

ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN

1. Tên học phần: An toàn và bảo mật thông tin (Information security)
- Mã số học phần: CT204

- Số tín chỉ học phần: 3 tín chỉ

- Số tiết học phần: 30 tiết lý thuyết, 30 tiết thực hành và 75 tiết tự học
2. Đơn vị phụ trách học phần:
- Bộ môn: Khoa học máy tính

- Khoa: Công nghệ thông tin & Truyền thông
3. Điều kiện:
- Điều kiện tiên quyết: không có.

- Điều kiện song hành: không có.
4. Mục tiêu của học phần:

| Mục tiêu | Nội dung mục tiêu   | CĐR CTĐT |
|----------|---|----------|
| 4.1      | Kiến thức về an toàn thông tin trong thế giới thực và các mô hình tin cậy dựa trên công nghệ mật mã ứng dụng trong quá trình lưu trữ và trao đổi thông tin trên mạng. | 2.1.3b   |
| 4.2      | Khả năng phân tích và đánh giá các nguy cơ của một hệ thống thông tin, từ đó đề ra các giải pháp nhằm đảm bảo an toàn và bảo mật thông tin.                           | 2.2.1b   |

5. Chuẩn đầu ra của học phần:

| CĐR HP | Nội dung chuẩn đầu ra   | Mục tiêu | CĐR CTĐT |
|--------|---|----------|----------|
|        | <b>Kiến thức</b>  |          |          |
| CO1    | Các hình thức tấn công của tin tặc dựa vào sơ hở thông tin của người dùng và các phương pháp cơ bản tạo mật mã thông tin.   | 4.1      | 2.1.3b   |
| CO2    | Các loại mô hình tin cậy dựa trên công nghệ tạo mật mã áp dụng trong quá trình lưu trữ và trao đổi thông tin như Web tin cậy, chứng thư số từ bên thứ ba tin cậy. | 4.1      | 2.1.3b   |
|        | <b>Kỹ năng</b>  |          |          |
| CO3    | Phân tích các nguy cơ của hệ thống và đề ra giải pháp đảm bảo an ninh thông tin.  | 4.2      | 2.2.1b   |
| CO4    | Thiết kế mô hình trao đổi thông tin đảm bảo an toàn và  | 4.2      | 2.2.1b   |

| CĐR HP | Nội dung chuẩn đầu ra  | Mục tiêu | CĐR CTĐT |
|--------|--|----------|----------|
|        | bảo mật, chẳng hạn chứng thư số sử dụng hệ thống phân phối khóa công khai. |          |          |

## 6. Mô tả tóm tắt nội dung học phần:

Học phần giới thiệu tổng quan về những nguy cơ dẫn đến mất an toàn thông tin tạo cơ hội cho những cuộc tấn công mạng diễn ra. Từ đó, những chính sách an ninh, kiểm tra an ninh và các giải pháp đảm bảo an toàn thông tin được đề ra nhằm nâng cao độ tin cậy trong quá trình lưu trữ và trao đổi thông tin. Các giải pháp an toàn thông tin gồm có phương pháp tạo mật mã, các mô hình tin cậy, hạ tầng an toàn khóa công khai và giao thức mật cho các lớp mạng OSI.

## 7. Cấu trúc nội dung học phần:

### 7.1. Lý thuyết

|                  | Nội dung                                     | Số tiết   | CĐR HP        |
|------------------|--|-----------|---------------|
| <b>Chương 1.</b> | <b>Tổng quan tấn công mạng</b>               | <b>6</b>  |               |
| 1.1.             | Nguy cơ từ người sử dụng                     | 1         | CO1; CO3      |
| 1.2.             | Các kỹ thuật cơ bản tấn công mạng            | 5         | CO1; CO3      |
| <b>Chương 2.</b> | <b>An toàn thông tin trong thế giới thực</b> | <b>3</b>  |               |
| 2.1.             | An ninh công sở                              | 1         | CO1; CO3      |
| 2.2.             | Chính sách an ninh và kiểm toán an ninh      | 2         | CO1; CO3      |
| <b>Chương 3.</b> | <b>Các mô hình tin cậy</b>                   | <b>12</b> |               |
| 3.1.             | Các phương pháp tạo mật mã                   | 6         | CO1; CO2; CO4 |
| 3.2.             | Các mô hình tin cậy                          | 6         | CO1; CO2; CO4 |
| <b>Chương 4.</b> | <b>Hạ tầng an toàn</b>                       | <b>9</b>  |               |
| 4.1.             | Hạ tầng khóa công khai PKI                   | 6         | CO2; CO3; CO4 |
| 4.2.             | Giao thức mật cho các lớp mạng OSI           | 3         | CO2; CO3; CO4 |

