|  |  |
| --- | --- |
| BỘ GIÁO DỤC VÀ ĐÀO TẠO  **TRƯỜNG ĐẠI HỌC KINH TẾ QUỐC DÂN** | **CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM**  **Độc lập – Tự do – Hạnh phúc** |

**ĐỀ CƯƠNG HỌC PHẦN TỔNG QUÁT**

*(Ban hành kèm theo quyết định số QĐ/ĐHKTQD, ngày tháng năm 2022)*

**1. THÔNG TIN TỔNG QUÁT (GENERAL INFORMATION)**

|  |  |
| --- | --- |
| ***- Tên học phần (tiếng Việt):*** | **An toàn và bảo mật thông tin** |
| ***- Tên học phần (tiếng Anh)*** | **Cryptography and Security Information** |
| ***- Mã số học phần*** | **CNTT1168** |
| ***- Thuộc khối kiến thức*** | **Các học phần tự chọn** |
| ***- Số tín chỉ*** | **3 tín chỉ** (45 giờ tín chỉ; 50 phút/giờ) |
| ***+ Số tiết lý thuyết*** | **30** |
| ***+ Số tiết thảo luận/thực hành***  ***+ Số tiết tự học*** | **15**  ***90*** |
| ***- Các học phần tiên quyết:*** | **CNTT1128, TIKT1130, TIHT1101, CNTT1114** |

**2. THÔNG TIN BỘ MÔN QUẢN LÝ VÀ GIẢNG VIÊN GIẢNG DẠY**

Bộ môn quản lý: **Bộ môn Công nghệ thông tin**

Địa chỉ: Phòng **1310 Nhà A1, Trường ĐH Kinh tế Quốc dân**

Giảng viên:

|  |  |  |
| --- | --- | --- |
| ThS. Lưu Minh Tuấn | 0904143460 | tuanlm@neu.edu.vn |
| TS. Đặng Minh Quân | 0364102376 | quandm@neu.edu.vn |

**3. MÔ TẢ HỌC PHẦN (COURSE DESCRIPTIONS)**

Học phần trang bị cho người học các kiến thức cơ bản và chuyên sâu về lĩnh vực an toàn và bảo mật thông tin (ATBMTT) đó là tổng quan về an toàn và bảo mật thông tin như: Các mối đe dọa đối với hệ thống và biện pháp ngăn chặn, các hiểm họa và quản lý rủi ro, các mục tiêu và nguyên tắc chung của ATBMTT, vấn đề an toàn bảo mật thông tin truyền trên mạng, các thành phần chính của ATBMTT; một số dạng tấn công an toàn bảo mật thông tin và các kỹ thuật xâm nhập; một số giải pháp an toàn bảo mật thông tin và lý thuyết mật mã đối với vấn đề bảo mật thông tin; Các vấn đề về mã hóa đối xứng, các hệ mã hóa đối xứng (các hệ mã hóa cổ điển, mã hóa đối xứng (khóa bí mật) hiện đại), vấn đề chứng thực & tính không thoái thác của mã hóa đối xứng, trao đổi khóa bí mật bằng trung tâm phân phối khóa; Mã hóa khóa công khai, các vấn đề về lý thuyết số học liên quan đến mã hóa khóa công khai, các hệ mã hóa khóa công khai, trao đổi quản lý khóa và hạ tầng cơ sở khóa công khai (PKI). Học phần cũng giới thiệu các vấn đề về hàm băm và chữ ký điện tử, các sơ đồ chữ ký thông dụng và các ứng dụng.

Học phần rèn luyện kỹ năng tư duy, khả năng nghiên cứu, phát triển, phân tích, tổng hợp, giải quyết và đánh giá các bài toán về an toàn và bảo mật thông tin trong thực tế. Đồng thời học phần cũng phát triển kỹ năng làm việc độc lập, làm việc nhóm và khả năng tự chủ, tự chịu trách nhiệm.

**4. TÀI LIỆU THAM KHẢO (LEARNING RESOURCES: COURSE BOOKS, REFERENCE BOOKS, AND SOFTWARES)**

**Giáo trình:**

[1] Nguyễn Khanh Văn (2014), Giáo trình cơ sở an toàn thông tin, Nhà xuất bản Đại học Bách khoa Hà nội.

