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

**ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN**

**Trình độ đào tạo: Đại học Ngành: Khoa học máy tính**

**1. Thông tin chung về học phần**

|  |  |
| --- | --- |
| ***1.1. Mã học phần:*** | IT608026 |
| ***1.2. Tên học phần:*** | An toàn và an ninh mạng |
| ***1.3. Tên tiếng Anh:*** | Network safety and security |
| ***1.4. Số tín chỉ:*** | 3 |
| ***1.5. Phân bố thời gian*** |  |
| **-** Lý thuyết: | 45 giờ (3 tín chỉ) |
| - Thực hành: | 0 giờ (0 tín chỉ) |
| - Tự học: | 90 giờ |
| ***1.6. Quản lí, phụ trách học phần*** |  |
| - Khoa quản lí học phần: | Khoa Công nghệ thông tin |
| - Giảng viên phụ trách chính: | ThS. Trịnh Thị Vân |
| - Danh sách giảng viên cùng giảng dạy: |  |
| ***1.7. Điều kiện tham gia học phần*** |  |
| **-** Học phần tiên quyết: | Mạng máy tính |
| - Học phần học trước: | Nhập môn An toàn thông tin |
| - Học phần song hành: | Không |

**2. Mục tiêu học phần**

***2.1. Mục tiêu chung***

Sau khi học xong học phần, sinh viên có kiến thức cơ bản của an toàn và an ninh mạng, trong đó tập trung vào các công nghệ và giao thức chuẩn đã được sử dụng rộng rãi để đảm bảo an toàn cho các dữ liệu truyền qua mạng.

Ngoài ra, học phần còn giới thiệu về lĩnh vực an toàn và an ninh mạng, sau đó được tổ chức thành hai phần. Phần thứ nhất gồm hai chương điểm lại những kiến thức mật mã học cơ bản bao gồm các chủ đề về mã hóa đối xứng, mật mã khóa công khai, xác thực thông báo, hàm băm, và chữ ký số là nền tảng chung cho các ứng dụng an ninh mạng. Phần thứ hai trải dài trong bốn chương là nội dung chính của học phần. Chúng đề cập đến một loạt các ứng dụng và chuẩn an ninh mạng quan trọng bao gồm hệ thống xác thực phân tán Kerberos, các chứng thực X.509v3, giao thức an toàn giao vận SSL/TLS, giao thức an toàn Web HTTPS, chuẩn truyền thông an toàn SSH, chương trình thư điện tử PGP, chuẩn mở rộng khuôn dạng thư điện tử S/MIME, và giao thức an toàn tầng IP IPSec.

***2.2. Mục tiêu cụ thể (COs)***

*2.2.1. Về kiến thức*

- CO 1: Có kiến thức về về an ninh truyền thông và an ninh hệ thống; Tổng quan về các giải thuật và giao thức mã hóa khối đối xứng, mật mã khóa công khai, các phương pháp xác thực, hàm băm, chữ ký số, và các kỹ thuật quản lý khóa

- CO 2: Có kiến thức về các kỹ thuật, phương pháp xác thực phổ biến ở mức ứng dụng; Một số phương thức chủ yếu đảm bảo an ninh thư điện tử; Cơ chế an ninh mạng ở tầng IP; Một số phương thức chuẩn đảm bảo an ninh cho các tác vụ trên nền Web

*2.2.2. Về kỹ năng*

- CO 3: Vận dụng các phương pháp mật mã học trong các giao thức mạng phục vụ mục đích đảm bảo an ninh truyền thông và những vấn đề chính yếu liên quan đến an ninh mạng; Phân tích phát hiện các yếu điểm của các hệ thống mạng và các hiểm họa tấn công. Áp dụng một cách thích hợp các kỹ thuật căn bản đảm bảo an ninh truyền thông và an ninh hệ thống trong các tình huống cần thiết; Đề xuất và xây dựng các giải pháp đảm bảo an ninh của các hệ thống mạng

