|  |  |
| --- | --- |
| **BỘ GIÁO DỤC VÀ ĐÀO TẠO**  **Trường Đại học GTVT**  Khoa: Công nghệ thông tin | **MINISTRY OF EDUCATION AND TRAINING**  **University of Transport and Communications**  Faculty of Information Technology |

ĐỀ CƯƠNG HỌC PHẦN

AN TOÀN VÀ BẢO MẬT THÔNG TIN

CRYPTOGRAPHY AND INFORMATION SECURITY

**1. Thông tin tổng quát** *(general information)*

|  |  |
| --- | --- |
| * Tên học phần: | An toàn và bảo mật thông tin |
| * Mã số học phần: | IT1.222.3 |
| * Ngành/Chuyên ngành đào tạo |  |
| * Thuộc khối kiến thức/ kỹ năng:   ◻ Kiến thức cơ bản ◻ Kiến thức chuyên ngành  🗹 Kiến thức cơ sở ngành ◻ Kiến thức ngành | |
| * Số tín chỉ: | 03 |
| + Số tiết lý thuyết học trực tiếp (LT): | 21 |
| + Số tiết lý thuyết học trực truyến (TT): | 9 |
| + BTL | 0 |
| + Số tiết Thảo luận,Bài tập: | 15 |
| + Số tiết,thực hành,thí nghiệm: | 15 |
| + Số tiết tự học: | 90 |
| * Học phần tiên quyết: | Tin học đại cương |
| * Học phần học trước: | Toán rời rạc |
| * Học phần song hành: |  |
| * Yêu cầu khác đối với học phần: | Phòng học có máy chiếu/Bảng thông minh |

*(Số tiết phân bổ cho lý thuyết, thảo luận, bài tập, bài tập lớn, thực hành, thí nghiệm điền và bôi đậm tùy theo học phần cụ thể)*

**2. Mô tả học phần***(course descriptions)*

*(vị trí của học phần đối với CTĐT, những mục đích và nội dung chính yếu của học phần, kỹ năng yêu cầu)*

Học phần An toàn và bảo mật thông tin nằm trong khối kiến thức cơ sở ngành, cung cấp cho người học những kiến thức cơ bản về an toàn và bảo mật thông tin bao gồm lý thuyết mã hóa, lý thuyết số, xác thực, chữ ký điện tử, phân phối khóa.

Sau khi kết thúc học phần, người học hiểu được và biết cài đặt các thuật toán về mã hóa cổ điển, mã hóa đối xứng, mã khóa công khai và áp dụng các thuật toán vào một số ứng dụng như bảo mật, trao đổi khóa, xác thực, chữ ký điện tử, để tổ chức và khai thác thông tin an toàn bảo mật.

**3. Nguồn học liệu** *(learning resources: course books, reference books, and softwares)*

*(Các giáo trình, tài liệu tham khảo, các phần mềm, không quá 5 cuốn)*

***Giáo trình:***

[1] - Slide bài giảng điện tử - Bộ môn Khoa học máy tính

[2] - Trần Văn Dũng. Bài giảng: An toàn và bảo mật thông tin. Bộ môn Khoa học máy tính, 2015.

***Tài liệu khác:***

[1] William Stalling, “Cryptography and Network Security: Principles and Practice”, 5th edition, 2011.

**4. Mục tiêu học phần** *(course goals)*

*(các mục tiêu tổng quát của học phần, thể hiện sự liên quan với CĐR của CTĐT được phân nhiệm cho MH, Viết cô đọng)*

|  |  |  |
| --- | --- | --- |
| **Mục tiêu (G.x) [1]** | **Mô tả mục tiêu [2]** | **CĐR liên quan của CTĐT [3]** |
| **G.1** | **Diễn giải** những kiến thức cơ bản về an toàn và bảo mật thông tin như mã đối xứng, mã công khai, xác thực, chữ ký điện tử, phân phối khóa.  **So sánh, đánh giá, áp dụng** các phương pháp, thuật toán mã hóa, xác thực, chữ ký điện tử vào lĩnh vực bảo mật và an toàn thông tin. | CĐR2 (1.2) |
| **G.2** | - **Vận dụng** các kỹ năng phân tích lập luận giải quyết vấn đề, **khảo sát, đánh giá** vào thử nghiệm các phương pháp mã hóa, xác thực, chữ ký điện tử.  - **Áp dụng** kỹ năng làm việc nhóm trong thảo luận các nội dung môn học, bài tập nhóm. | CĐR7,8 (2.2)  CĐR10 (3.1) |

