**TRƯỜNG ĐẠI HỌC NHA TRANG**

**KHOA CÔNG NGHỆ THÔNG TIN**

**BỘ MÔN HỆ THỐNG THÔNG TIN**

**ĐỀ CƯƠNG HỌC PHẦN**

*(Ban hành kèm theo Quyết định số: /QĐ-ĐHNT ngày tháng năm của Hiệu trưởng Trường Đại học Nha Trang)*

**1. Thông tin về học phần:**

Tên học phần:

* Tiếng Việt: **AN TOÀN VÀ BẢO MẬT THÔNG TIN**
* Tiếng Anh: **INFORMATION SECURITY**

Mã học phần: Số tín chỉ: 3 (3-0)

Đào tạo trình độ: Đại học

Học phần tiên quyết: Kỹ thuật lập trình, Mạng máy tính

**2. Mô tả tóm tắt học phần:**

Học phần trang bị cho người học kiến thức về những cơ chế, mô hình và kỹ thuật để giữ bí mật, bảo đảm tính toàn vẹn và sẵn sàng trong các hệ thống thông tin. Những chủ đề chính bao gồm các phương pháp bảo vệ dữ liệu: Cơ bản về mã hoá, thiết kế bảo mật cơ sở dữ liệu, kiểm soát dòng thông tin, kiểm định… Người học có kỹ năng ứng dụng các kỹ thuật bảo mật vào các hệ thống thông tin.

**3. Mục tiêu:**

- Nắm vững nguyên lý của tấn công phá hoại và cách thức phòng chống.

- Nắm vững kiến thức cơ bản về các thuật toán mã hóa và các giao thức bảo mật.

- Có kỹ năng lập trình ứng dụng các thuật toán mã và giao thức bảo mật.

- Kỹ năng tự nghiên cứu và làm việc theo nhóm.

**4. Chuẩn đầu ra (CLOs):** Sau khi học xong học phần, sinh viên có thể:

1. Hiểu được các nguyên lý cơ bản của tấn công phá hoại và cách thức phòng chống.
2. Hiểu mô hình tổng quát và các thuật toán mã hóa thuộc mã hóa đối xứng cổ điển, mã hóa đối xứng hiện đại, mã hóa khóa công khai và hàm băm.
3. Lập trình thực hiện các phương pháp mã hóa đối xứng cổ điển, lập trình ứng dụng mã hóa đối xứng hiện đại, mã hóa khóa công khai và hàm băm.
4. Hiểu nguyên tắc của các giao thức bảo mật và ứng dụng giao thức bảo mật trong thực tế.

**6. Ma trận tương thích giữa Chuẩn đầu ra học phần với Chuẩn đầu ra CTĐT ngành CNTT:**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **CĐR HP (CLOs)** | **CĐR CTĐT (PLOs)** | | | | | | | | | |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** |
| **a** |  |  |  | **x** |  |  |  |  |  |  |
| **b** |  |  |  | **x** |  |  |  |  |  |  |
| **c** |  |  |  | **x** | **x** |  |  |  |  |  |
| **d** |  |  |  |  |  |  | **x** | **x** | **x** |  |