- CO 4: Có kỹ năng thuyết trình, hoạt động nhóm

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

- CO 5: 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

**3. Chuẩn đầu ra của học phần (CLOs)**

**Bảng 1. Chuẩn đầu ra (CLOs) của học phần**

Khi học xong học phần, SV có khả năng:

| **Ký hiệu** | **Chuẩn đầu ra học phần (CLOs)** | **Hỗ trợ cho**  **mục tiêu** |
| --- | --- | --- |
| CLO1 | Nêu được các khái niệm cơ bản về an ninh truyền thông và an ninh hệ thống. Trình bày được tổng quan về các giải thuật và giao thức mã hóa đối xứng và bảo mật thông báo. | CO1, CO3, CO4, CO5 |
| CLO2 | Trình bày được tổng quan về các giải thuật và giao thức mã khoá công khai và xác thực thông báo. | CO1, CO3, CO4, CO5 |
| CLO3 | Trình bày được tổng quan về các giải thuật và giao thức phân phối khoá và xác thực người dùng. | CO1, CO3, CO4, CO5 |
| CLO4 | Trình bày được tổng quan về an ninh mức giao vận | CO1, CO2, CO4, CO5 |
| CLO5 | Trình bày được tổng quan về an ninh thư điện tử | CO1, CO2, CO4, CO5 |
| CLO6 | Trình bày được tổng quan về an ninh IP | CO1, CO2, CO4, CO5 |

**4. Mối liên hệ giữa CĐR HP(CLO) với CĐR CTĐT (PLO)**

Mức độ đóng góp, hỗ trợ của CLO đối với PLO được xác định cụ thể như sau:

*I (Introduced) – CLO có hỗ trợ đạt được PLO và ở mức giới thiệu/bắt đầu*

*R (Reinforced) – CLO có hỗ trợ đạt được PLO và ở mức nâng cao hơn mức bắt đầu, có nhiều cơ hội được thực hành, thí nghiệm, thực tế,…*

*M (Mastery) – CLO có hỗ trợ cao đạt được PLO và ở mức thuần thục/thông hiểu*

*A (Assessed) – Học phần quan trọng (hỗ trợ tối đa việc đạt được PLO) cần được thu thập minh chứng để đánh giá CĐR CTĐT.*

**Bảng 2. Mối liên hệ giữa CLO với PLO**

| **PLO** | (1) | (2 | (3) | (4) | (5) | (6) | (7) | (8) | (9) | (10) | (11) | (12) |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| CLO1 |  | I |  |  |  |  |  |  |  | R | R |  |
| CLO2 |  | R | R |  |  |  |  | I |  | I | I | I |
| CLO3 |  | I | R |  |  |  |  | R |  | I | I | I |
| CLO4 |  | R | I |  |  |  |  |  |  | I | R | I |
| CLO5 |  | I |  |  |  |  |  | R |  | R | I | I |
| CLO6 |  | R | R |  |  |  |  | R |  |  | I |  |
| Tổng hợp học phần |  | R | R |  |  |  |  | R |  | R | R | I |

**5. Học liệu**

***5.1. Tài liệu chính***

[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.

***5.2. Tài liệu tham khảo***

*a) Tài liệu trong nước*

[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.

*b) Tài liệu nước ngoài*

[5]. William Stallings. *Network Security Essentials: Applications and Standards, Fourth Edition*. Prentice Hall, 2011.

[6]. Vincent Nestler, Gregory White, Wm. Arthur Conklin, and Matthew Hirsch. *Principles of Computer Security: CompTIA Security+ and Beyond, Lab Manual, Second Edition*. McGraw- Hill, 2011.

[7]. Mark Ciampa. *Security+ Guide to Network Security Fundamentals, Third Edition*. Course Technology, 2008.

[8]. William Stallings. *Cryptography and Network Security: Principles and Practice, Fifth Edition*. Prentice Hall, 2010.

[9]. Wm. Arthur Conklin and Gregory White. *Principles of Computer Security, CompTIA Security+ and Beyond (Exam SY0-301), Third Edition*. McGraw-Hill, 2011.

