

**BỘ CÔNG THƯƠNG  
TRƯỜNG ĐẠI HỌC SAO ĐỎ  
\*\*\*\*\***

**ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN  
BẢO MẬT THÔNG TIN**

**Số tín chỉ: 03**

**Trình độ đào tạo: Đại học**

**Ngành đào tạo: Công nghệ thông tin**

**Năm 2018**

## ĐỀ CƯƠNG CHI TIẾT HỌC PHẦN

Trình độ đào tạo: Đại học

Ngành đào tạo: Công nghệ thông tin

- Tên học phần:** Bảo mật thông tin
- Mã học phần:** TIN 341
- Số tín chỉ:** 3 (2, 1)
- Trình độ cho sinh viên:** Năm thứ tư
- Phân bổ thời gian**
  - Lên lớp: 30 tiết lý thuyết, 30 tiết thực hành
  - Tự học: 90 giờ
- Điều kiện tiên quyết:** Toán rời rạc, Mạng máy tính
- Giảng viên**

STT	Học hàm, học vị, họ tên	Số điện thoại	Email
1	ThS. Hoàng Thị Ngọc Diệp	0969.803.788	HTNDiep@saodo.edu.vn
2	ThS. Phạm Thị Hương	0972.306.806	PTHuong@saodo.edu.vn

### 8. Mô tả nội dung của học phần

Học phần Bảo mật thông tin gồm các kiến thức cơ bản về bảo mật thông tin, bảo mật mạng; giới thiệu các phương pháp mã hóa, giải mã, thám mã hệ mã đối xứng, bất đối xứng, mã khối, sơ đồ chữ ký số, hàm băm và ứng dụng của chúng trong bảo mật thông tin.

### 9. Mục tiêu và chuẩn đầu ra học phần

#### 9.1. Mục tiêu

Mục tiêu học phần thỏa mãn mục tiêu của chương trình đào tạo:

Mục tiêu	Mô tả	Mức độ theo thang đo Bloom	Phân bổ mục tiêu học phần trong CTĐT
<b>MT1</b>	<b>Kiến thức</b>		
MT1.1	Trình bày nội dung của an toàn và bảo mật thông tin, các chiến lược an toàn hệ thống, các mức bảo vệ trên mạng, ý tưởng chung của an toàn thông tin bằng mật mã và tiêu chuẩn để đánh giá một hệ mật mã.	2	[1.2.1.2a]
MT1.2	Trình bày các giải thuật mã hóa, giải mã, thám mã các hệ bất đối xứng, đối xứng, sơ đồ chữ ký số, hàm băm vào mã hóa, giải mã thông tin.	2	[1.2.1.2b]

<b>Mục tiêu</b>	<b>Mô tả</b>	<b>Mức độ theo thang đo Bloom</b>	<b>Phân bổ mục tiêu học phần trong CTĐT</b>
MT1.3	Tính toán các khóa, bản mã, bản rõ, chữ ký của từng hệ mật mã.	3	[1.2.1.2b]
<b>MT2</b>	<b>Kỹ năng</b>		
MT2.1	Áp dụng các phương pháp mã hóa, giải mã, thám mã các hệ mật mã vào thực hành cài đặt chương trình để bảo mật thông tin.	3	[1.2.2.2]
MT2.2	Phân tích kỹ thuật mã hóa, giải mã của hệ mật mã; kỹ thuật ký và xác minh của các hệ chữ ký.	4	[1.2.2.2]
MT2.3	Đánh giá các hệ mật mã và ứng dụng bảo mật thông tin dùng hệ mật mã và chữ ký số.	5	[1.2.2.2]
<b>MT3</b>	<b>Mức tự chủ và trách nhiệm</b>		
MT3.1	Có thái độ nghiêm túc, tự giác, tích cực, khoa học, độc lập, cẩn thận, tuân thủ trong công việc.	3	[1.2.3.1]
MT3.2	Có năng lực giải quyết các công việc liên quan đến bảo mật thông tin.	4	[1.2.3.1]

## 9.2. Chuẩn đầu ra

Sự phù hợp của chuẩn đầu ra học phần với chuẩn đầu ra của chương trình đào tạo:

