|  |  |
| --- | --- |
| TRƯỜNG ĐẠI HỌC HẠ LONG | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM** |
| **KHOA CÔNG NGHỆ THÔNG TIN** |  **Độc lập - Tự do - Hạnh phúc** |

**CHƯƠNG TRÌNH GIÁO DỤC ĐẠI HỌC**

**Trình độ đào tạo: Đại học**

**Ngành: Khoa học máy tính**

**ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN**

**AN TOÀN VÀ AN NINH MẠNG**

**1. Tên học phần**: AN TOÀN VÀ AN NINH MẠNG

**2. Mã học phần**: IT3.35

**3. Số tín chỉ**: **3** **Học phần**: *Tự chọn*

Lý thuyết: 45 tiết

Tự học: 90 giờ

**4. Phân bố thời gian**

Thời điểm thực hiện: Học kỳ 7

Số tiết/ tuần: 3 tiết

Tổng số tuần: 15 tuần

**5. Bộ môn/ Khoa phụ trách**: Khoa Công nghệ thông tin

**6. Điều kiện ràng buộc**: Mạng máy tính (1)

**7. Mô tả học phần**

Học phần An toàn và an ninh mạng là học phần tự chọn, nằm trong khối kiến thức giáo dục chuyên nghiệp, phần kiến thức chuyên sâu của ngành. Học phần có 7 đơn vị kiến thức, giới thiệu các nguyên tắc cơ bản của an ninh mạng, trong đó chú trọng vào các phương pháp và chuẩn công nghệ đã được sử dụng rộng rãi để đảm bảo an toàn cho các dữ liệu truyền trên mạng. Cụ thể: Chương đầu giới thiệu chung về học phần. Chương 2 và chương 3 trình bày các giải thuật và giao thức mật mã học cơ sở như mật mã đối xứng và khóa công khai, xác thực thông báo, hàm băm, và chữ ký số. Từ chương 4 đến chương 7 giới thiệu các nội dung chính về các ứng dụng và chuẩn an ninh mạng quan trọng như hệ thống xác thực người dùng Kerberos, chứng thực khóa công khai X.509, chuẩn an ninh giao vận SSL/TLS, giao thức truyền thông an toàn SSH, chương trình an ninh thư điện tử PGP, chuẩn an ninh thư điện tử S/MIME, và tính năng an ninh IP.

**8. Mục tiêu học phần**

Học phần này nhằm trang bị cho sinh viên:

*8.1. Về kiến thức*:

- Trình bày được các khái niệm an toàn thông tin và các nguyên lý của mật mã học, chuẩn an ninh IP.

- Nêu được các giải thuật mã hóa đối xứng quan trọng nhất và các phương thức mã hóa thông báo, các giải thuật khóa công khai được sử dụng rộng rãi nhất, các phương pháp an ninh thư điện tử đang được sử dụng rộng rãi.

- Nêu được các khía cạnh của chức năng xác thực thông báo, các kỹ thuật phân phối khóa và ứng dụng xác thực người dùng tiêu biểu, các phương pháp an ninh chuẩn hóa ở tầng giao vận. Phát hiện và phân tích các điểm nhạy cảm trong các giao thức mạng.

*8.2. Về kỹ năng*:

- Sử dụng từ vựng và thuật ngữ chính xác trong lĩnh vực an ninh mạng.

- Vận dụng được các phương pháp mật mã học để thiết kế các giao thức và dịch vụ mạng an toàn.

- Chọn lựa được các cơ chế thích hợp để bảo vệ an ninh của các hệ thống truyền thông khi cần thiết.

- Sử dụng được các công cụ phần mềm để xem xét các chi tiết hoạt động bên trong của các giao thức, khảo sát hiện trạng và đảm bảo an toàn cho các trao đổi qua mạng khỏi các tấn công tiềm tàng.

*8.3. Về năng lực tự chủ và trách nhiệm*

Tự học và phát triển kỹ năng phù hợp để có thể tham gia vào các dự án về an toàn và an ninh mạng.

**9. Nhiệm vụ của sinh viên**

*9.1. Nhiệm vụ*

- Nghiên cứu trước giáo trình, chuẩn bị các ý kiến hỏi, đề xuất khi nghe giảng;

- Sưu tầm, nghiên cứu các tài liệu có liên quan đến nội dung của từng phần, từng chương, mục hay chuyên đề theo sự hướng dẫn của giảng viên;

- Tham dự đầy đủ các giờ giảng của giảng viên và các buổi tổ chức thảo luận dưới sự hướng dẫn và điều khiển của giảng viên theo quy chế.