**6. Cấu trúc học phần**

- Tổng số tiết trên lớp: 3 tiết;

- Tổng số tuần học: 15 tuần;

- Phân bố: 3 tiết/ buổi x 1 buổi/ tuần = 15 buổi;

- Kiểm tra, đánh giá:

+ Đánh giá chuyên cần: Tất cả các buổi học;

+ Kiểm tra định kì: 2 bài;

+ Thi kết thúc học phần: 1 bài

**7. Kế hoạch dạy học**

**Bảng 3. Kế hoạch dạy học**

| **Tuần**  **Buổi** | **Nội dung dạy học** | **Số tiết** | **CĐR**  **của bài học** | **Hướng tới**  **CLOs** | **Hoạt động**  **dạy - học** |
| --- | --- | --- | --- | --- | --- |
| 1 | **Chương 1. Giới thiệu**  1.1. Bối cảnh  1.2. Các khái niệm an toàn thông tin  1.3. Kiến trúc an ninh OSI  1.4. Các tấn công an ninh | 3 | *Giới thiệu học phần (\*)*  Trình bày được bối cảnh công nghệ thông tin của Việt Nam và Thế Giới.  Nêu được khái niệm an toàn thông tin  Trình bày được mô hình kiến trúc an ninh OSI  Nêu được các hình thức tấn công an ninh hiện nay. | CLO1 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 2 | **Chương 1. Giới thiệu**  1.5. Các dịch vụ an ninh  1.6. Các cơ chế an ninh  1.7. Mô hình an ninh mạng  1.8. Tổng quan về mật mã học | 3 | Trình bày được các dịch vụ về an ninh.  Nêu và phân tích được các cơ chế an ninh.  Phân tích được mô hình an ninh mạng.  Trình bày được tổng quan về mật mã học. | CLO1 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 3 | **Chương 2. Mã hóa đối xứng và bảo mật thông báo**  2.1. Các nguyên tắc mã hóa đối xứng  2.2. Các giải thuật mã hóa đối xứng  2.3. Các số ngẫu nhiên và giả ngẫu nhiên | 3 | Trình bày và phân tích được các nguyên tắc mã hoá đối xứng.  Nêu được các giải thuật mã hoá đối xứng.  Nêu được các số ngẫu nhiên và giả ngẫu nhiên | CLO1 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 4 | **Chương 2. Mã hóa đối xứng và bảo mật thông báo**  2.4. Mã hóa luồng và giải thuật RC4  2.5. Các chế độ hoạt động của các giải thuật mã hóa khối | 3 | Trình bày được mã hóa luồng và giải thuật RC4  Nêu và giải thích được các chế độ hoạt động của các giải thuật mã hóa khối | CLO1 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 5 | **Chương 3. Mật mã khóa công khai và xác thực thông báo**  3.1. Các phương pháp xác thực thông báo  3.2. Hàm băm và giải thuật SHA | 3 | Trình bày được các phương pháp xác thực thông báo.  Nêu và giải thích được khái niệm hàm băm và giải thuật SHA. | CLO2 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 6 | **Chương 3. Mật mã khóa công khai và xác thực thông báo**  3.3. Các phương pháp mã xác thực thông báo  3.4. Các giải thuật mật mã khóa công khai | 3 | Trình bày được các phương pháp mã xác thực thông báo  Nêu và phân tích được giải thuật mật mã khóa công khai | CLO2 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 7 | **Chương 3. Mật mã khóa công khai và xác thực thông báo**  3.5. Chữ ký số  *Bài kiểm tra số 01* | 3 | Trình bày được khái niệm chữ ký số.  Phân tích được các bài toán về chữ ký số. | CLO2 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 8 | **Chương 4. Phân phối khóa và xác thực người dùng**  4.1. Phân phối khóa đối xứng sử dụng mã hóa đối xứng  4.2. Hệ thống xác thực Kerberos  4.3. Phân phối khóa sử dụng mã hóa bất đối xứng | 3 | Trình bày được phân phối khóa đối xứng sử dụng mã hóa đối xứng.  Phân tích được hệ thống xác thực Kerberos  Nêu được phân phối khóa sử dụng mã hóa bất đối xứng | CLO3 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 9 | **Chương 4. Phân phối khóa và xác thực người dùng**  4.4. Các chứng thực X.509  4.5. Cơ sở hạ tầng khóa công khai | 3 | Trình bày được các chứng thực X.509  Nêu được cơ sở hạ tầng khóa công khai. | CLO3 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 10 | **Chương 5. An ninh mức giao vận**  5.1. Vấn đề an ninh Web  5.2. Giao thức SSL  5.3. Chuẩn TLS | 3 | Trình bày được các vấn đề về an ninh Web  Trình bày được giao thức SSL  Trình bày và phân tích được chuẩn TLS | CLO4 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 11 | **Chương 5. An ninh mức giao vận**  5.4. Giao thức HTTPS  5.5. Giao thức SSH | 3 | Trình bày được giao thức HTTPS  Trình bày được giao thức SSH | CLO4 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 12 | **Chương 6. An ninh thư điện tử**  6.1. Chương trình PGP | 3 | Phân tích được chương trình PGP | CLO5 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 13 | **Chương 6. An ninh thư điện tử**  6.2. Chuẩn S/MIME | 3 | Phân tích được chuẩn S/MIME | CLO5 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 14 | **Chương 7: An ninh IP**  7.1. Khái niệm an ninh IP  7.2. Chính sách an ninh IP  7.3. Giao thức ESP | 3 | Trình bày được khái niệm an ninh IP  Nêu và phân tích được chính sách an ninh IP  Phân tích được giao thức ESP | CLO6 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |
| 15 | **Chương 7: An ninh IP**  7.4. Kết hợp các liên kết an ninh  7.5. Trao đổi khóa Internet  *Bài kiểm tra số 02* | 3 | Trình bày và phân tích được các liên kết an ninh.  Liệt kê và phân tích được các cách trao đổi khoá Internet | CLO6 | GV trình bày, hướng dẫn  SV lắng nghe, thực hiện |

