng
  4. Lý thuyết số.

- Yêu cầu SV chuẩn bị**:**

Đọc trước TL[1]: chương 4. Đọc trước TL[4]: chương 2. Đọc trước TL[2]: chương 3,4,5,6.

Tự đọc: Ví dụ cuối chương 3,4,5,6 của TL [2].

Bài tập về nhà cho Chương II: Cuối chương 3,4,5,6 của TL [2].

Bài giảng 4: Các thuật toán mật mã khóa đối xứng

Chương III Mục 1 + 2

Tiết thứ: 13 - 16 Tuần thứ: 4

- ***Mục đích, yêu cầu***:
  - Nghiên cứu về Mật mã khối và chuẩn mã hóa dữ liệu (DES)
  - Nghiên cứu về Chuẩn mã hóa dữ liệu nâng cao (AES)
  - Xây dựng chương trình demo.
- ***Hình thức tổ chức dạy học***: Lý thuyết, bài tập, tự học, tự nghiên cứu

- ***Thời gian*****:** Lý thuyết, bài tập: 4t; Tự học, tự nghiên cứu: 4t

- ***Địa điểm*****:** Giảng đường do P2 phân công.

- ***Nội dung chính*****:**

1. Mật mã khối và chuẩn mã hóa dữ liệu (DES)

2. Chuẩn mã hóa dữ liệu nâng cao (AES).

- Yêu cầu SV chuẩn bị**:**

Đọc trước TL[1]: chương 3,4,5. Đọc trước TL[4]: chương 3. Đọc trước TL[2]: chương 7.

Tự đọc: Ví dụ cuối chương 7 của TL [2].

Bài tập về nhà cho Chương III: Cuối chương 7 của TL [2].

Bài giảng 5: Các thuật toán mật mã khóa đối xứng

Chương III Mục 3 + 4 + 5

Tiết thứ: 17 - 20 Tuần thứ: 5

- ***Mục đích, yêu cầu***:

- Tìm hiểu về Các thuật toán mật mã khối: RC6, MARS, Twofish, SERPENT
- Tìm hiểu về Mật mã dòng và thuật toán RC4
- Tìm hiểu về Thám mã vi sai và tuyến tính các thuật toán mật mã khóa đối xứng
- Xây dựng chương trình demo.

- ***Hình thức tổ chức dạy học***: Lý thuyết, bài tập, tự học, tự nghiên cứu

- ***Thời gian*****:** Lý thuyết, bài tập: 4t; Tự học, tự nghiên cứu: 4t

- ***Địa điểm*****:** Giảng đường do P2 phân công.

- ***Nội dung chính*****:**

1. Tìm hiểu về Các thuật toán mật mã khối: RC6, MARS, Twofish, SERPENT

2. Tìm hiểu về Mật mã dòng và thuật toán RC4

3. Tìm hiểu về Thám mã vi sai và tuyến tính các thuật toán mật mã khóa đối xứng

4. Xây dựng chương trình demo.

- Yêu cầu SV chuẩn bị**:**

Đọc trước TL[1]: chương 5,6. Đọc trước TL[2]: chương 7.

Tự đọc: Ví dụ cuối chương 7 của TL [2].

Bài tập về nhà cho Chương III: Cuối chương 7 của TL [2].

Bài giảng 6: Các thuật toán mật mã khóa công khai

Chương IV Mục 1 + 2

Tiết thứ: 21 - 24 Tuần thứ: 6

- ***Mục đích, yêu cầu***:
  - Nghiên cứu về Mật mã khóa công khai và hệ mật RSA
  - Nghiên cứu về Vấn đề logarit rời rạc và hệ mật Elgamal
  - Xây dựng chương trình demo.
- ***Hình thức tổ chức dạy học***: Lý thuyết, bài tập, tự học, tự nghiên cứu
- ***Thời gian*****:** Lý thuyết, bài tập: 4t; Tự học, tự nghiên cứu: 4t
- ***Địa điểm*****:** Giảng đường do P2 phân công.
- ***Nội dung chính*****:**

1. Nghiên cứu về Mật mã khóa công khai và hệ mật RSA

2. Nghiên cứu về Vấn đề logarit rời rạc và hệ mật Elgamal

3. Xây dựng chương trình demo.

- Yêu cầu SV chuẩn bị**:**

Đọc trước TL[1]: chương 8,9. Đọc trước TL[2]: chương 8. Đọc trước TL[4]: chương 4,5.