*[1]: Ký hiệu mục tiêu của học phần. [2]: Mô tả mục tiêu. [3]: Ký hiệu CĐR của CTĐT và chuẩn đầu ra CDIO tương ứng.*

**5. Chuẩn đầu ra học phần** *(course learning outcomes)*

|  |  |  |  |
| --- | --- | --- | --- |
| **CĐR HP cấp độ 3**  **(G.x.y) [1]** | **Mô tả CĐR học phần [2]** | **Mức độ chung HP theo Bloom [3]** | |
| **Mức độ Bloom** | **% thời lượng** |
| **G.1.1** | **Diễn giải** những kiến thức cơ bản về an toàn và bảo mật thông tin bao gồm lý thuyết mã hóa, lý thuyết số, xác thực, chữ ký điện tử, phân phối khóa. | 1.2 – TUA4 | 20% |
| **G.1.2** | **So sánh, đánh giá** các thuật toán mã hóa cổ điển, mã đối xứng, mã hóa khóa công khai. | 1.2 – TUA4 | 20% |
| **G.1.3** | **Phân tích** độ an toàn thông tin, **Áp dụng** các thuật toán mã hóa, xác thực, chữ ký điện tử vào lĩnh vực bảo mật và an toàn thông tin. | 1.2 – TUA4 | 20% |
| **G.2.1** | **Vận dụng** các kỹ năng phân tích lập luận giải quyết vấn đề, **khảo sát, đánh giá** vào thử nghiệm các phương pháp mã hóa, xác thực, chữ ký điện tử. | 2.2(1-4) -TUA2 | 20% |
| **G.2.2** | **Áp dụng, đánh giá** kỹ năng làm việc nhóm trong thảo luận các nội dung của môn học và làm bài thực hành. | 3.1 (1-2) - UA3 | 20% |

*[1]: Ký hiệu CĐR của học phần. [2]: Mô tả CĐR học phần, bao gồm các động từ chủ động theo Bloom’s Toxonomi, khuyến khích viết tích hợp kỹ năng và kiến thức [3]: Mức độ năng lực mà HP đảm trách theo hoạt động TUA.*

**6. Đánh giá học phần** *(course assessment)*

*(các thành phần, các bài đánh giá, các tiêu chí đánh giá, chuẩn đánh giá, và tỷ lệ đánh giá, thể hiện sự liên quan với các CĐR của học phần)*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Thành phần đánh giá [1]** | **Hình thức đánh giá (A.x.y) [2]** | **CĐR học phần (G.x.y) [3]** | **Tiêu chí**  **đánh giá [4]** | **Tỷ lệ (%)[5]** |
| A1. Đánh giá quá trình | A1.1 Bài kiểm viết | G.1.1  G.1.2 | Hiểu, So sánh, đánh giá các thuật toán | 15% |
| A1.2 Thực hành | G.1.2  G.2.2 | Chương trình máy tính hoạt động đúng đắn | 20% |
| A1.3 Chuyên cần | G.1.1  G.1.2 | Hiểu và giải thích được các thuật toán | 15% |
| A2. Đánh giá kết thúc học phần ít nhất 50%) | A.2.1 Kiểm tra viết. | G.1.(1-3)  G.2.3 | Hiểu, giải thích, so sánh, áp dụng được các thuật toán, kiến thức về an toàn và bảo mật thông tin trong bài làm. | 50% |

*[1]: Các thành phần đánh giá của học phần. [2]: Các bài đánh giá. [3]: Các CĐR được đánh giá. [4]: Tiêu chí đánh giá. [5]: Tỷ lệ điểm của các bài đánh giá trong tổng điểm học phần.*

