ET3310 Lý thuyết mật mã

1. Tên học phần: Lý thuyết mật mã

2. Mã số: ET3310

3. Khối lượng: *3(3-1-1-6)*

- Lý thuyết: 45 tiết
- BTL: 5
- Thí nghiệm: 15 (x bài x y tiết)

4. Đối tượng tham dự: Sinh viên đại học các ngành Điện tử – Viễn thông từ học kỳ 4

5. Điều kiện học phần:

- Học phần tiên quyết:
- Học phần học trước:
- Học phần song hành:

6. Mục tiêu học phần và kết quả mong đợi

Môn học nhằm trang bị cho sinh viên các kiến thức cơ bản về mã hóa đảm bảo an toàn và bảo mật thông tin. Môn học tập trung vào các phương pháp mã hóa khóa đối xứng; Phương pháp mã hóa khóa công khai; Các hệ mật mã dòng và vấn đề tạo dãy giả ngẫu nhiên; Lược đồ chữ ký số Elgamal và chuẩn chữ ký số ECDSA; Độ phức tạp xử lý và độ phức tạp dữ liệu của một tấn công cụ thể vào hệ thống mật mã; Đặc trưng an toàn của phương thức mã hóa; Thám mã tuyến tính, thám mã vi sai và các vấn đề về xây dựng hệ mã bảo mật cho các ứng dụng. Cung cấp các kiến thức cần thiết để sinh viên có thể tiếp tục nghiên cứu sâu hơn về các thuật toán mật mã và ứng dụng trong thực tiễn.

Sau khi hoàn thành học phần này, yêu cầu sinh viên có khả năng:

- Có các kiến thức cơ bản về các phương pháp mã hóa khóa đối xứng, khóa công khai, mã dòng, xác thực và hàm băm, chữ ký số.
- Nắm được một số vấn đề quan trọng trong các dịch vụ an toàn thông tin như xác thực và đảm bảo tính toàn vẹn.
- Nắm được các thủ tục ứng dụng trong thực tế như chữ ký số, trao đổi và phân phối khoá.

Mức độ đóng góp cho các tiêu chí đầu ra của chương trình đào tạo: *<Xác định theo 3 loại: GT (chỉ giới thiệu), GD (giảng dạy) hoặc SD (yêu cầu SV sử dụng, rèn luyện) để đáp ứng với những tiêu chí con trong chuẩn đầu ra của chương trình đào tạo>*

Tiêu chí	1.1	1.2	1.3	2.1	2.2	2.3	2.4	2.5	2.6	3.1	3.2	3.3	4.1	4.2	4.3	4.4	4.5
Mức độ	GD	GT		SD	GD	SD								GT	GT	GT	GT

7. Nội dung vắn tắt học phần:

Học phần trình bày phương pháp mã hóa khóa đối xứng, phương pháp mã hóa khóa công khai, các hệ mật mã dòng và vấn đề tạo dãy giả ngẫu nhiên, lược đồ chữ ký số Elgamal và chuẩn chữ ký số ECDSA, độ phức tạp xử lý và độ phức tạp dữ liệu của một tấn công cụ thể vào hệ thống mật mã; đặc trưng an toàn của phương thức mã hóa, thám mã tuyến tính, thám mã vi sai và các vấn đề về xây dựng hệ mã bảo mật cho các ứng dụng.

8. Tài liệu học tập:

- Sách giáo trình: Lý thuyết bảo mật thông tin

- Bài giảng: slides bài giảng
- Sách tham khảo:
  1. A. J. Menezes, P. C. Van Oorschot, S. A. Vanstone, *Handbook of applied cryptography*, CRC Press 1998.
  2. B. Schneier*, Applied Cryptography*. John Wiley Press 1996.
  3. M. R. A. Huth*, Secure Communicating Systems*, Cambridge University Press 2001.
  4. W. Stallings*, Network Security Essentials*, *Applications and Standards,* Prentice Hall. 2000.

9. Phương pháp học tập và nhiệm vụ của sinh viên:

- Sinh viên cần ôn tập lại các kiến thức về xác suất thống kê, cơ sở mạng thông tin, mạng máy tính.
- Sinh viên cần làm bài tập sau mỗi chương, đọc thêm sách tham khảo, thực hiện các thí nghiệm trong nội dung học phần.

