ĐẠI HỌC QUỐC GIA TP. HỒ CHÍ MINH

**TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN**

**ĐỀ CƯƠNG MÔN HỌC**

**NT219 – MẬT MÃ HỌC**

# THÔNG TIN CHUNG (General information)

Tên môn học (tiếng Việt): **Mật mã học** Tên môn học (tiếng Anh): **Cryptography** Mã môn học: NT219

Thuộc khối kiến thức: Môn học cơ sở ngành Khoa/Bộ môn phụ trách: Bộ môn An toàn Thông tin Giảng viên phụ trách: Tô Nguyễn Nhật Quang

Email: [quangtnn@uit.edu.vn](mailto:quangtnn@uit.edu.vn) Giảng viên tham gia giảng dạy: ThS. Trần Tuấn Dũng

Số tín chỉ: 3

Lý thuyết: 30 tiết

Thực hành: 15 tiết

Tự học: 30 tiết

Tính chất của môn Bắt buộc đối với sinh viên ngành An toàn Thông

tin

Môn học tiên quyết:

Môn học trước: Nhập môn mạng máy tính (Computer Network Foundation)

# MÔ TẢ MÔN HỌC (Course description)

Môn học cung cấp cho sinh viên các kiến thức cơ bản về mật mã, bao gồm sự hiểu biết khái quát về mã hoá như lịch sử của mật mã học, các giải thuật mã hoá cổ điển, mã hoá khoá đối xứng, giải thuật trao đổi khoá, mã hoá khoá công khai, các phương thức tấn công mật mã và ứng dụng của nó trong việc chứng thực, toàn vẹn dữ liệu, chữ ký số. Sinh viên cũng được giới thiệu về hạ tầng khoá công khai, quản lý khoá, một số giao thức bảo mật mạng dựa trên mã hoá như IPSec, SSL, PGP, Kerberos, SSH.

# MỤC TIÊU MÔN HỌC (Course Goals)

Bảng 1.

|  |  |
| --- | --- |
| **Mô tả** | **Mục tiêu**  **(Theo CĐR cấp 3)** |
| Kiến thức về mật mã và ứng dụng | 1.3.2 |
| Giải pháp và khuyến nghị | 2.1.4 |
| Hình thành giả thuyết | 2.2.1 |
| Khảo sát tài liệu | 2.2.2 |
| Thử nghiệm | 2.2.3 |
| Kiểm chứng và bảo vệ luận điểm | 2.2.4 |

# CHUẨN ĐẦU RA MÔN HỌC (Course learning outcomes)

Bảng 2.

|  |  |  |
| --- | --- | --- |
| **CĐRMH** | **Mô tả CĐRMH (mục tiêu cụ thể)** | **Mức độ giảng dạy** |
| G1 (1.3.2.1) | Kiến thức về mật mã | TU |
| G2 (1.3.2.2) | Kiến thức về áp dụng mật mã cho các giao thức trong thực tế | TU |
| G3 (2.1.4.1) | Đưa ra được các giải pháp về mặt công nghệ, qui trình nhằm đảm bảo tính toàn vẹn, bảo mật và sẵn sàng của hệ thống. | T |
| G5 (2.2.1.1) | Dựa vào vận hành của giao thức mạng, phần mềm, hệ điều hành, phần cứng đưa ra được các giả thuyết về các tấn công ảnh hưởng đến tính an toàn của hệ thống | T |
| G5 (2.2.2.2) | Biết tìm kiếm tài liệu từ các nguồn khác nhau | U |
| G6 (2.2.3.1) | Từ các giả thuyết xây dựng được mô hình, xác định dữ liệu đầu vào, thu thập dữ liệu đầu vào | T |
| G7 (2.2.4.2) | Liên hệ kết quả thử nghiệm và giả thuyết | T |