(\*) Giới thiệu học phần: Vị trí, vai trò của học phần trong CTĐT của ngành; CO, CLO, nội dung học phần, các hình thức, trọng số, tiêu chí, biểu điểm các bài kiểm tra, …

**8. Đánh giá học phần**

***8.1. Phương pháp, hình thức kiểm tra - đánh giá***

**Bảng 4. Kiểm tra - đánh giá**

| **Thành phần, tên bài đánh giá** | **Trọng số** | **Nội dung đánh giá** | **Trọng số**  **con** | **Rubric**  **(đánh dấu x nếu có)** | **Hướng tới**  **đánh giá CLOs** | **Cách thức đánh giá** |
| --- | --- | --- | --- | --- | --- | --- |
| (1) | (2) | (3) | (4) | (5) | (6) | (7) |
| A1  Đánh giá chuyên cần | 10% | Ý thức tham gia học tập. |  |  |  | Theo dõi và đánh giá cả quá trình học tập. |
| A2  Đánh giá định kỳ | 30% | Kiến thức về an ninh mạng và mật mã học.  Kiến thức về mã hóa đối xứng và bảo mật thông báo, mật mã khóa công khai và xác thực thông báo | 50% |  | CLO1, CLO2 | SV làm bài viết trên lớp, GV thu bài về chấm điểm |
| Kiến thức về phân phối khóa và xác thực người dùng; An ninh mức giao vận; An ninh thư điện tử; An ninh IP | 50% |  | CLO2 CLO3 CLO4  CLO5  CLO6 | SV làm bài viết trên lớp, GV thu bài về chấm điểm |
| A3  Đánh giá cuối kỳ | 60% | Kiến thức về an ninh mạng và mật mã học; Mã hóa đối xứng và bảo mật thông báo, mật mã khóa công khai và xác thực thông báo. Kiến thức về phân phối khóa và xác thực người dùng; An ninh mức giao vận; An ninh thư điện tử; An ninh IP |  |  | CLO1, CLO2,  CLO3, CLO4, CLO5, CLO6, | Sinh viên làm bài thi lý thuyết theo tổ chức của phòng Khảo thí, giáo viên chấm điểm. |