Tự đọc: Ví dụ cuối chương 8 của TL [2]. Ví dụ cuối chương 4,5 của TL [4]

Bài tập về nhà cho Chương IV: Cuối chương 8 của TL [2]. Cuối chương 4,5 của TL [4].

Bài giảng 7: Các thuật toán mật mã khóa công khai

Chương IV Mục 3 + 4

Tiết thứ: 25 - 28 Tuần thứ: 7

- ***Mục đích, yêu cầu***:
  - Nghiên cứu về Mật mã trên vành Elliptic
  - Các phương pháp tấn công các hệ mật khóa công khai
  - Xây dựng chương trình demo.
- ***Hình thức tổ chức dạy học***: Lý thuyết, bài tập, tự học, tự nghiên cứu
- ***Thời gian*****:** Lý thuyết, bài tập: 4t; Tự học, tự nghiên cứu: 4t
- ***Địa điểm*****:** Giảng đường do P2 phân công.

***- Nội dung chính*:**

1. Mật mã trên vành Elliptic

2. Các phương pháp tấn công các hệ mật khóa công khai

3. Xây dựng chương trình demo.

***- Yêu cầu SV chuẩn bị*:**

Đọc trước TL[1]: chương 9,10. Đọc trước TL[2]: chương 5. Đọc trước TL[4]: chương 4,5.

Tự đọc: Ví dụ cuối chương 5 của TL [2]. Ví dụ cuối chương 4,5 của TL [4]

Bài tập về nhà cho Chương IV: Cuối chương 8 của TL [2]. Cuối chương 4,5 của TL [4].

Bài giảng 8: Hàm băm và chữ ký số

Chương V Mục 1 - 7

Tiết thứ: 29 - 32 Tuần thứ: 8

***- Mục đích, yêu cầu*:**

- Nghiên cứu về Mã xác thực bản tin (MAC)
- Nghiên cứu về Các hàm băm mật mã: MDx, SHAx
- Nghiên cứu về Lược đồ chữ ký số RSA
- Nghiên cứu về Lược đồ chữ ký số Elgamal và chuẩn chữ ký số DSS
- Nghiên cứu về Chuẩn chữ ký số ECDSS
- Nghiên cứu về Một số đánh giá về các sơ đồ chữ ký số.

- Hình thức tổ chức dạy học: Lý thuyết, bài tập, tự học, tự nghiên cứu

***- Thời gian*:** Lý thuyết, bài tập: 4t; Tự học, tự nghiên cứu: 4t

***- Địa điểm*:** Giảng đường do P2 phân công.

***- Nội dung chính*:**

1. Mã xác thực bản tin (MAC)

2. Các hàm băm mật mã: MDx, SHAx

3. Lược đồ chữ ký số RSA

4. Lược đồ chữ ký số Elgamal và chuẩn chữ ký số DSS

5. Chuẩn chữ ký số ECDSS

6. Một số đánh giá về các sơ đồ chữ ký số.

7. Xây dựng chương trình demo.

***- Yêu cầu SV chuẩn bị*:**

Đọc trước TL[1]: chương 11,12,13. Đọc trước TL[2]: chương 10. Đọc trước TL[4]: chương 6,7.

Tự đọc: Ví dụ cuối chương 10 của TL [2]. Ví dụ cuối chương 6,7 của TL [4]

Bài tập về nhà cho Chương V: Cuối chương 10 của TL [2]. Cuối chương 6,7 của TL [4].

Bài giảng 9: Quản lý khóa trong mật mã

Chương VI Mục 1 - 3

Tiết thứ: 33 - 36 Tuần thứ: 9

- Mục đích, yêu cầu:

- Nghiên cứu về Quản lý khóa cho các hệ mật khóa đối xứng
- Nghiên cứu về Quản lý khóa cho các hệ mật khóa công khai
- Nghiên cứu về Hạ tầng khóa công khai PKI.

- Hình thức tổ chức dạy học: Lý thuyết, bài tập, tự học, tự nghiên cứu

***- Thời gian*:** Lý thuyết, bài tập: 4t; Tự học, tự nghiên cứu: 4t

***- Địa điểm*:** Giảng đường do P2 phân công.

***- Nội dung chính*:**

1. Quản lý khóa cho các hệ mật khóa đối xứng
2. Quản lý khóa cho các hệ mật khóa công khai
3. Hạ tầng khóa công khai PKI.
4. Chương trình demo

***- Yêu cầu SV chuẩn bị*:**

Đọc trước TL[1]: chương 10. Đọc trước TL[2]: chương 11,12,13. Đọc trước TL[4]: chương 8.