<b>CĐR học phần</b>	<b>Mô tả</b>	<b>Thang đo Bloom</b>	<b>Phân bổ CĐR học phần trong CTĐT</b>
<b>CĐR1</b>	<b>Kiến thức</b>		
CĐR1.1	Giải thích được nội dung bí mật, xác thực, trách nhiệm của an toàn thông tin; 6 chiến lược an toàn hệ thống, 6 mức bảo vệ trên mạng; ý nghĩa 5 thành phần của an toàn thông tin bằng mật mã và 3 tiêu chuẩn để đánh giá một hệ mật mã.	2	[2.1.5]
CĐR1.2	Diễn giải được các giải thuật mã hóa, giải mã, thám mã hệ mật mã đối xứng, bất đối xứng, chữ ký.	2	[2.1.5]
CĐR1.3	Phân tích được bản rõ, bản mã, phương pháp mã hóa, giải mã, thám mã ứng với từng hệ mật mã.	4	[2.1.5]

<b>CDR học phần</b>	<b>Mô tả</b>	<b>Thang đo Bloom</b>	<b>Phân bố CDR học phần trong CTĐT</b>
<b>CDR2</b>	<b>Kỹ năng</b>		
CDR2.1	Áp dụng các phương pháp mật mã cổ điển, mã khối, mã công khai, chữ ký số vào thực tế bảo mật thông tin.	3	[2.2.1]
CDR2.2	Phân biệt được các hệ mật mã công khai về ý tưởng, giải thuật và áp dụng so với hệ mã bí mật.	4	[2.2.3]
CDR2.3	Đánh giá được các chương trình sử dụng hệ chữ ký số để kiểm tra tính toàn vẹn và tính không chối cãi của file dữ liệu.	5	[2.2.3]
<b>CDR3</b>	<b>Mức tự chủ và trách nhiệm</b>		
CDR3.1	Có thái độ nghiêm túc, tuân thủ trong việc sử dụng thông tin hợp pháp. Có thái độ làm việc tích cực, khoa học, độc lập và cẩn thận; ý thức trách nhiệm trong việc bảo mật và sử dụng thông tin; thái độ hợp tác và chia sẻ khi làm việc theo nhóm. Có thái độ nghiêm túc, tự giác, tích cực, khoa học, độc lập, cẩn thận, tuân thủ trong công việc.	3	[2.3.1]
CDR3.2	Có năng lực định hướng, hướng dẫn người khác bảo mật thông tin và sử dụng thông tin hợp pháp.	4	[2.3.2]

#### 10. Ma trận liên kết nội dung với chuẩn đầu ra học phần

<b>Chương</b>	<b>Nội dung học phần</b>	<b>Chuẩn đầu ra của học phần</b>							
		<b>CDR1</b>			<b>CDR2</b>			<b>CDR3</b>	
		<b>CDR 1.1</b>	<b>CDR 1.2</b>	<b>CDR 1.3</b>	<b>CDR 2.1</b>	<b>CDR 2.2</b>	<b>CDR 2.3</b>	<b>CDR 3.1</b>	<b>CDR 3.2</b>
1	<b>Chương 1. Tổng quan về an toàn và bảo mật thông tin</b> 1.1. Nội dung của an toàn và bảo mật thông tin 1.2. Các chiến lược an toàn hệ thống	x						x	

Chương	Nội dung học phần	Chuẩn đầu ra của học phần							
		CĐR1			CĐR2			CĐR3	
		CĐR 1.1	CĐR 1.2	CĐR 1.3	CĐR 2.1	CĐR 2.2	CĐR 2.3	CĐR 3.1	CĐR 3.2
	1.3. Các mức bảo vệ trên mạng 1.4. An toàn thông tin bằng mật mã 1.5. Vai trò của hệ mật mã 1.6. Phân loại hệ mật mã 1.7. Tiêu chuẩn đánh giá hệ mật mã								
2	<b>Chương 2. Các phương pháp mã hóa cổ điển</b> 2.1. Các hệ mật mã cổ điển 2.2. Thám mã các hệ mã cổ điển		x	x	x			x	
3	<b>Chương 3. Chuẩn mã dữ liệu DES</b> 3.1. Giới thiệu chung về DES 3.2. Mô tả thuật toán 3.3. Hoán vị khởi đầu 3.4. Khoá chuyển đổi 3.5. Hoán vị mở rộng 3.6. Hộp thay thế S		x	x	x			x	

