

## ĐỀ CƯƠNG MÔN HỌC

### CTT404 – Mã hóa Mật mã

#### 1. THÔNG TIN CHUNG

*(Hướng dẫn: mô tả các thông tin cơ bản của môn học)*

|                           |                    |
|---------------------------|--------------------|
| Tên môn học (tiếng Việt): | Mã hóa – Mật mã    |
| Tên môn học (tiếng Anh):  | Cryptography 1     |
| Mã số môn học:            | CTT404             |
| Thuộc khối kiến thức:     | Chuyên ngành       |
| Số tín chỉ:               | 4                  |
| Số tiết lý thuyết:        | 45                 |
| Số tiết thực hành:        | 30                 |
| Số tiết tự học:           | 90                 |
| Các môn học tiên quyết    | Nhập môn lập trình |

#### 2. MÔ TẢ MÔN HỌC (COURSE DESCRIPTION)

*(Hướng dẫn: một đoạn văn mô tả tóm tắt về nội dung của môn học)*

Môn học nhằm giúp sinh viên lĩnh hội các kiến thức cơ bản về các hệ thống mã hóa mật mã như hệ mã công khai, hệ mã bí mật, hàm băm và mã dòng... Sinh viên có thể áp dụng các kiến thức này để xây dựng giải pháp cho các yêu cầu về bảo mật như xác thực, kiểm soát truy cập... Thêm vào đó, môn học cũng giúp sinh viên rèn luyện thêm các kỹ năng làm việc nhóm, cũng như tư duy, giải quyết vấn đề 1 cách độc lập và sử dụng các thuật ngữ tiếng Anh trong lĩnh vực mã hóa... Sinh viên cũng có thể hình thành ý thức trách nhiệm liên quan đến an toàn thông tin.

#### 3. MỤC TIÊU MÔN HỌC (COURSE GOALS)

*(Hướng dẫn: Liệt kê các mục tiêu môn học, từ 5-8 mục tiêu ở mức độ tổng quát. Sử dụng động từ Bloom ở mức độ nhóm. Mỗi mục tiêu môn học được mapping với chuẩn đầu ra cấp chương trình)*

Sinh viên học xong môn học này có khả năng :

| Mục tiêu | Mô tả (mức tổng quát )                                                                                                                              | CĐR CDIO của chương trình                              |
|----------|-----------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| G1       | Biết cách làm việc ở mức độ cá nhân và cộng tác nhóm để giải quyết các bài toán mã hóa bằng tay hoặc bằng máy.                                      | 1.1.1, 2.1, 2.2, 4.2, 5.1.1, 5.1.2                     |
| G2       | Sử dụng kỹ năng ngoại ngữ: hiểu các thuật ngữ, đọc được tài liệu tiếng Anh.                                                                         | 1.1.1, 1.2.2, 2.4                                      |
| G3       | Xây dựng tư duy phân tích và phản biện.                                                                                                             | 2.1, 2.3, 4.1, 4.2                                     |
| G4       | Hiểu rõ và áp dụng được các kiến thức cơ bản của mã hóa mật mã, bảo mật thông tin, các hệ thống mã, một số hệ mã cơ bản, hàm băm mật mã và mã dòng. | 1.1.1, 1.2.2, 2.1.1, 2.1.2, 2.1.3, 5.1.1, 5.3.1, 6.1.1 |
| G5       | Ứng dụng kiến thức về MH-MM để xây dựng lời giải cho bài toán chứng thực và bài toán kiểm soát truy cập.                                            | 1.2.1, 2.1.4, 5.1.1, 5.3.1, 6.1.1                      |
| G6       | Áp dụng kỹ năng lập trình và sử dụng các công cụ ứng dụng hạ tầng khóa công khai vào các bài toán cụ thể.                                           | 1.2.1, 1.3.4, 2.1.2, 5.1.1, 5.3.1, 6.1.1               |
| G7       | Biết bảo vệ an toàn thông tin của mình và không xâm hại thông tin của người/tổ chức khác.                                                           | 3.1, 3.3.1, 3.3.2                                      |