Tự đọc: Ví dụ cuối chương 11,12,13 của TL [2]. Ví dụ cuối chương 8 của TL [4]

Bài tập về nhà cho Chương VI: Cuối chương 11,12,13 của TL [2]. Cuối chương 8 của TL [4].

Bài giảng 10: Các ứng dụng mật mã trong an ninh mạng

Chương VII Mục 1 - 3

Tiết thứ: 37 - 40 Tuần thứ: 10

- Mục đích, yêu cầu:

- Nghiên cứu về Các ứng dụng xác thực
- Nghiên cứu về An toàn thư điện tử
- Nghiên cứu về An toàn Web.

- Hình thức tổ chức dạy học: Lý thuyết, bài tập, tự học, tự nghiên cứu

- Thời gian**:** Lý thuyết, bài tập: 4t; Tự học, tự nghiên cứu: 4t

- Địa điểm**:** Giảng đường do P2 phân công.

- Nội dung chính**:**

1. Các ứng dụng xác thực

2. An toàn thư điện tử

3. An toàn Web.

4. Chương trình demo

- Yêu cầu SV chuẩn bị**:**

Đọc trước TL[1]: chương 14,15,17.

Tự đọc: Ví dụ cuối chương 14,15,17 của TL [1].

Bài tập về nhà cho Chương VII: Cuối chương 14,15,17 của TL [1].

Bài giảng 11: Tổng hợp bài tập các chương

Chương VIII Mục 1 – 5

Tiết thứ: 41 – 44 Tuần thứ: 11

- Mục đích, yêu cầu:

- Hoàn thành một số bài tập mật mã cổ điển.
- Hoàn thành một số bài tập mật mã khóa đối xứng.
- Hoàn thành một số bài tập mật mã khóa công khai.
- Hoàn thành một số bài tập hàm băm và chữ ký số.
- Hoàn thành một số bài tập về ứng dụng mật mã.

- Hình thức tổ chức dạy học: Bài tập, tự học, tự nghiên cứu

- Thời gian**:** Lý thuyết, bài tập: 4t; Tự học, tự nghiên cứu: 4t

- Địa điểm**:** Giảng đường do P2 phân công.

- Nội dung chính**:**

1. Bài tập mật mã cổ điển.

2. Bài tập mật mã khóa đối xứng.

3. Bài tập mật mã khóa công khai.

4. Bài tập hàm băm và chữ ký số.

5. Bài tập một số ứng dụng mật mã.

***- Yêu cầu SV chuẩn bị*:**

Đọc trước TL[1], Đọc trước TL[2], Đọc trước TL[4], Đọc trước TL[3],.

Tự đọc: Ví dụ cuối chương của TL [1,2,3,4].

Bài tập về nhà cho Chương VIII: Cuối chương của TL [1,2,3,4].

Bài giảng 12: Thảo luận các nội dung đã học

Chương IX Mục 1 – 4

Tiết thứ: 45 – 48 Tuần thứ: 12

- Mục đích, yêu cầu:

- Thảo luận về Cơ sở toán học.
- Thảo luận về Mật mã khóa đối xứng.
- Thảo luận về Mật mã khóa công khai.
- Thảo luận về Hàm băm và chữ ký số.

- Hình thức tổ chức dạy học: Thảo luận, tự học, tự nghiên cứu

***- Thời gian*:** Thảo luận: 4t; Tự học, tự nghiên cứu: 4t

***- Địa điểm*:** Giảng đường do P2 phân công.

***- Nội dung chính*:**

1. Cơ sở toán học.

2. Mật mã khóa đối xứng.

3. Mật mã khóa công khai.

4. Hàm băm và chữ ký số.

***- Yêu cầu SV chuẩn bị*:**

Đọc trước TL[1], Đọc trước TL[2], Đọc trước TL[4], Đọc trước TL[3].

Tự đọc: Ví dụ cuối chương của TL [1,2,3,4].

Bài tập về nhà cho Chương IX: Cuối chương của TL [1,2,3,4].

Bài giảng 13: Thảo luận các nội dung đã học

Chương IX Mục 1 – 2

Tiết thứ: 49 – 52 Tuần thứ: 13

- Mục đích, yêu cầu:

- Thảo luận về Quản lý khóa trong mật mã.
- Thảo luận về Một số ứng dụng của mật mã

- Hình thức tổ chức dạy học: Lý thuyết, bài tập, tự học, tự nghiên cứu

***- Thời gian*:** Thảo luận: 4t; Tự học, tự nghiên cứu: 4t

***- Địa điểm*:** Giảng đường do P2 phân công.

***- Nội dung chính*:**

1. Quản lý khóa trong mật mã.

2. Một số ứng dụng của mật mã.

***- Yêu cầu SV chuẩn bị*:**

Đọc trước TL[1], Đọc trước TL[2], Đọc trước TL[4], Đọc trước TL[3].