**7. Khung kế hoạch giảng dạy***:*

*(Các nội dung giảng dạy theo buổi học, thể hiện sự liên quan với các CĐR của học phần, các hoạt động dạy và học (ở lớp, ở nhà), và các bài đánh giá của học phần, Việc giảng dạy kỹ năng trong môn học có thể dạy lý thuyết và áp dụng hoặc có thể học qua trải nghiệm)*. Trong môn học này, kỹ năng được dạy theo phương pháp trải nghiệm, được tích hợp trong môn học.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TT** | **Nội dung [2]** | **Số tiết** | **CĐR HP [3]** | **Hoạt động dạy và học [4]** | **Bài đánh giá [5]** |
| **1** | **Chương 1. Mã cổ điển**  1.1. Các khái niệm về mã  1.2. Mã thế  1.3. Mã chuyển vị | 3LT+1BT+0TH | G1.1  G2.3 | **Giảng viên:**  - Giới thiệu về môn học  - Giảng mục 1.1, 1.2, 1.3  *Sử dụng phương pháp truyền đạt thuyết giảng (lecturing)*  - Ra bài tập, hướng dẫn sinh viên làm bài tập, hướng dẫn sinh viên thực hành  *Sử dụng phương pháp truyền đạt đôi bạn cùng tiến (peer-to-peer) hoặc phương pháp học nhóm* (Team-based-learning).  **Sinh viên:**  - Học ở lớp: Nghe giảng lý thuyết, làm bài tập nhóm, - Học ở nhà: Làm bài tập củng cố kỹ năng lập trình | A1.1 |
| **2** | **Chương 2. Trường hữu hạn**  2.1. Các phép toán modulo  2.2. Định lý Fecma, Euler  2.3 Định lý phần dư Trung hoa  2.4 Logarit rời rạc | 8LT + 5BT+  3TH | G1.1  G2.2  G2.3 | **Giảng viên:**  - Giảng mục 2.1, 2.2, 2.3, 2.4  Sử dụng phương pháp truyền đạt thuyết giảng (lecturing)  - Ra bài tập, hướng dẫn sinh viên làm bài tập  *Sử dụng phương pháp truyền đạt đôi bạn cùng tiến (peer-to-peer) hoặc phương pháp học nhóm (Team-based-learning).*  - Tổ chức kiểm tra kiến thức chương 1, 2  **Sinh viên:**  - Học ở lớp: Nghe giảng lý thuyết, làm bài tập theo sự hướng dẫn của giảng viên, làm bài kiểm tra kiến thức chương 1, 2. Làm bài thực hành theo hướng dẫn của giảng viên.  - Học ở nhà: Làm bài tập củng cố kỹ năng lý thuyết, cài đặt một số thuật toán. | A1.1 |
| **3** | **Chương 3. Mã khối hiện đại**  3.1 Khái niệm  3.2 Chuẩn mã dữ liệu  3.3. Chuẩn mã nâng cao  3.4. Mã dòng hiện đại | 4LT+0BT+3TH+ | G1.2  G2.1  G2.3 | **Giảng viên:**  - Giảng mục 3.1, 3.2, 3.3, 3.4  *Sử dụng phương pháp truyền đạt thuyết giảng (lecturing)*  - Hướng dẫn sinh viên thảo luận các mục 3.2, 3.3  *Sử dụng phương pháp truyền đạt theo mô hình đảo ngược (flipped -classroom)*  - Hướng dẫn sinh viên hoàn thành mục 3.2, 3.3 thông qua một số bài tập áp dụng các cấu trúc dữ liệu đã học.  *Sử dụng phương pháp truyền đạt đôi bạn cùng tiến (peer-to-peer) hoặc phương pháp học nhóm (Team-based-learning).*  **Sinh viên:**  - Học ở lớp: Nghe giảng lý thuyết mục 3.1, 3.2, 3.3; thảo luận kiến thức mục 3.2, 3.3, làm bài tập nhóm trong mục, thực hành trên phòng máy tính.  - Học ở nhà: tìm hiểu các kiến thức mục 3.2, 3.3, 3.4; thực hành cài đặt. | A1.2  A2.1 |
| **4** | **Chương 4. Mã công khai**  4.1 Khái niệm về mã công khai  4.2 Mã công khai RSA  4.3 Mã công khai Elgamal  4.4 Trao đổi khóa Diffie-Hellman | 6LT + 6BT+6TH | G.1.2  G2.1  G2.3 | **Giảng viên:**  - Hướng dẫn sinh viên thảo luận các mục 4.1, 4.2, 4.3, 4.4  *Sử dụng phương pháp truyền đạt thuyết giảng (lecturing)*  - Hướng dẫn sinh viên hoàn thành mục 4.2, 4.3, 4.4 thông qua một số bài tập.  *Sử dụng phương pháp truyền đạt đôi bạn cùng tiến (peer-to-peer) hoặc phương pháp học nhóm (Team-based-learning).*  **Sinh viên:**  - Học ở lớp: Thảo luận kiến thức mục 4.1, 4.2, 4.3, làm bài tập, thực hành trên phòng máy tính.  - Học ở nhà: tìm hiểu các kiến thức mục 4.1, 4.2, 4.3, 4.4; thực hành cài cài đặt các bài tập. | A1.2  A2.1 |
| **5** | **Chương 5. Xác thực thông điệp**  5.1. Mã xác thực thông điệp  5.2. Hàm băm  5.3 SHA  5.4. Chữ ký điện tử DSA | 3LT + 0BT+ 0TH+ | G1.2  G2.1  G2.3 | **Giảng viên:**  - Hướng dẫn sinh viên thảo luận các mục 5.1, 5.2, 5.3  *Sử dụng phương pháp truyền đạt thuyết giảng (lecturing)*  - Hướng dẫn sinh viên hiểu sâu hơn về lý thuyết.  *Sử dụng phương pháp truyền đạt đôi bạn cùng tiến (peer-to-peer) hoặc phương pháp học nhóm (Team-based-learning).*  **Sinh viên:**  - Học ở lớp: Thảo luận kiến thức mục 5.1, 5.2, 5.3, 5.4,  - Học ở nhà: tìm hiểu các kiến thức mục 5.1, 5.2, 5.3; | A1.2  A2.1 |
| **6** | **Chương 6. Một số ứng dụng bảo mật trên mạng**  6.1. Trao đổi khóa  6.2. Xác thực người sử dụng Kerberos  6.3 Một số giao thức an ninh  6.4 An toàn thư điện tử  6.5 Thanh toán điện tử an toàn | 3LT+  0BT+0TH | G1.3  G2.2  G2.3 | **Giảng viên:**  - Hướng dẫn sinh viên thảo luận các mục 6.1, 6.2, 6.3  *Sử dụng phương pháp truyền đạt thuyết giảng (lecturing)*  - Hướng dẫn sinh viên tìm hiểu các ứng dụng thực tế  *Sử dụng phương pháp truyền đạt đôi bạn cùng tiến (peer-to-peer) hoặc phương pháp học nhóm (Team-based-learning).*  **Sinh viên:**  - Học ở lớp: Thảo luận kiến thức mục 6.1, 6.2, 6.3,  - Học ở nhà: tìm hiểu các kiến thức mục 6.1, 6.2, 6.3; | A1.3  A2.1 |
| **7** | **Chương 7. An ninh hệ thống**  7.1 Kẻ xâm nhập  7.2 Phần mềm có hại  7.3 Bức tường lửa  7.4 Hệ thống thông tin an toàn | 2LT + 0BT+  0TH | G1.3  G2.2  G2.3 | **Giảng viên:**  - Hướng dẫn sinh viên thảo luận các mục 7.1, 7.2, 7.3, 7.4  *Sử dụng phương pháp truyền đạt thuyết giảng (lecturing)*  - Hướng dẫn sinh viên tìm hiểu ứng dụng thực tế  **Sinh viên:**  - Học ở lớp: thảo luận kiến thức mục 7.1, 7.2, 7.3, 7.4  - Học ở nhà: tìm hiểu các kiến thức mục 7.1, 7.2, 7.3, 7.4. | A1.3  A2.1 |