# NỘI DUNG MÔN HỌC, KẾ HOẠCH GIẢNG DẠY (Course content, Lesson plan)

* 1. **Lý thuyết**

Bảng 3.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Buổi học (tiết)** | **Nội dung** | **CĐRMH** | **Hoạt động dạy và học** | **Thành phần đánh giá** |
| 2 tiết | **Chương 1: Giới thiệu**   1. Giới thiệu về mật mã học 2. Lịch sử của mật mã 3. Bài tập | G1, G5 | **Dạy:** GV thuyết giảng  **Học ở lớp:**   * Trao đổi những vấn đề chưa rõ hoặc chưa hiểu trong buổi học * Chia nhóm 3-4 sinh viên/nhóm để làm bài tập nhóm và Seminar   **Học ở nhà:** Sinh viên tham khảo trước tài liệu [3]. | A1.1, A4 |
| 4 tiết | **Chương 2: Mã hoá cổ điển**   1. Các giải thuật mã hoá cổ điển 2. Tấn công một hệ thống mật mã 3. Bài tập | G1, G6, G7 | **Dạy:**   * GV thuyết giảng * Hướng dẫn sinh viên sử dụng phần mềm Cryp tool   **Học ở lớp:**   * Trao đổi những vấn đề chưa rõ hoặc chưa hiểu trong buổi học * Làm bài tập trên lớp   **Học ở nhà:**   * Tham khảo trước tài liệu 2, 3. | A1.1,  A1.2, A3, A4 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | * Làm bài tập nhóm cuối chương. |  |
| 4 tiết | **Chương 3: Mã hoá đối xứng**   1. Tổng quan 2. Mã hoá khối 3. Chuẩn mã hoá dữ liệu DES 4. Tiêu chuẩn mã hoá tiên tiến AES 5. Một số giải thuật mã hoá họ RC 6. Bài tập | G1 | **Dạy:** GV thuyết giảng  **Học ở lớp:**   * Trao đổi những vấn đề chưa rõ hoặc chưa hiểu trong buổi học * Làm bài tập trên lớp   **Học ở nhà:**   * Tham khảo trước tài liệu 2, 3. * Làm bài tập nhóm cuối chương. | A1.1,  A1.2,  A1.3, A3, A4 |
| 4 tiết | **Chương 4: Mã hoá khoá công khai**   1. Tổng quan 2. Số nguyên tố 3. Giao thức trao đổi khoá Diffie-Hellman 4. Hệ RSA 5. Quản lý khoá 6. Bài tập | G1, G3, G4 | **Dạy:** GV thuyết giảng  **Học ở lớp:**   * Trao đổi những vấn đề chưa rõ hoặc chưa hiểu trong buổi học * Làm bài tập trên lớp   **Học ở nhà:**   * Tham khảo trước tài liệu 2, 3. * Làm bài tập nhóm cuối chương. | A1.1,  A1.2,  A1.3, A3, A4 |
| 4 tiết | **Chương 5: Chứng thực dữ liệu**   1. Mở đầu 2. Mã chứng thực thông điệp 3. Hàm băm 4. Chữ ký số | G2, G4, G6, G7 | **Dạy:** GV thuyết giảng  **Học ở lớp:**   * Trao đổi những vấn đề chưa rõ hoặc chưa hiểu trong buổi học * Làm bài tập trên lớp | A1.1,  A1.2,  A1.3, A3, A4 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | 5. Bài tập |  | **Học ở nhà:**   * Tham khảo trước tài liệu 2, 3 * Làm bài tập nhóm cuối chương |  |
| 6 tiết | **Chương 6: Các giao thức bảo mật**   1. Vị trí của mật mã trong mạng máy tính 2. Cơ sở hạ tầng khoá công khai 3. IPSec 4. SSL/TLS 5. PGP và SMIME 6. Kerberos 7. SSH 8. Bài tập | G2, G3, G4 | **Dạy:** GV thuyết giảng  **Học ở lớp:**   * Trao đổi những vấn đề chưa rõ hoặc chưa hiểu trong buổi học * Làm bài tập trên lớp   **Học ở nhà:**   * Tham khảo trước tài liệu 1, 2 * Làm bài tập nhóm cuối chương | A1.1,  A1.2,  A1.3, A3, A4 |
| 4 tiết | **Seminar của các nhóm sinh viên** | G1, G2, G3, G4 G5, G6, G7 | **Dạy:**   * GV đánh giá các seminar * Trả lời thắc mắc, ôn tập   **Học ở lớp:**   * Sinh viên trình bày seminar * Nêu các thắc mắc   **Học ở nhà:**   * Chuẩn bị seminar và hoàn chỉnh các bài tập nhóm * Làm bài tập nhóm | A1.1,  A1.2, A1.3 |
| 2 tiết | **Ôn tập** | G1, G2,  G3, G4, | **Dạy:** | A4 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | G5, G6, G7 | * GV nhắc lại các nội dung quan trọng của môn học |  |
|  | * Trình bày cách thức và nội dung thi cuối kỳ |
|  | * Kiểm tra tình trạng nộp bài tập các loại của sinh viên |
|  | * Trả lời thắc mắc, ôn tập |
|  | **Học ở lớp:** |
|  | * Sinh viên xác nhận tình trạng các bài tập nhóm đã nộp và còn thiếu |
|  | * Nêu các thắc mắc |
|  | **Học ở nhà:** |
|  | * Chuẩn bị cho kỳ thi cuối kỳ |