### 7.2. Thực hành

|               | Nội dung                              | Số tiết  | CĐR HP                    |
|---------------|---------------------------------------|----------|---------------------------|
| <b>Bài 1.</b> | <b>Mã hóa bí mật</b>                  | <b>5</b> | <b>CO1; CO4</b>           |
| <b>Bài 2.</b> | <b>Mã hóa công khai</b>               | <b>5</b> | <b>CO1; CO4</b>           |
| <b>Bài 3.</b> | <b>Mô hình tin cậy</b>                | <b>5</b> | <b>CO2; CO3; CO4</b>      |
| <b>Bài 4.</b> | <b>Hạ tầng khóa công khai</b>         | <b>5</b> | <b>CO2; CO3; CO4</b>      |
| <b>Bài 5.</b> | <b>An ninh trên các tầng mạng OSI</b> | <b>5</b> | <b>CO2; CO4</b>           |
| <b>Bài 6.</b> | <b>Bài thực hành tổng hợp</b>         | <b>5</b> | <b>CO1; CO2; CO3; CO4</b> |

## 8. Phương pháp giảng dạy:

### - Giờ lý thuyết:

+ Kết hợp giảng bài bằng trình chiếu và viết bảng để tăng thêm tính sinh động và uyển chuyển của môn học.

+ Kiểm tra kiến thức cũ bằng cách đặt ra các câu hỏi trong quá trình giảng dạy kiến thức mới có liên quan.



- + Đặt ra các câu hỏi suy luận về vấn đề mới để kích thích tư duy của sinh viên.
- + Sau mỗi buổi học, có nhắc lại nội dung chính và những điểm nhấn mạnh của bài giảng.

#### - Giờ bài tập:

- + Hướng dẫn cách làm một số bài tập áp dụng lý thuyết vừa học.
- + Kiểm tra bài tập đã giao từ buổi trước.
- + Gọi tên hoặc cho xung phong lên bảng trình bày bài giải (yêu cầu giảng lại bài làm và giải đáp các thắc mắc có liên quan).
- + Cung cấp thêm các bài tập khó để sinh viên có cơ hội phát triển tư duy.

#### - Giờ thực hành:

- + Ôn tập ngắn gọn những điểm lý thuyết liên quan đến bài thực hành.
- + Giải thích nội dung thực hành và mục tiêu đạt được của mỗi buổi.
- + Cho sinh viên viết chương trình trên máy tính để giải quyết những yêu cầu đặt ra của các bài thực hành.
- + Giải đáp các câu hỏi của sinh viên liên quan đến bài thực hành.
- + Hướng dẫn và hỗ trợ sinh viên hoàn thành các bài thực hành.

### 9. Nhiệm vụ của sinh viên:

Sinh viên phải thực hiện các nhiệm vụ như sau:

- Bổ sung kiến thức nền tảng cần thiết.
- Tham dự tối thiểu 80% số tiết học lý thuyết.
- Tham gia đầy đủ 100% giờ thực hành và có báo cáo kết quả.
- Nắm vững kiến thức lý thuyết và vận dụng giải đầy đủ các bài tập cuối chương.
- Tham dự kiểm tra giữa học kỳ.
- Tham dự thi kết thúc học phần.
- Chủ động tổ chức thực hiện giờ tự học và nên nghiên cứu các chương theo đúng trình tự được trình bày.

### 10. Đánh giá kết quả học tập của sinh viên:

#### 10.1. Cách đánh giá

Sinh viên được đánh giá tích lũy học phần như sau:

| TT | Điểm thành phần | Quy định   | Trọng số                    | CĐR HP                |
|----|-----------------|--|-----------------------------|-----------------------|
| 1  | Điểm giữa kỳ    | - Thi giữa kỳ (có thể tính điểm chuyên cần, kiểm tra đột xuất) | 30%                         | CO1, CO3              |
| 2  | Điểm cuối kỳ    | - Thi lý thuyết và thi thực hành/báo cáo<br>- Bắt buộc dự thi  | 70%<br>(40% LT<br>+ 30% TH) | CO1, CO2,<br>CO3, CO4 |

#### 10.2. Cách tính điểm

- Điểm đánh giá thành phần và điểm thi kết thúc học phần được chấm theo thang điểm 10 (từ 0 đến 10), làm tròn đến một chữ số thập phân.
- Điểm học phần là tổng điểm của tất cả các điểm đánh giá thành phần của học phần nhân với trọng số tương ứng. Điểm học phần theo thang điểm 10 làm tròn đến một chữ số thập phân, sau đó được quy đổi sang điểm chữ và điểm số theo thang điểm 4 theo quy định về công tác học vụ của Trường.

| Thông tin về tài liệu   | Số đăng ký cá biệt |
|---|--------------------|
| [1] William Stallings, “ <i>Cryptography and network security Principles and practice</i> ”, Upper Saddle River, NJ: Pearson Prentice-Hall, 2003. | CNTT.000795        |
| [2] Atul Kahate, “ <i>Cryptography and networking security</i> ”, New Delhi, India: Tata McGraw-Hill, 2003.                                       | MON.003767         |
| [3] Klaus Schmeh, “ <i>Cryptography and public key infrastructure on the internet</i> ”, Chichester, Eng: John Wiley and Sons, 2001.              | CNTT000585         |