#### 4. CHUẨN ĐẦU RA MÔN HỌC

(Hướng dẫn: Mô tả chi tiết các chuẩn đầu ra của môn học. Ứng với mỗi mục tiêu ở mục phía trên có thể có 1 hay nhiều chuẩn đầu ra chi tiết. Đánh mã số chuẩn đầu ra môn học ở cấp 2 tương ứng với mỗi mục tiêu môn học. Mức độ được thể hiện bằng các ký hiệu I-Introduce, T-Teach và U-Utilize. Các động từ mô tả được sử dụng từ các động từ chi tiết của Bloom cho mức độ tương ứng – xem thêm bảng các động từ Bloom chi tiết cho ngành kỹ thuật.)

| Chuẩn đầu ra | Mô tả (Mức chi tiết - hành động)                                | Mức độ (I/T/U) |
|--------------|-----------------------------------------------------------------|----------------|
| G1.1         | Độc lập nghiên cứu, tự phát triển, tự thích nghi.               | I              |
| G1.2         | Thành lập, tổ chức, vận hành và quản lý nhóm.                   | U              |
| G1.3         | Tham gia thảo luận, tranh luận theo nhóm trên chủ đề môn học.   | U              |
| G1.4         | Giải các bài tập mã hóa bằng tay hoặc bằng máy theo nhóm.       | U              |
| G2.1         | Biết, hiểu thuật ngữ tiếng Anh chuyên ngành của môn học.        | I              |
| G2.2         | Đọc hiểu tài liệu tiếng Anh liên quan đến các bài giảng.        | I              |
| G3.1         | Xây dựng tư duy phân tích giải quyết các vấn đề bảo mật cơ bản. | I              |

|      |                                                                                           |    |
|------|-------------------------------------------------------------------------------------------|----|
| G3.2 | Thảo luận, tranh luận, phản biện, phê phán trên cơ sở lý luận khoa học.                   | TU |
| G4.1 | Hiểu rõ các kiến thức cơ bản của mã hóa mật mã và bảo mật thông tin.                      | T  |
| G4.2 | Hiểu rõ các kiến thức về các hệ thống mã công khai và một số hệ mã công khai cơ bản.      | T  |
| G4.3 | Hiểu rõ các kiến thức về các hệ thống mã bí mật và một số hệ mã bí mật cơ bản.            | T  |
| G4.4 | Tìm hiểu, sử dụng, tùy biến một hệ thống mã hóa mật mã thông thường.                      | T  |
| G4.5 | Hiểu rõ các kiến thức về hàm băm mật mã.                                                  | T  |
| G4.6 | Hiểu rõ các kiến thức về hệ mã dòng.                                                      | T  |
| G5.1 | Ứng dụng kiến thức về mã hóa mật mã để xây dựng lời giải cho bài toán chứng thực.         | U  |
| G5.2 | Ứng dụng kiến thức về mã hóa mật mã để xây dựng lời giải cho bài toán kiểm soát truy cập. | U  |
| G6.1 | Sử dụng các công cụ và ứng dụng hạ tầng khóa công khai.                                   | U  |
| G6.2 | Lập trình chuyên dụng trong mã hóa.                                                       | T  |
| G7.1 | Ý thức bảo vệ an toàn thông tin của mình.                                                 | IT |
| G7.2 | Không xâm hại thông tin của người/tổ chức khác.                                           | IT |

## 5. KẾ HOẠCH GIẢNG DẠY LÝ THUYẾT

*(Hướng dẫn: Mô tả chi tiết quá trình giảng dạy theo từng chủ đề: tên chủ đề, danh sách các chuẩn đầu ra chi tiết tương ứng với mỗi chủ đề, các hoạt động dạy và học gợi ý, các hoạt động đánh giá nếu có)*

| STT | Tên chủ đề                        | Chuẩn đầu ra                             | Hoạt động dạy/<br>Hoạt động học (gợi ý) | Hoạt động đánh giá |
|-----|-----------------------------------|------------------------------------------|-----------------------------------------|--------------------|
| 1   | Giới thiệu về lý thuyết thông tin | G1.2, G2.1,<br>G2.2, G4.1,<br>G7.1, G7.2 | Thuyết giảng                            |                    |
| 2   | Mã hóa công khai                  | G1.1, G1.3,                              | Thuyết giảng                            | BT#1               |