[2] William Stallings (2005), Cryptography and Network Security Principles and Practices, Fourth Edition.

**Tài liệu khác:**

[3] Lưu Minh Tuấn (2015), Slide bài giảng An toàn và bảo mật thông tin, Bộ môn CNTT - Viện CNTT & KTS *(Lưu hành nội bộ)*.

[4] Hà Huy Khoái, Phạm Huy Điển (2003), Số học thuật toán, NXB ĐHQGHN.

[5] Bùi Doãn Khanh, Nguyễn Đình Thúc (2004), Mã hóa thông tin - Lý thuyết và ứng dụng, NXB Lao động xã hội.

[6] Nguyễn Xuân Dũng (2007), Bảo mật thông tin - Mô hình và ứng dụng, NXB Thống kê.

[7] Phan Đình Diệu (2002), Lý thuyết mật mã và an toàn thông tin, NXB ĐHQGHN.

[8] VN – GUIDE (2006), Bảo mật trên mạng - Bí quyết & Giải pháp, NXB Thống Kê.

[9] Edward Amoroso (1994), Fundamentals of Computer Security Technology (Bản dịch), Prentice Hall.

[10] Douglas R. Stinson (1995), Cryptography Theory and practice, CRC Press.

**5. MỤC TIÊU HỌC PHẦN (COURSE GOALS)**

**Bảng 5.1. Mục tiêu học phần**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT** | **Mô tả**  **mục tiêu học phần** | **CĐR (PLO) của CTĐT** | **Mức độ** |
| **[1]** | **[2]** | **[3]** | **[4]** |
| G1 | Học phần cung cấp các kiến thức cơ bản và chuyên sâu trong lĩnh vực An toàn thông tin, đó là các phương pháp tấn công cũng như một số giải pháp an toàn và bảo mật thông tin; các phương pháp mã hoá đặc biệt là mã hóa đối xứng, mã hóa khoá công khai, các vấn đề về hàm băm và chữ ký điện tử | PLO1.4A | 4 |
| G2 | Người học có kỹ năng tìm hiểu, nghiên cứu, phân tích, tổng hợp, giải quyết và đánh giá các bài toán về an toàn và bảo mật thông tin | PLO2.3A | 4U |
| G3 | Thể hiện khả năng làm việc độc lập và làm việc theo nhóm, hiểu và thực hiện đúng đắn trách nhiệm thực thi công việc và đạo đức nghề nghiệp. | PLO3.1.1, PLO3.1.2, PLO3.2.3 | 3 |

**6. CHUẨN ĐẦU RA HỌC PHẦN (COURSE LEARNING OUTCOMES)**

**Bảng 6.1. Chuẩn đầu ra học phần (CLO)**

| **Mục tiêu** | **CLOs** | **Mô tả CLOs\*** | **Mức độ đạt được\*\*** |
| --- | --- | --- | --- |
| **[1]** | **[2]** | **[3]** | **[4]** |
| G1 | CLO1.1 | Vận dụng thích hợp các kiến thức cơ bản về an toàn và bảo mật thông tin, một số dạng tấn công an toàn bảo mật thông tin và các giải pháp an toàn bảo mật thông tin | 4 |
| CLO1.2 | Vận dụng thành thạo kiến thức về mã hóa đối xứng, các hệ mã hóa đối xứng, vấn đề chứng thực và trao đổi khóa bí mật bằng trung tâm phân phối khóa | 4 |
| CLO1.3 | Vận dụng thành thạo kiến thức về mã hóa khóa công khai, các hệ mã hóa khóa công khai, vấn đề trao đổi quản lý khóa và hạ tầng cơ sở khóa công khai (PKI) | 4 |
| CLO1.4 | Vận dụng thành thạo kiến thức về hàm băm, chữ ký điện tử và các sơ đồ chữ ký điện tử | 4 |
| G2 | CLO2.1 | Có kỹ năng tìm kiếm, thu thập, tổng hợp, phân tích, đánh giá các bài toán an toàn và bảo mật thông tin | 4U |
| CLO2.2 | Có kỹ năng nghiên cứu, phát triển các ứng dụng an toàn bảo mật thông tin cho các hệ thống | 4U |
| CLO2.3 | Có kỹ năng nghiên cứu, phát triển các ứng dụng chữ ký điện tử cho các hệ thống | 4U |
| G3 | CLO3.1 | Thể hiện khả năng tự học tập, tìm hiểu, nghiên cứu tài liệu để hoàn thành các bài học và bài tập được giao | 3 |
| CLO3.2 | Thể hiện ý thức tổ chức kỷ luật lớp học, tuân thủ các nội quy lớp học, có tinh thần hợp tác và trách nhiệm cá nhân đối với các hoạt động nhóm và hoạt động của lớp học | 3 |
| CLO3.3 | Thể hiện khả năng học tập, tìm hiểu, nghiên cứu tài liệu và làm việc theo nhóm | 3 |