Chương	Nội dung học phần	Chuẩn đầu ra của học phần							
		CĐR1			CĐR2			CĐR3	
		CĐR 1.1	CĐR 1.2	CĐR 1.3	CĐR 2.1	CĐR 2.2	CĐR 2.3	CĐR 3.1	CĐR 3.2
	3.7. Hộp hoán vị P 3.8. Hoán vị cuối cùng 3.9. Giải mã DES 3.10. Phần cứng và phần mềm thực hiện DES 3.11. Sự an toàn của DES 3.12. Tranh luận về DES 3.13. DES trong thực tế 3.14. Các chế độ hoạt động của DES								
4	<b>Chương 4. Mật mã công khai</b> 4.1. Giới thiệu về hệ mật mã khóa công khai 4.2. Hệ mật RSA 4.3. Hệ mật mã Rabin 4.4. Hệ mật Elgamal và các hệ tương tự 4.5. Các hệ mật mã dựa trên các bài toán NP - đầy đủ		x	x	x	x		x	
5	<b>Chương 5. Các sơ đồ chữ ký số</b>		x	x	x		x		x

Chương	Nội dung học phần	Chuẩn đầu ra của học phần							
		CĐR1			CĐR2			CĐR3	
		CĐR 1.1	CĐR 1.2	CĐR 1.3	CĐR 2.1	CĐR 2.2	CĐR 2.3	CĐR 3.1	CĐR 3.2
	5.1. Định nghĩa sơ đồ chữ ký số 5.2. Sơ đồ chữ ký RSA 5.3. Sơ đồ chữ ký ELGAMAL 5.4. Sơ đồ chữ ký không phủ định được 5.5. Hàm băm và chữ ký số								

## 11. Đánh giá học phần

### 11.1. Kiểm tra và đánh giá trình độ

Chuẩn đầu ra	Mức độ thành thạo được đánh giá bởi
CĐR1	Kiểm tra thường xuyên, bài tập thực hành, kiểm tra thực hiện nhiệm vụ về nhà, kiểm tra giữa học phần.
CĐR2	Bài tập thực hành, thực hiện nhiệm vụ về nhà, kiểm tra giữa học phần, thi kết thúc học phần.
CĐR3	Kiểm tra thường xuyên, kết quả thực hiện nhiệm vụ của cá nhân và theo nhóm, thi kết thúc học phần.

**11.2. Cách tính điểm học phần:** Tính theo thang điểm 10 sau đó chuyển thành thang điểm chữ và thang điểm 4

STT	Điểm thành phần	Quy định	Trọng số	Ghi chú
1	Điểm thường xuyên; điểm chuyên cần; điểm thực hành;...	01 điểm	20%	Điểm trung bình của các lần đánh giá
2	Điểm kiểm tra giữa học phần	01 điểm	30%	
3	Điểm thi kết thúc học phần	01 điểm	50%	

### 11.3. Phương pháp đánh giá

- Đánh giá chuyên cần: Vấn đáp.
- Kiểm tra giữa học phần: Tự luận (Thời gian 90 phút).
- Thi kết thúc học phần: Tự luận (Thời gian 90 phút).

## 12. Phương pháp dạy và học

- Lý thuyết: Thuyết trình; dạy học dựa trên vấn đề; hoạt động nhóm.
- Thực hành: Hướng dẫn thực hành trên máy tính.

### 13. Yêu cầu học phần

- *Yêu cầu về ý thức, thái độ học tập:* Sinh viên chuẩn bị đầy đủ tài liệu trước khi đến lớp, thực hiện tốt nhiệm vụ được giảng viên phân công, ghi chép và tích cực thảo luận, xây dựng bài trên lớp, tham dự ít nhất 80% thời lượng học phần theo quy chế, thực hiện nghiêm túc nhiệm vụ về nhà theo sự hướng dẫn của giảng viên và luôn có ý thức tự học.

- *Yêu cầu về nghiên cứu tài liệu:* Sinh viên đọc giáo trình trước khi đến lớp, đọc thêm các tài liệu khác về bảo mật thông tin bằng mật mã.

- *Yêu cầu về kiểm tra, đánh giá:* Sinh viên thực hiện theo quy chế.

### 14. Tài liệu phục vụ học phần

- *Tài liệu bắt buộc:*

[1] - Trường Đại học Sao Đỏ (2018), *Giáo trình Bảo mật thông tin*.