|   |                                                       |                                                                                 |                           |      |
|---|-------------------------------------------------------|---------------------------------------------------------------------------------|---------------------------|------|
|   |                                                       | G1.4, G2.1,<br>G2.2, G3.2,<br>G4.2, G4.4                                        | Thảo luận                 |      |
| 3 | Mã đối xứng (symmetric cryptography)                  | G1.1, G1.3,<br>G1.4, G2.1,<br>G2.2, G4.3,<br>G4.4                               | Thuyết giảng<br>Thảo luận | BT#2 |
| 4 | Mã xác thực thông điệp (message authentication codes) | G1.1, G1.3,<br>G1.4, G2.1,<br>G2.2, G3.1,<br>G3.2, G4.2,<br>G7.1, G7.2          | Thuyết giảng<br>Thảo luận |      |
| 5 | Hàm băm                                               | G1.1, G1.3,<br>G1.4, G2.1,<br>G2.2, G4.5                                        | Thuyết giảng<br>Thảo luận | BT#3 |
| 6 | Mã dòng                                               | G1.1, G1.3,<br>G1.4, G2.1,<br>G2.2, G4.6                                        | Thuyết giảng<br>Thảo luận |      |
| 7 | Các tính chất bảo mật                                 | G1.1, G1.3,<br>G1.4, G2.1,<br>G2.2, G3.1,<br>G3.2, G4.1,<br>G7.1, G7.2          | Thuyết giảng<br>Thảo luận |      |
| 8 | Chứng thực và Kiểm soát truy cập                      | G1.1, G1.3,<br>G1.4, G2.1,<br>G2.2, G3.1,<br>G3.2, G5.1,<br>G5.2, G7.1,<br>G7.2 | Thuyết giảng<br>Thảo luận | BT#4 |
| 9 | Hạ tầng khóa công khai (PKI)                          | G1.1, G1.3,<br>G1.4, G2.1,<br>G2.2, G3.1,                                       | Thuyết giảng<br>Thảo luận | BT#5 |

|    |        |                                    |              |  |
|----|--------|------------------------------------|--------------|--|
|    |        | G3.2, G6.1,<br>G6.2, G7.1,<br>G7.2 |              |  |
| 10 | Ôn tập | G1.1, G3.1,<br>G4 -> G7            | Giải bài tập |  |

## 6. KẾ HOẠCH GIẢNG DẠY THỰC HÀNH (nếu có)

*(Hướng dẫn: Mô tả tương tự như kế hoạch giảng dạy lý thuyết. Các chủ đề được liệt kê tuần tự và các chuẩn đầu ra, hoạt động giảng dạy và đánh giá tương ứng cho từng chủ đề.*

*Lưu ý: đối với hình thức thực hành là hình thức 2 – nghĩa là GVTH không lên lớp thì có thể ghi trong hoạt động dạy & học là “thảo luận và trả lời thắc mắc trên diễn đàn môn học”)*

| Tuần | Chủ đề                            | Chuẩn đầu ra                                                                    | Hoạt động dạy/<br>Hoạt động học (gợi ý)              | Hoạt động đánh giá |
|------|-----------------------------------|---------------------------------------------------------------------------------|------------------------------------------------------|--------------------|
| 1    | Hệ mã khóa công khai              | G1.1, G1.3,                                                                     | Thảo luận và trả lời thắc mắc trên diễn đàn môn học. | BT#1               |
| 2    |                                   | G1.4, G2.1,<br>G2.2, G3.2,<br>G4.2, G4.4                                        |                                                      |                    |
| 3    | Hệ mã khóa bí mật                 | G1.1, G1.3,                                                                     | Thảo luận và trả lời thắc mắc trên diễn đàn môn học. | BT#2               |
| 4    |                                   | G1.4, G2.1,<br>G2.2, G4.3,<br>G4.4                                              |                                                      |                    |
| 5    | Hàm băm                           | G1.1, G1.3,                                                                     | Thảo luận và trả lời thắc mắc trên diễn đàn môn học. | BT#3               |
| 6    |                                   | G1.4, G2.1,                                                                     |                                                      |                    |
| 7    |                                   | G2.2, G4.5                                                                      |                                                      |                    |
| 8    | Kiểm soát truy cập/Chữ kí điện tử | G1.1, G1.3,<br>G1.4, G2.1,<br>G2.2, G3.1,<br>G3.2, G5.1,<br>G5.2, G7.1,<br>G7.2 | Thảo luận và trả lời thắc mắc trên diễn đàn môn học. | BT#4               |
| 9    | PKI/CA                            | G1.1, G1.3,                                                                     | Thảo luận và trả lời thắc mắc trên diễn đàn          | BT#5               |
| 10   |                                   | G1.4, G2.1,                                                                     |                                                      |                    |