*9.2. Nội dung cần đạt*

 - Kiến thức:

 + Nắm vững các khái niệm về an ninh truyền thông và an ninh truyền thống, chuẩn an ninh IP.

 + Hiểu được các giải thuật và giao thức mã hóa khối đối xứng, mật mã khóa công khai và các kỹ thuật quản lý khóa.

 - Kĩ năng:

 + Phân tích phát hiện các yếu điểm của hệ thống mạng và các hiểm họa tấn công.

 + Áp dụng các kỹ thuật căn bản đảm bảo an ninh truyền thông và an ninh hệ thống trong các tình huống cần thiết.

 - Thái độ:

+ Tích cực tìm hiểu và tự tạo cơ hội vận dụng các quản trị mạng.

**10. Tài liệu tham khảo**

[1]. Hồ Văn Canh, Lê Danh Cường, *Mật mã và an toàn thông tin lý thuyết và ứng dụng*, NXB Thông tin và truyền thông, 2014.

[2]. Lê Văn Phùng, *An toàn thông tin*, NXB Thông tin và truyền thông, 2014.

[3]. Hồ Văn Canh, Nguyễn Viết Thế, *Nhập môn Phân tích thông tin có bảo mật*, NXB Thông tin và truyền thông, 2013.

[4]. Nguyễn Phạm Anh Dũng, *An ninh trong các hệ thống thông tin di động*, NXB Thông tin và truyền thông, 2012.

**11. Trang, thiết bị dạy - học**: Máy tính, máy chiếu.

**12. Tiêu chuẩn đánh giá sinh viên**

Theo Điều 10, Điều 19, Điều 21, Điều 22 của Quy chế đào tạo đại học và cao đẳng chính quy theo hệ thống tín chỉ ban hành kèm theo Quyết định số 43/2007/QĐ- BGDĐT, ngày 15 tháng 8 năm 2007 của Bộ trưởng Bộ Giáo dục và Đào tạo, sinh viên tham dự học mỗi học phần được đánh giá loại đạt nếu:

- Có đăng ký học học phần đúng thời hạn và đảm bảo điều kiện tiên quyết vào đầu môi học kỳ với phòng Đào tạo nhà trường.

- Tích cực tham dự lớp học, hoàn thành đầy đủ các điểm đánh giá bộ phận (Ai) và điểm kết thúc học phần (ĐKTHP). Sinh viên vắng mặt không có lý do chính đáng trong buổi kiếm tra đánh giá điểm bộ phận hoặc thi kết thúc học phần sẽ nhận điểm 0.

- Có điểm học phần (ĐHP) đạt một trong các mức điểm A, B, C, D.

**13. Thang điểm**

 Thang điểm tính theo Quy chế đào tạo đại học và cao đẳng chính quy theo hệ thống tín chỉ ban hành kèm theo Quyết định số 43/2007/QĐ- BGDĐT, ngày 15 tháng 8 năm 2007 của Bộ trưởng Bộ Giáo dục và Đào tạo và Thông tư số 57/2012/TT-BGDĐT, ngày 27/12/2012 của Bộ trưởng Bộ Giáo dục và Đào tạo sửa đổi, bổ sung một số điều của Quy chế đào tạo đại học và cao đẳng chính quy theo hệ thống tín chỉ ban hành kèm theo Quyết định số 43/2007/QĐ- BGDĐT, ngày 15 tháng 8 năm 2007 của Bộ trưởng Bộ Giáo dục và Đào tạo, cụ thể như sau:

| **Xếp loại** | **Thang điểm 10** | **Thang điểm chữ** | **Thang điểm 4** |
| --- | --- | --- | --- |
| Đạt(Tích lũy) | Giỏi | 9,0 – 10,0 | A+ | 4,0 |
| 8,5 – 8,9 | A | 3,8 |
| Khá | 8,0 – 8,4 | B+ | 3,5 |
| 7,0 – 7,9 | B | 3,0 |
| Trung bình | 6,5 – 6,9 | C+ | 2,5 |
| 5,5 – 6,4 | C | 2,0 |
| Trung bình yếu | 5,0 – 5,4 | D+ | 1,5 |
| 4,0 – 4,9 | D | 1,0 |
| Không đạt | Kém | < 4,0 | F | 0 |