# Thực hành

Bảng 4.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Buổi học (X tiết)** | **Nội dung** | **CĐRMH** | **Hoạt động dạy và học** | **Thành phần**  **đánh giá** |
| Buổi 1: | **Bài thực hành 1:** | G1 | * Giảng viên hướng dẫn sinh viên | A3 |
| 5 tiết | Các giải thuật mã hoá dữ liệu cổ điển |  | cách sử dụng phần mềm Cryptool   * Sinh viên: |  |
|  |  |  | o Sử dụng Cryptool để thực hiện |  |
|  |  |  | các bài tập về mã hoá và giải |  |
|  |  |  | mã với các giải thuật mã hoá |  |
|  |  |  | cổ điển |  |
|  |  |  | o Viết các ứng dụng mô phỏng |  |
|  |  |  | Cryptool cho một số giải thuật |  |
|  |  |  | mã hoá cổ điển |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Buổi 2:  5 tiết | **Bài thực hành 2:**  Các giải thuật mã hoá dữ liệu đối xứng | G1 | * Giảng viên hướng dẫn sinh viên cách sử dụng phần mềm Cryptool * Sinh viên sử dụng phần mềm Cryptool để:   + Hiểu được cơ chế hoạt động của DES và AES.   + Thực hiện các bài tập về mã hoá đối xứng | A3 |
| Buổi 3: | **Bài thực hành 3:** | G1, G3 | * Giảng viên hướng dẫn sinh viên | A3 |
| 5 tiết | Giải thuật mã hoá dữ liệu bất đối xứng |  | về cơ chế mã hoá bất đối xứng và cách sử dụng Cryptool để minh hoạ |  |
|  |  |  | * Sinh viên sử dụng phần mềm |  |
|  |  |  | Cryptool để: |  |
|  |  |  | o Hiểu được cơ chế trao đổi |  |
|  |  |  | khoá Diffie-Hellman |  |
|  |  |  | o Hiểu được cơ chế hoạt động |  |
|  |  |  | của RSA |  |
|  |  |  | o Xây dựng ứng dụng mô phỏng |  |
|  |  |  | giao thức trao đổi khoá và mã |  |
|  |  |  | hoá RSA |  |
| Buổi 4: | **Bài thực hành 4:** | G2, G3, | * Giảng viên trình bày nội dung | A3 |
| 5 tiết | * Toàn vẹn dữ liệu, chứng thực và chữ ký số | G4, G5 | buổi thực hành và những điểm cần lưu ý   * Sinh viên sử dụng phần mềm Cryptool để: |  |
|  |  |  | o Làm quen với các hàm băm sử |  |
|  |  |  | dụng trong chứng thực và toàn |  |
|  |  |  | vẹn dữ liệu |  |
|  |  |  | o Cách tạo chữ ký số |  |
|  |  |  | o Cách tấn công vào mã hoá và |  |
|  |  |  | chứng thực |  |
| Buổi 5:  5 tiết | **Bài thực hành 5:**  Tấn công mật mã | G4, G7 | * Giảng viên nêu yêu cầu, hướng dẫn sinh viên cách sử dụng các phần mềm. * Sinh viên thực hiện: | A3 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  |  | * Tấn công tần suất trên mã hoá cổ điển * Tấn công DES với khoá yếu * Tấn công RSA với N nhỏ * Tấn công hàm băm và chữ ký số |  |
| Buổi 6: | **Bài thực hành 6:** | G1, G2, | * Giảng viên:   + Kiểm tra các bài thực hành nhóm   + Nhận xét, đánh giá nhóm và cá nhân sinh viên * Sinh viên:   + Trình bày các bài tập nhóm, các ứng dụng tự viết   + Trả lời các câu hỏi của giảng viên | A3 |
| 5 tiết | Kiểm tra bài tập nhóm và các ứng dụng đã viết | G3 |  |