|  |  |                                                   |          |  |
|--|--|---------------------------------------------------|----------|--|
|  |  | G2.2, G3.1,<br>G3.2, G6.1,<br>G6.2, G7.1,<br>G7.2 | môn học. |  |
|--|--|---------------------------------------------------|----------|--|

## 7. ĐÁNH GIÁ

*(Hướng dẫn: Mô tả các thành phần bài tập, bài thi, đồ án... dùng để đánh giá kết quả của sinh viên khi tham gia môn học này. Bên cạnh mỗi nhóm bài tập, bài thi... cần có tỉ lệ % điểm tương ứng)*

| Mã        | Tên                               | Mô tả (gợi ý) | Các chuẩn đầu ra được đánh giá                                                  | Tỉ lệ (%)  |
|-----------|-----------------------------------|---------------|---------------------------------------------------------------------------------|------------|
| <b>BT</b> | <b>Bài tập</b>                    |               |                                                                                 | <b>50%</b> |
| BT#1      | Hệ mã khóa công khai              |               | G1.1, G1.3,<br>G1.4, G2.1,<br>G2.2, G3.2,<br>G4.2, G4.4                         | 10%        |
| BT#2      | Hệ mã khóa bí mật                 |               | G1.1, G1.3,<br>G1.4, G2.1,<br>G2.2, G4.3,<br>G4.4                               | 10%        |
| BT#3      | Hàm băm                           |               | G1.1, G1.3,<br>G1.4, G2.1,<br>G2.2, G4.5                                        | 10%        |
| BT#4      | Kiểm soát truy cập/Chữ kí điện tử |               | G1.1, G1.3,<br>G1.4, G2.1,<br>G2.2, G3.1,<br>G3.2, G5.1,<br>G5.2, G7.1,<br>G7.2 | 10%        |
| BT#5      | PKI/CA                            |               | G1.1, G1.3,<br>G1.4, G2.1,<br>G2.2, G3.1,<br>G3.2, G6.1,                        | 10%        |

|      |                       |         |                     |     |
|------|-----------------------|---------|---------------------|-----|
|      |                       |         | G6.2, G7.1,<br>G7.2 |     |
| LTCK | Thi lý thuyết cuối kỳ | Vấn đáp | G1.1, G2 -><br>G7   | 50% |

## 8. TÀI NGUYÊN MÔN HỌC

### Giáo trình

...

### Tài liệu tham khảo

*Nhap Mon Tin Hoc Ly Thuyet. Tinh Toan Va cac Otomat.* Arto Salomaa, Vietnamese translation of *Computation and Automata* published by Nha Xuat Ban Khoa Hoc Va Ky Thuat, Hanoi, 1992.

*Public-Key Cryptography*, Arto Salomaa, Second, Enlarged Edition. Springer-Verlag, Berlin, Heidelberg, New York, x+271 pp, 1996.

*Cryptography: Theory And Practice, Third Edition*, Douglas Stinson, Chapman and Hall/CRC, 2005

*Handbook of Applied Cryptography*, Menezes, P. van Oorschot, S. Vanstone, CRC Press.

### Tài nguyên khác

Visual Studio .NET

## 9. CÁC QUY ĐỊNH CHUNG

- Sinh viên cần tuân thủ nghiêm túc các nội quy và quy định của Khoa và Trường.
- Sinh viên không được vắng quá 3 buổi trên tổng số các buổi học lý thuyết.
- Đối với bất kỳ sự gian lận nào trong quá trình làm bài tập hay bài thi, sinh viên phải chịu mọi hình thức kỷ luật của Khoa/Trường và bị 0 điểm cho môn học này.