***8.2. Tiêu chí đánh giá***

*8.2.1. Đánh giá chuyên cần*

- Đi học đầy đủ: 6 điểm (60%, nghỉ 3 tiết học không lý do trừ 1 điểm)

- Hoàn thành đúng hạn các yêu cầu của giảng viên: 2 điểm (20%)

- Tích cực phát biểu, thảo luận trên lớp: 1 điểm (10%)

- Tự học, chủ động tìm tòi kiến thức: 1 điểm (10%)

*8.2.2. Kiểm tra định kỳ*

\* Bài kiểm tra 1:

- Nội dung: Kiến thức về An toàn trong mạng và mật mã học, mã hóa đối xứng và bảo mật thông báo, mật mã khóa công khai và xác thực thông báo

- Thời gian: 50 phút

- Hình thức: Kiểm tra viết

| **STT** | **Nội dung** | **Tiêu chí đánh giá** |  | **Điểm** |
| --- | --- | --- | --- | --- |
| 1 | Kiến thức về an ninh mạng và mật mã học.  Nêu, phân biệt được các khái niệm, trình bày một nội dung cụ thể. | Đúng kiến thức, đủ yêu cầu | | 5 |
| 2 | Kiến thức về mã hóa đối xứng và bảo mật thông báo, mật mã khóa công khai và xác thực thông báo | Đúng kiến thức, đủ yêu cầu | | 5 |
| **Tổng điểm** | | | | **10** |

\* Bài kiểm tra 2:

- Nội dung:

+ Kiến thức về phân phối khóa và xác thực người dùng;

+ Kiến thức về an ninh mức giao vận; An ninh thư điện tử; An ninh IP.

- Thời gian: 50 phút

- Hình thức: Kiểm tra viết

**Bảng 5. Tiêu chí, biểu điểm đánh giá bài kiểm tra định kì**

| **STT** | **Nội dung** | **Tiêu chí đánh giá** |  | **Điểm** |
| --- | --- | --- | --- | --- |
| 1 | Kiến thức về phân phối khóa và xác thực người dùng;  Nêu, phân biệt được các khái niệm  Trình bày một nội dung cụ thể | Đúng kiến thức, đủ yêu cầu | | 5 |
| 2 | Nêu được một số ví dụ thực tế vào an ninh mức giao vận; An ninh thư điện tử; An ninh IP | Đúng kiến thức, đủ yêu cầu | | 5 |
| **Tổng điểm** | | | | **10** |

*8.2.3. Thi kết thúc học phần*

- Nội dung: Kiến thức về quá trình phát triển phần mềm

- Hình thức: Thi viết

- Thời gian: 90 phút

**Bảng 6. Tiêu chí, biểu điểm đánh giá bài thi kết thúc học phần**

| **STT** | **Nội dung** | **Tiêu chí đánh giá** |  | **Điểm** |
| --- | --- | --- | --- | --- |
| 1 | Kiến thức về an ninh mạng và mật mã học; Mã hóa đối xứng và bảo mật thông báo, mật mã khóa công khai và xác thực thông báo. Kiến thức về phân phối khóa và xác thực người dùng; | Đúng kiến thức, đủ yêu cầu | | 5 |
| 2 | Nêu được một số ví dụ thực tế vào An ninh mức giao vận; An ninh thư điện tử; An ninh IP | Đúng kiến thức, đủ yêu cầu | | 5 |
| **Tổng điểm** | | | | **10** |

*Quảng Ninh, ngày 20 tháng 7 năm 2020*

|  |  |  |  |
| --- | --- | --- | --- |
| **Hiệu trưởng** | **Trưởng khoa**  **Lương Khắc Định** | **Trưởng bộ môn** | **Người biên soạn**  **Trịnh Thị Vân** |