**7. ĐÁNH GIÁ HỌC PHẦN (COURSE ASSESSMENT)**

**Bảng 7.1. Đánh giá học phần**

|  |  |  |
| --- | --- | --- |
| **Hình thức đánh giá** | **CLOs** | **Tỷ lệ (%)** |
| **[1]** | **[4]** | **[6]** |
| Chuyên cần | CLO1.1, CLO1.2, CLO1.3, CLO1.4, CLO2.1, CLO3.2 | 10% |
| Đánh giá quá trình | CLO1.1, CLO1.2, CLO1.3, CLO1.4, CLO2.1, CLO2.2, CLO2.3, CLO3.1, CLO3.2, CLO3.3 | 40% |
| Đánh giá cuối kỳ | CLO1.1, CLO1.2, CLO1.3, CLO1.4 | 50% |

**8. KẾ HOẠCH GIẢNG DẠY (LESSON PLAN)**

**Bảng 8.1. Kế hoạch giảng dạy**

|  |  |  |  |
| --- | --- | --- | --- |
| **Tuần** | **Nội dung giảng dạy\*** | **CLOs** | **Công cụ đánh giá\*\*\*\*** |
| **[1]** | **[2]** | **[3]** | **[4]** |
| 1-3 | **Làm quen, giới thiệu học phần, logic của học phần và vai trò, vị trí của học phần trong CTĐT**  **Chương 1: Tổng quan về an toàn và bảo mật thông tin**  **1.1. Giới thiệu chung**  1.1.1. Giới thiệu  1.1.2. Hệ thống và tài nguyên thông tin  1.1.3. Các mối đe dọa đối với hệ thống  1.1.4. Các hiểm họa và quản lý rủi ro  1.1.5. Các mục tiêu và nguyên tắc chung của ATBMTT  1.1.6. An toàn bảo mật thông tin truyền trên mạng  1.1.7. Các thành phần chính của ATBMTT  [**1.2. M**](#_Toc364783899)**ột số dạng tấn công an toàn thông tin**  1.2.1. Kẻ xâm nhập  1.2.2. Các loại hình tấn công  1.2.3. Phần mềm có hại  1.2.4. Tấn công từ chối dịch vụ (DOS/DDOS)  1.2.5. Tràn bộ đệm  *1.2.6\*. Một số phương pháp tấn công khác*  [**1.3. M**](#_Toc364783899)**ột số giải pháp an toàn và bảo mật thông tin**  1.3.1. Tường lửa  1.3.2. Mạng riêng ảo  1.3.3. An toàn thiết bị mạng  1.3.4. Bảo mật mạng không dây  [1.3.5. An toàn giao thức mạng IP](#_Toc364783893)  1.3.6. An toàn bảo mật các dịch vụ mạng Internet  1.3.7. Kiểm soát truy nhập và xác thực  1.3.8. Hệ thống phát hiện xâm nhập  *1.3.9\*. Một số giải pháp an toàn và bảo mật thông tin khác* | CLO1.1  CLO2.1  CLO3.1  CLO3.2 | - Mức độ tham gia  - Mức độ tương tác  - Chất lượng câu trả lời  - Chất lượng thảo luận |
| 4-6 | **Chương 2: Mã hóa đối xứng**  [**2.1. Mã hóa đối xứng**](#_Toc364783872)  **2.2. Mã hóa đối xứng cổ điển**  [2.2.1. Các mã thế cổ điển thay thế](#_Toc364783872)  [2.2.2. Các mã thế cổ điển hoán vị](#_Toc364783873)  [2.2.3. Một số vấn đề khác](#_Toc364783874)  **2.3. Mã hóa đối xứng hiện đại**  2.3.1. Mã dòng (Stream Cipher)  2.3.1.1. Hệ mã A5/1  2.3.1.2. Hệ mã RC4  2.3.2. Mã khối (Block Cipher)  2.3.2.1. Mã khối an toàn lý tưởng  2.3.2.2. Mạng SPN  2.3.2.3. Mô hình mã Feistel  2.3.2.4. Hệ mã DES (Data Encryption Standard)  2.3.2.4.1. Hệ mã TinyDES (mô hình thu nhỏ của mã DES)  2.3.2.4.2. Hệ mã DES  *2.3.2.4.3\*. Hệ mã Double DES và Triple DES*  2.3.2.5. Hệ mã AES (Advance Encryption Standard)  *2.3.3\*. Các mô hình ứng dụng mã khối*  2.3.3.1. Electronic Codebook - ECB  2.3.3.2. Cipher Block Chaining - CBC  2.3.3.3. Counter - CTR  2.3.3.4. Output Feedback  2.3.3.5. Cipher Feedback - CFB  **2.4. Tính chứng thực của mã hóa đối xứng**  **2.5. Tính không thoái thác của mã hóa đối xứng**  **2.6. Trao đổi khóa bí mật bằng trung tâm phân phối khóa** | CLO1.2  CLO2.1  CLO2.2  CLO3.1  CLO3.2  CLO3.3 | - Mức độ tham gia  - Mức độ tương tác  - Bài tập áp dụng  - Chất lượng câu trả lời  - Chất lượng thảo luận |