**6. Nội dung:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Chương/Chủ đề** | **Nhằm đạt CLOs** | **Số tiết** | |
| **LT** | **TH** |
| **1**  1.1  1.2 | **Yêu cầu của hệ an toàn bảo mật**  Các hình thức tấn công một hệ truyền tin.  Tính bí mật, tính chứng thực, tính không thoái thác | a | 2 |  |
| **2**  2.1  2.2  2.3  2.4  2.5 | **Mã hóa đối xứng cổ điển**  Mã hóa Ceasar, đơn bảng  Mã hóa đa bảng,  Mã hóa hoán vị  Phá mã: vét cạn khóa, thống kê tần suất  Phá mã trong trường hợp known-plaintext, chosen plaintext | b,c | 7 |  |
| **3**  3.1  3.2  3.3  3.4 | **Mã hóa đối xứng hiện đại**  Mã dòng: A5/1, RC4  Mã khối: hệ mã Fiestel, mã DES.  Mô hình ứng dụng mã khối: ECB, CBC, CTR, OFB, CFB.  Tính chứng thực và không thoái thác của mã đối xứng | b,c | 9 |  |
| **4**  4.1  4.2  4.3  4.4 | **Mã hóa khóa công khai**  Lý thuyết số và hàm một chiều.  Mã hóa RSA.  Truyền khóa Diffie-Hellman.  Tính chứng thực và không thoái thác của mã công khai | b,c | 9 |  |
| **5**  5.1  5.2  5.3  5.4  5.5 | **Mã chứng thực thông điệp và hàm băm, chữ ký điện tử**  Checksum CRC  Mã chứng thực thông điệp MAC  Nghịch lý ngày sinh và hàm băm  Ứng dụng hàm băm  Chữ ký điện tử | b,c,d | 7 |  |
| **6**  6.1  6.2  6.3  6.4 | **Giao thức bảo mật**  Cơ chế chống replay-attack  Chứng chỉ X509  Giao thức SSL  Giao thức S-MIME. | d | 6 |  |
| **7**  7.1  7.2  7.3 | **Bảo mật cơ sở dữ liệu**  Cơ chế phân quyền  Mã hóa cơ sở dữ liệu  Tấn công SQL Injection, XSS. | d | 5 |  |

**7. Phương pháp dạy học:**

|  |  |  |  |
| --- | --- | --- | --- |
| **TT.** | **Phương pháp dạy học** | **Áp dụng cho chủ đề** | **Nhằm đạt CLOs** |
| 1 | Thuyết giảng – làm bài tập - thảo luận. | 1,2,3,4,5,6,7 | a,b,c,d |
| 2 | Thuyết giảng – làm bài tập thực hành | 2,3,4,7 | c,d |

**8. Đánh giá kết quả học tập:**

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Hình thức/tiêu chí đánh giá** | **Nhằm đạt CLOs** | **Trọng số (%)** |
| 1 | Tham gia học trên lớp: *lên lớp đầy đủ*, *chuẩn bị bài tốt, tích cực thảo luận…* | a,b,c,d | 10 |
| 2 | Tự nghiên cứu: *bài tập nhóm theo tháng* | d | 20 |
| 3 | Thi giữa kỳ | a,c,d | 30 |
| 4 | Thi kết thúc học phần | a,b,d | 40 |

**9. Tài liệu dạy và học:**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **STT** | **Tên tác giả** | **Tên tài liệu** | **Năm xuất bản** | **Nhà xuất bản** | **Địa chỉ khai thác tài liệu** | **Mục đích sử dụng** | |
| **Tài liệu chính** | **Tham khảo** |
| 1 | Trần Minh Văn | An toàn bảo mật thông tin | 2016 | NXB Thông tin Truyền thông | Thư viện | x |  |
| 1 | William Stalling | Cryptography and Network Security, 7th | 2016 | Pearson | Thư viện | x |  |
| 2 | Thái Thanh Tùng | Giáo trình Mật mã học và An toàn thông tin | 2011 | NXB Thông tin Truyền thông | Thư viện |  | x |
| 3 | Mark Stamp | Information Security: Principle and Practice 3rd | 2021 | Wiley | Thư viện |  | x |
| 4 | Simon Sign | Mật mã, từ cổ điển đến lượng tử | 2008 | Nhà xuất bản Trẻ | Thư viện |  | x |

*Ngày cập nhật*: 04/2024

**CHỦ NHIỆM HỌC PHẦN TRƯỞNG BỘ MÔN**

*(Ký và ghi họ tên) (Ký và ghi họ tên)*

**Trần Minh Văn Nguyễn Khắc Cường**

**BAN CHỦ NHIỆM CTĐT**

*(Ký và ghi họ tên)*

**Phạm Thị Thu Thúy**