*[1]: Thông tin về tuần/ buổi học. [2]: Liệt kê nội dung giảng dạy theo chương, mục. [3]: Liệt kê CĐR liên quan của học phần (ghi ký hiệu Gx.y). [4]: Liệt kê các hoạt động dạy và học (ở lớp, ở nhà), bao gồm đọc trước tài liệu (nếu có yêu cầu). [5]: Liệt kê các bài đánh giá liên quan (ghi ký hiệu Ax.y).*

**8. Quy định của học phần** *(course requirements and expectations)*

Sinh viên phải tham dự đầy đủ các bài kiểm tra, phải tham gia ít nhất 80% buổi học trên lớp và 80% số buổi thực hành trên phòng máy, tham gia bảo vệ bài tập lớn mới được tính điểm đánh giá kết thúc học phần

*.*

**9. Phụ trách học phần**

- Khoa/ Bộ môn: Khoa Công nghệ thông tin/ Bộ môn Khoa học máy tính

- Địa chỉ và email liên hệ: P309, Nhà A9

|  |  |  |
| --- | --- | --- |
| **Trưởng Khoa**  **TS. Hoàng Văn Thông** |  | **Trưởng Bộ môn**  **TS. Hoàng Văn Thông** |
| **PHÊ DUYỆT CỦA NHÀ TRƯỜNG** | | |