## 12. Hướng dẫn sinh viên tự học:

| Tuần | Nội dung   | Lý thuyết (tiết) | Thực hành (tiết) | Nhiệm vụ của sinh viên   |
|------|--|------------------|------------------|--|
| 1-2  | <b>Chương 1. Tổng quan tấn công mạng</b><br>1.1. Nguy cơ từ người sử dụng<br>1.2. Các kỹ thuật cơ bản tấn công mạng  | 6                | 0                | - Nghiên cứu trước:<br>+ Tài liệu [1]: Nội dung từ mục 1.1 đến 1.2, Chương 1<br>+ Tra cứu về hiện trạng sử dụng hệ thống tin học tại công sở và các doanh nghiệp<br>+ Đọc thêm về tấn công mạng từ các thông tin tìm kiếm được trên mạng<br>- Tham khảo thêm ở tài liệu [2] và [3]   |
| 3    | <b>Chương 2. An toàn thông tin trong thế giới thực</b><br>2.1. An ninh công sở<br>2.2. Chính sách an ninh (Security Policy) và Kiểm toán an ninh (Security Audit). | 3                | 0                | - Nghiên cứu trước:<br>+ Tài liệu [1]: Nội dung từ mục 2.1 đến 2.2, Chương 2<br>+ Ôn lại kiến thức buổi học trước<br>+ Tra cứu an toàn thông tin tại các doanh nghiệp và trường học từ các tạp chí công nghệ thông tin<br>- Tham khảo thêm ở các tài liệu [2], [3] và [4]<br>- Ôn lại lý thuyết và trả lời các câu hỏi liên quan ở cuối chương |
| 4-7  | <b>Chương 3. Các mô hình tin cậy</b><br>3.1. Các phương pháp tạo mật mã (Cryptography).<br>3.2. Các mô hình tin cậy (Trust Models).                                | 12               | 0                | - Nghiên cứu trước:<br>+ Tài liệu [1]: Nội dung từ mục 3.1 đến 3.2, Chương 3<br>+ Ôn lại kiến thức buổi học trước<br>+ Đọc thêm các tài liệu về các giải pháp bảo vệ thông tin của các trang thương mại điện tử và phương pháp tạo mật mã<br>- Tham khảo thêm ở tài liệu [2] và [3]<br>- Ôn lại lý thuyết và làm bài tập ở cuối chương         |
| 8-10 | <b>Chương 4. Hạ tầng an toàn</b><br>4.1. Hạ tầng khóa công   | 9                | 0                | - Nghiên cứu trước:<br>+ Tài liệu [1]: Nội dung từ mục 4.1 đến 4.2, Chương 4   |



| Tuần | Nội dung  | Lý thuyết (tiết) | Thực hành (tiết) | Nhiệm vụ của sinh viên   |
|------|---|------------------|------------------|--|
|      | khái PKI (Public Key Infrastructure)<br>4.2. Giao thức mật cho các lớp mạng OSI (Open System Interconnection) |                  |                  | <ul style="list-style-type: none"> <li>+ Ôn lại kiến thức trong buổi học trước</li> <li>+ Đọc thêm các tài liệu về PKI, OSI, HTTPS và các giao thức mật cho an toàn mạng.</li> <li>- Tham khảo thêm ở tài liệu [2] và [3]</li> <li>- Ôn lại lý thuyết và làm bài tập ở cuối chương.</li> </ul> |
| 11   | Bài thực hành 1   | 0                | 5                | <ul style="list-style-type: none"> <li>- Nghiên cứu trước:</li> <li>+ Thực hiện trước bài thực hành 2</li> <li>- Ôn tập lại bài thực hành số 1</li> </ul>  |
| 12   | Bài thực hành 2   | 0                | 5                | <ul style="list-style-type: none"> <li>- Nghiên cứu trước:</li> <li>+ Thực hiện trước bài thực hành 3</li> <li>- Ôn tập lại bài thực hành số 2</li> </ul>  |
| 13   | Bài thực hành 3   | 0                | 5                | <ul style="list-style-type: none"> <li>- Nghiên cứu trước:</li> <li>+ Thực hiện trước bài thực hành 4</li> <li>- Ôn tập lại bài thực hành số 3</li> </ul>  |
| 14   | Bài thực hành 4   | 0                | 5                | <ul style="list-style-type: none"> <li>- Nghiên cứu trước:</li> <li>+ Thực hiện trước bài thực hành 5</li> <li>- Ôn tập lại bài thực hành số 4</li> </ul>  |
| 15   | Bài thực hành 5   | 0                | 5                | <ul style="list-style-type: none"> <li>- Nghiên cứu trước:</li> <li>+ Thực hiện trước bài thực hành 6</li> <li>- Ôn tập lại bài thực hành số 5</li> </ul>  |
| 16   | Bài thực hành 6   | 0                | 5                | <ul style="list-style-type: none"> <li>- Nghiên cứu trước:</li> <li>+ Ôn các bài thực hành trước</li> <li>- Ôn tập lại bài thực hành số 6</li> </ul>   |

Cần Thơ, ngày 09 tháng 5 năm 2019

**TRƯỞNG BỘ MÔN**



**Nguyễn Hữu Hòa**

**Trần Nguyễn Minh Thư**