**14. Nội dung học phần**

**Chương 1. GIỚI THIỆU**

*Tổng số: 6 tiết, trong đó Lý thuyết: 6 tiết; Thực hành: 0 tiết; Tự học: 12 giờ*

1. Bối cảnh môn học

2. Các khái niệm an toàn thông tin

3. Kiến trúc an ninh OSI

4. Các tấn công an ninh

5. Các dịch vụ an ninh

6. Các cơ chế an ninh

7. Mô hình an ninh mạng

8. Tổng quan về mật mã học

**Chương 2. MÃ HÓA ĐỐI XỨNG VÀ BẢO MẬT THÔNG BÁO**

*Tổng số: 6 tiết, trong đó Lý thuyết: 6 tiết; Thực hành: 0 tiết; Tự học: 12 giờ*

1. Các nguyên tắc mã hóa đối xứng

2. Các giải thuật mã hóa khối đối xứng

3. Các số ngẫu nhiên và giả ngẫu nhiên

4. Các hệ mã hóa luồng và RC4

5. Các phương thức mã hóa thông báo

**Chương 3. MẬT MÃ KHÓA CÔNG KHAI VÀ XÁC THỰC THÔNG BÁO**

*Tổng số: 9 tiết, trong đó Lý thuyết: 9 tiết; Thực hành: 0 tiết; Tự học: 18 giờ*

1. Các phương pháp xác thực thông báo

2. Hàm băm và SHA

3. Mã xác thực thông báo

4. Các nguyên tắc của mật mã khóa công khai

5. Các giải thuật mật mã khóa công khai

6. Chữ ký số

**Chương 4. MẬT MÃ KHÓA CÔNG KHAI VÀ XÁC THỰC THÔNG BÁO**

*Tổng số: 6 tiết, trong đó Lý thuyết: 6 tiết; Thực hành: 0 tiết; Tự học: 12 giờ*

1. Phân phối khóa đối xứng sử dụng mật mã đối xứng

2. Kerberos

3. Phân phối khóa sử dụng mã hóa bất đối xứng

4. Chứng thực X.509

5. Cơ sở hạ tầng khóa công khai

**Chương 5. AN NINH TẦNG GIAO VẬN**

*Tổng số: 6 tiết, trong đó Lý thuyết: 6 tiết; Thực hành: 0 tiết; Tự học: 12 giờ*

1. SSL

2. TLS

3. HTTPS

4. SSH

**Chương 6. AN NINH THƯ ĐIỆN TỬ**

*Tổng số: 6 tiết, trong đó Lý thuyết: 6 tiết; Thực hành: 0 tiết; Tự học: 12 giờ*

1. PGP

2. S/MIME

**Chương 7. AN NINH IP**

*Tổng số: 6 tiết, trong đó Lý thuyết: 6 tiết; Thực hành: 0 tiết; Tự học: 12 giờ*

1. Tổng quan an ninh IP

2. Chính sách an ninh IP

3. AH

4. ESP

5. Kết hợp các liên kết an ninh

6. Trao đổi khóa Internet

**15. Phương pháp đánh giá học phần**

Quy định số lần kiểm tra bài tập hoặc tiểu luận, thi, số bài thực hành, trọng số của mỗi lần đánh giá:

|  |  |  |  |
| --- | --- | --- | --- |
| TP | Chuyên cần | Định kỳ | Thi |
| Trọng số 10% | 30% | 60% |
| TC | (1) | (2) | (3) | (4) | (5) | (6) | (7) | (8) |
| SL | HS | SL | HS | SL | HS | SL | HS | SL | HS | SL | HS | SL | HS |
|  | 1 | 1 |  |  | 1 | 1 |  |  |  |  | 2 | 1 | 1 | 1 |
| Liên hệ với 9.2 |  |  |  |  |  |  |  |  |  |  | x |  | x |  |
|  |  |  |  |  |  |  |  |  |  | x |  | x |  |
|  |  |  |  |  |  |  |  |  |  | x |  | x |  |
|  |  |  |  |  |  |  |  |  |  | x |  | x |  |
| x |  |  |  |  |  |  |  |  |  |  |  |  |  |

Tích (X) nếu bài kiểm tra, đánh giá liên quan đến những nội dung cần đạt tại mục 9.2

(1) Điểm chuyên cần (vắng học 2% tổng số tiết trừ 1 điểm, tính theo thang điểm 10)

(2) Điểm kiểm tra thường xuyên trong quá trình học tập;

(3) Điểm đánh giá nhận thức và thái độ tham gia thảo luận;

(4) Điểm đánh giá thực hiện bài tập, thực hành;

(5) Điểm thi giữa kỳ;

(6) Điểm đánh giá định kỳ;

(7) Thi kết thúc học phần hoặc Điểm tiểu luận.

 Điểm thi kết thúc học phần có trọng số 60%. Hình thức thi: Thi viết.

**16. Phương pháp dạy và học:** Giảng dạy lý thuyết kết hợp với thảo luận.

|  |  |  |
| --- | --- | --- |
| **Ban Giám hiệu** | **Trưởng khoa** | **Người soạn** |