| 7-10 | **Chương 3: Mã hóa khóa công khai**  **3.1. Lý thuyết số học**  [3.1.1. Một](#_Toc364783879) số khái niệm cơ bản  [3.1.2. Số học trên Modulo](#_Toc364783877)  [3.1.3. Một số thuật toán trên Zn](#_Toc364783878)  3.1.4. Các thuật toán kiểm tra số nguyên tố  [**3.2. Mã hóa khóa**](#_Toc364783872) **công khai**  3.2.1. Mã hóa khóa công khai  3.2.2. Các hệ mã khóa công khai  3.2.2.1. Hệ mã ba lô (Knapsack)  3.2.2.1.1. Bài toán xuất phát (Bài toán xếp ba lô) (Knapsack)  3.2.2.1.2. Bài toán xếp ba lô với véc tơ ba lô siêu tăng  3.2.2.1.3. Xáo trộn Bài toán ba lô siêu tăng  3.2.2.1.4. Hệ mã ba lô (Knapsack)  3.2.2.2. Hệ mã RSA (Ron Rivest, Adi Shamir và Len Adleman)  3.2.2.2.1. Nguyên tắc thực hiện của RSA  3.2.2.2.2. Độ phức tạp tính toán trong RSA  3.2.2.2.3. Độ an toàn của RSA  *3.2.2.3\*. Các hệ mã hóa khóa công khai khác*  3.2.2.3.1. Hệ mã Rabin  3.2.2.3.2. Hệ mã El-Gammal  *3.2.2.4\*. Các hệ mã dựa trên các đường cong Elliptic*  3.2.3. Bảo mật và chứng thực với mã hóa khóa công khai  **3.3. Trao đổi quản lý khóa**  3.3.1. Trao đổi quản lý khóa công khai  3.3.2. Sử dụng mã hóa khóa công khai để trao đổi khóa bí mật  3.3.3. Phương pháp trao đổi khóa Diffie – Hellman  **3.4. Hạ tầng cơ sở khóa công khai (PKI)**  **Chia nhóm và giao bài tập lớn môn học** | CLO1.3  CLO2.1  CLO2.2  CLO3.1  CLO3.2  CLO3.3 | - Mức độ tham gia  - Mức độ tương tác  - Bài tập áp dụng  - Chất lượng câu trả lời  - Chất lượng thảo luận |
| **Kiểm tra giữa kỳ (20%) các chương 1, 2, 3** | CLO1.1  CLO1.2  CLO1.3  CLO2.1  CLO2.2 | Đề kiểm tra tự luận |
| 11-13 | **Chương 4: Hàm băm và chữ ký điện tử**  **4.1. Hàm băm**  4.1.1. Khái niệm  4.1.2. Đặc tính của hàm băm  4.1.3. Tấn công nghịch lý ngày sinh (birthday attack)  4.1.4. Các hàm Băm thông dụng  4.1.5. Các ứng dụng của hàm băm  **4.2. Chữ ký điện tử** (Digital Signature)  4.2.1. Khái niệm về chữ ký điện tử  4.2.2. Hệ Balô tạo chữ ký điện tử (Knapsack)  4.2.3. Hệ chữ ký điện tử RSA  4.2.4. Chuẩn chữ ký điện tử (Digital Signature Standard)  4.2.5. Các ứng dụng của chữ ký điện tử  *4.3\*. Các hàm băm và hệ chữ ký điện tử khác*  **Bài tập lớn môn học** | CLO1.4  CLO2.1  CLO2.2  CLO2.3  CLO3.1  CLO3.2  CLO3.3 | - Mức độ tham gia  - Mức độ tương tác  - Bài tập áp dụng  - Chất lượng câu trả lời  - Chất lượng thảo luận |
| 14-15 | **Trình bày bài tập lớn**  **Nộp bài bài tập lớn (20%)** | CLO1.1  CLO1.2  CLO1.3  CLO1.4  CLO2.1  CLO2.2  CLO2.3  CLO3.1  CLO3.2  CLO3.3 | Phiếu đánh giá các tiêu chí:  - Nội dung  - Hình thức  - Thời gian trình bày  - Mức độ hợp tác |
| - | **Bài thi cuối kỳ** | CLO1.1  CLO1.2  CLO1.3  CLO1.4 | Theo yêu cầu bài thi cuối học kỳ |