Tự đọc: Ví dụ cuối chương của TL [1,2,3,4].

Bài tập về nhà cho Chương IX: Cuối chương của TL [1,2,3,4,5,6].

Bài giảng 14: Thực hành các nội dung đã học

Chương X Mục 1 – 2

Tiết thứ: 53 – 56 Tuần thứ: 14

- Mục đích, yêu cầu:

- Thử nghiệm các thuật toán mật mã cổ điển.
- Thử nghiệm các thuật toán mật mã khóa đối xứng.

- Hình thức tổ chức dạy học: Thực hành, tự học, tự nghiên cứu

***- Thời gian*:** Thực hành: 4t; Tự học, tự nghiên cứu: 4t

***- Địa điểm*:** Tại PTN An ninh mạng.

***- Nội dung chính*:**

1. Thử nghiệm các thuật toán mật mã cổ điển.

2. Thử nghiệm các thuật toán mật mã khóa đối xứng.

***- Yêu cầu SV chuẩn bị*:**

Đọc trước TL[1], Đọc trước TL[2], Đọc trước TL[4], Đọc trước TL[3].

Tự đọc: Ví dụ cuối chương của TL [1,2,3,4].

Bài tập về nhà cho Chương X: Cuối chương của TL [1,2,3,4,5,6].

<u>Bài giảng 15</u>: Thực hành các nội dung đã học

Chương X Mục 1 – 2

Tiết thứ: 57 – 60 Tuần thứ: 15

- Mục đích, yêu cầu:

- Thử nghiệm các thuật toán mật mã khóa công khai.
- Thử nghiệm các thuật toán hàm băm và chữ ký số.

- Hình thức tổ chức dạy học: Thực hành, tự học, tự nghiên cứu

***- Thời gian*:** Thực hành: 4t; Tự học, tự nghiên cứu: 4t

***- Địa điểm*:** Tại PTN An ninh mạng.

***- Nội dung chính*:**

1. Thử nghiệm các thuật toán mật mã khóa công khai.

2. Thử nghiệm các thuật toán hàm băm và chữ ký số.

***- Yêu cầu SV chuẩn bị*:**

Đọc trước TL[1], Đọc trước TL[2], Đọc trước TL[4], Đọc trước TL[3].

Tự đọc: Ví dụ cuối chương của TL [1,2,3,4].

<u>Bài tập về nhà cho Chương X</u>: Cuối chương của TL [1,2,3,4,5,6].

8. Chính sách đối với học phần và các yêu cầu khác của giáo viên

Sinh viên cần có mặt tại lớp đủ số tiết theo yêu cầu, tích cực tham gia thảo luận, tham gia các hoạt động giáo viên tổ chức.

Chuẩn bị bài tốt trước khi tới lớp học.

Thực hiện tốt các bài tập giáo viên giao về nhà: nộp bài đúng hạn, chất lượng từ trung bình trở lên.

Tham gia bài thi hết môn.

- Bài tập học phần (làm theo nhóm)
  - Trình bày tổng quan về cơ sở lý thuyết: 30%
  - Các phân tích,đánh giá chuyên sâu: 30%
  - Phần chương trình: 30%
  - Trình bày khoa học, nộp bài đúng hạn: 10%

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

9.1. Kiểm tra – đánh giá thường xuyên

Thường xuyên điểm danh vào thời điểm thích hợp.

9.2. Kiểm tra - đánh giá định kì

- Tham gia học tập trên lớp (đi học đầy đủ, chuẩn bị bài tốt và tích cực thảo luận,…): *Hệ số 0.1*.
- Hoàn thành tốt Bài tập về nhà, Kiểm tra giữa kì: *Hệ số 0.2*.
- Thi kết thúc học phần tốt: *Hệ số 0.7*.

Chủ nhiệm Khoa	**Chủ nhiệm Bộ môn**	**Giảng viên biên soạn**
(Ký và ghi rõ họ tên)	*(Ký và ghi rõ họ tên)*	*(Ký và ghi rõ họ tên)*
PGS.TS. Đào Thanh Tĩnh	PGS.TS. Nguyễn Hiếu Minh	PGS. TS.Nguyễn Hiếu Minh