10. Đánh giá kết quả:

- Điểm quá trình sẽ được đánh giá bằng kiểm tra giữa kỳ
- Kết quả cuối kỳ được đánh giá bằng bài thi cuối kỳ dưới dạng tự luận và trắc nghiệm, bao gồm lý thuyết và bài tập

11. Nội dung và kế hoạch học tập cụ thể

Tuần	Nội dung	Giáo trình	BT, TN
1	**Chương 1. Tổng quan** 1.1. Giới thiệu chung về các hệ thống mật mã 1.1.1. Khái niệm, mô hình của hệ thống mật mã 1.1.2. Phân loại các hệ thống mật mã 1.1.3. Một số hệ thống mật mã ban đầu 1.1.4. Những cách thức tấn công vào một hệ thống mật mã 1.2. Tính bí mật của các hệ thống mật mã 1.3. Cơ sở toán học	Chương 1	<Thông tin về bài tập, thí nghiệm và các hoạt động khác SV cần thực hiện>
2	**Chương 2. Mã hóa khóa đối xứng** 2.1. Hệ thống mã hóa quy ước 2.2. Mật mã thay thế 2.2.1.Phương pháp mã hóa dịch chuyển (Mật mã dịch vòng) 2.2.2. Phương pháp mã hóa thay thế 2.2.3. Phương pháp mật mã Vigenère 2.3. Phương pháp mật mã hoán vị	Chương 2	
3	2.4. Phương pháp mật mã Hill 2.5. Phương pháp Affine 2.6. Các hệ mật mã tích	Chương 2	
4	2.8. Chuẩn mã dữ liệu - Phương pháp DES 2.9. Phương pháp chuẩn mã hóa nâng cao AES	Chương 2	

5	**Chương 3. Mã hóa khóa công khai** 3.1. Giới thiệu 3.2. Phân tích thừa số và hệ mật RSA	Chương 3	
6	3.3. Hệ mật Rabin 3.4. Logarit rời rạc và hệ mật Elgamal	Chương 3	
7	3.5. Bài toán sửa sai và hệ mật McEliece 3.6. Bài toán xếp ba lô và hệ mật Merkle-Hellman	Chương 3	
8	3.7. Mật mã trên vành Elliptic Kiểm tra giữa kỳ	Chương 3	
9	**Chương 4. Hàm băm và chữ ký số** 4.1. Giới thiệu 4.2. Mã xác thực bản tin 4.3. Các hàm băm MDx và SHAx	Chương 4	
10	4.4. Lược đồ chữ ký số RSA 4.5. Lược đồ chữ ký số Elgamal và chuẩn chữ ký số DSS 4.6. Chuẩn chữ ký số ECDSA	Chương 4	
11	**Chương 5. Dãy giả ngẫu nhiên và hệ mã dòng** 5.1. Giới thiệu 5.2. Thanh ghi dịch hồi tiếp	Chương 5	
12	5.3. Mã dòng dựa trên LFSR 5.4. Các hệ mã dòng khác	Chương 5	
13	**Chương 6. Kỹ thuật quản lý khóa** 6.1. Giới thiệu 6.2. Phân phối khoá cho các mật mã khóa bí mật	Chương 6	
14	6.3. Phân phối khoá cho mã hóa khóa công khai 6.4. Phân phối khóa bí mật sử dụng mã hóa khóa công khai	Chương 6	
15	6.5. Hạ tầng khóa công khai (PKI) Ôn tập	Chương 6	

12. Nội dung các bài thí nghiệm

TN1: < Xây dựng một số hệ mật khóa bí mật >

TN2: < Xây dựng một số hệ mật khóa công khai >

TN3: < Áp dụng hàm băm trong các dịch vụ an toàn thông , và một số ứng dụng trong thực tế như chữ ký số, trao đổi khóa và phân phối khóa >

13. Bài tập dài

Sinh viên/học viên được yêu cầu tiếp cận các dự án mã nguồn mở để về các công nghệ mới để học tập, cài đặt, cấu hình, vận hành phần mềm an toàn thông tin. Nội dung các bài tập dài được cập nhật từng học kỳ theo sự phát triển công nghệ. Các chủ đề bài tập liên quan đến xây dựng các

phương thức mã hóa, xác thực thông tin, xây dựng các công cụ toán học phục vụ mã hóa, đảm bảo an toàn và xác thực trong mạng thế hệ sau NGN, các phương pháp mã hóa bảo mật đường truyền vật lý,…

NHÓM BIÊN SOẠN ĐỀ CƯƠNG

(Họ tên và chữ ký)

Bộ môn Điện tử Hàng không Vũ trụ

Ngày ….. tháng …… năm ….

CHỦ TỊCH HỘI ĐỒNG KH&ĐT

VIỆN ĐIỆN TỬ - VIỄN THÔNG

(Họ tên và chữ ký)