**9. QUY ĐỊNH CỦA HỌC PHẦN (COURSE REQUIREMENTS AND EXPECTATION)**

**9.1. Quy định về điều kiện thi kết thúc học phần**

Sinh viên được tham dự thi cuối kỳ/thi kết thúc học phần (50%) nếu có điểm chuyên cần (10%) đạt mức 5 điểm trở lên (thang 10).

**9.2. Quy định về tham dự lớp học**

* Sinh viên/học viên có trách nhiệm tham dự đầy đủ các buổi học. Trong trường hợp nghỉ học do lý do bất khả kháng thì phải có giấy tờ chứng minh đầy đủ và hợp lý. Mỗi buổi vắng mặt sẽ bị trừ 1 điểm chuyên cần. Sinh viên vắng quá 3 buổi học dù có lý do hay không có lý do đều bị coi như không hoàn thành khóa học và phải đăng ký học lại.
* Sinh viên được xem xét cộng điểm vào điểm chuyên cần, điểm kiểm tra cho việc tích cực xây dựng bài trong các buổi học.

**9.3. Quy định về hành vi lớp học**

* Học phần được thực hiện trên nguyên tắc tôn trọng người học và người dạy. Mọi hành vi làm ảnh hưởng đến quá trình dạy và học đều bị nghiêm cấm.
* Sinh viên phải đi học đúng giờ quy định. Sinh viên đi trễ quá 10 phút sau khi giờ học bắt đầu sẽ không được tham dự buổi học.
* Tuyệt đối không làm ồn, gây ảnh hưởng đến người khác trong quá trình học.
* Không được làm việc riêng trong giờ học. Tuyệt đối không được sử dụng các thiết bị công nghệ thông tin, truyền thông vào việc riêng trong giờ học.

|  |  |  |
| --- | --- | --- |
| **TRƯỞNG BỘ MÔN**  **TS. Phạm Xuân Lâm** | **TRƯỞNG KHOA/VIỆN**  **TS. Nguyễn Trung Tuấn** | **HIỆU TRƯỞNG**  **PGS.TS. Phạm Hồng Chương** |