# ĐÁNH GIÁ MÔN HỌC (Course assessment)

Bảng 5.

|  |  |  |
| --- | --- | --- |
| **Thành phần đánh giá** | **CĐRMH (Gx)** | **Tỷ lệ (%)** |
| A1. Quá trình |  | (30%) |
| A1.1. Kiểm tra trên lớp | G1, G2, G3, G4 | 10% |
| A1.2. Bài tập nhóm | G1, G2, G3, G4, G5 | 10% |
| A1.3. Seminar (Đồ án) | G1, G2, G3, G4, G5, G6, G7 | 10% |
| A2. Thi lý thuyết giữa kỳ |  | 0% |
| A3. Thi thực hành | G1, G2, G3, G4, G6, G7 | 20% |
| A4. Thi lý thuyết cuối kỳ | G1, G2, G3, G4, G6, G7 | 50% |

# QUY ĐỊNH CỦA MÔN HỌC (Course requirements and expectations)

* Sinh viên cần tham dự đầy đủ các buổi học lý thuyết và thực hành, tích cực phát biểu và trao đổi trên lớp.
* Các bài tập trên lớp có thể được thực hiện vào giữa hoặc cuối buổi học, dưới dạng bài tập cá nhân hoặc bài tập nhóm nhằm giúp sinh viên có thể tiếp thu ngay kiến thức vừa học thông qua thảo luận nhóm.
* Phần thực hành được thực hiện với hình thức 1, các sinh viên làm bài tập nhóm ở nhà theo hướng dẫn của giảng viên trên các phần mềm mô phỏng và các công cụ đã giới thiệu trên lớp. Trong 6 buổi thực hành tại phòng lab, sinh viên sẽ thực hiện lại một số bài thực hành đã làm và một số bài tập khác theo yêu cầu của giảng viên.
* Thi lý thuyết cuối kỳ được tiến hành dưới dạng bài thi tự luận. Sinh viên không tham dự kỳ thi lý thuyết cuối kỳ sẽ không đạt môn học này.
* Seminar được các nhóm chọn từ đầu học kỳ và được trình bày ở giữ và cuối học kỳ.

# TÀI LIỆU HỌC TẬP, THAM KHẢO

[1] Stallings, W. (2019). *Cryptography and network security : principles and practice (8th):* Pearson Education.

[2] Yan, S. Y.(2019). *Cybercryptography: Applicable Cryptography for Cyberspace Security*: Springer.

[3] Mihailescu, M. I., & Nita, S. L. (2021). *Pro cryptography and cryptanalysis with C++20: creating and programming advanced algorithms:* Apress.

[4] Katz, J., & Lindell, Y. (2020). *Introduction to modern cryptography* (3rd): CRC press.

# PHẦN MỀM HAY CÔNG CỤ HỖ TRỢ THỰC HÀNH

1. CrypTool 2: https://www.cryptool.org/en/ct2/
2. Crypto++ Library 8.5: https://www.cryptopp.com/
3. C++ Programing Language: Visual Studio Code & MSYS2

<https://www.msys2.org/>; <https://code.visualstudio.com/>

1. Windows and Linux OS; Windows 7, 10; Ubuntu 18 or Kali Linux

<https://www.kali.org/>; <https://releases.ubuntu.com/18.04/>

# Trưởng khoa/ bộ môn

(Ký và ghi rõ họ tên)

# Giảng viên

(Ký và ghi rõ họ tên)

TS. Nguyễn Ngọc Tự