- *Tài liệu tham khảo:*

[2] - Phan Đình Diệu (2002), *Lý thuyết mật mã và an toàn thông tin*.

### 15. Nội dung chi tiết học phần

TT	Nội dung giảng dạy	Lý thuyết	Thực hành	Tài liệu đọc trước	Nhiệm vụ của sinh viên
1	<b>Chương 1. Tổng quan về an toàn và bảo mật thông tin</b> <b>Mục tiêu chương:</b> Giải thích được các nội dung về an toàn và bảo mật thông tin, các chiến lược an toàn hệ thống, các mức bảo vệ trên mạng, cách phân loại và đánh giá một hệ mật mã. <b>Nội dung cụ thể:</b> 1.1. Nội dung của an toàn và bảo mật thông tin 1.2. Các chiến lược an toàn hệ thống 1.3. Các mức bảo vệ trên mạng 1.4. An toàn thông tin bằng mật mã 1.5. Vai trò của hệ mật mã 1.6. Phân loại hệ mật mã 1.7. Tiêu chuẩn đánh giá hệ mật mã Bài thực hành số 1	02	02	[1]	- Nghiên cứu mục tiêu, chương trình, kế hoạch dạy học học phần. - Chuẩn bị các học liệu và phương tiện học tập cần thiết. - Nghiên cứu tài liệu [1] - chương 1 mục 1.1 - 1.7. - Nghiên cứu bài thực hành số 1.



TT	Nội dung giảng dạy	Lý thuyết	Thực hành	Tài liệu đọc trước	Nhiệm vụ của sinh viên
2	<p><b>Chương 2. Các phương pháp mã hóa cổ điển</b></p> <p><b>Mục tiêu chương:</b></p> <ul style="list-style-type: none"> <li>- Giải thích được các phương pháp mã hóa, giải mã và thám mã các hệ mật mã cổ điển như mã dịch vòng, mã thay thế, mã affine, mã Vigenère, mã Hill, các hệ mã dòng.</li> <li>- Phân tích được bản rõ, bản mã, phương pháp mã hóa, giải mã, thám mã ứng với từng hệ mật mã trong hệ mã cổ điển.</li> <li>- Áp dụng vào thực hành cài đặt các hệ mật mã cổ điển trong vấn đề bảo mật thông tin.</li> </ul> <p><b>Nội dung cụ thể:</b></p> <p>2.1. Các hệ mật mã cổ điển</p> <p>2.1.1. Mã dịch vòng (Shift Cipher)</p> <p>2.1.2. Mã thay thế</p> <p>Bài thực hành số 2</p>	02	02	[1] [2]	<ul style="list-style-type: none"> <li>- Nghiên cứu tài liệu [1] - chương 2 mục 2.1.1 - 2.1.2</li> <li>- Nghiên cứu tài liệu tham khảo [2] - chương 2.</li> <li>- Nghiên cứu bài thực hành số 2.</li> </ul>
3	<p>2.1.3. Mã Affine</p> <p>2.1.4. Mã Vigenère</p> <p>Bài thực hành số 3</p>	02		[1] [2]	<ul style="list-style-type: none"> <li>- Nghiên cứu tài liệu [1] - chương 2, mục 2.1.3 - 2.1.4.</li> <li>- Nghiên cứu tài liệu tham khảo [2], chương 2.</li> <li>- Nghiên cứu bài thực hành số 3.</li> </ul>
4	<p>2.1.5. Mật mã Hill</p> <p>2.1.6. Các hệ mã dòng</p> <p>Bài thực hành số 4</p>	02	02	[1] [2]	<ul style="list-style-type: none"> <li>- Nghiên cứu tài liệu [1], chương 2, mục 2.1.5 - 2.1.6.</li> </ul>

TT	Nội dung giảng dạy	Lý thuyết	Thực hành	Tài liệu đọc trước	Nhiệm vụ của sinh viên
					- Nghiên cứu tài liệu tham khảo [2], chương 2. - Nghiên cứu bài thực hành số 4.
5	2.2. Thám mã các hệ mã cổ điển 2.2.1. Thám mã Affine 2.2.2. Thám mã thay thế 2.2.3. Thám mã Vigenère Bài thực hành số 5	02	02	[1] [2]	- Nghiên cứu tài liệu [1] - chương 2 mục 2.2.1- 2.2.3. - Nghiên cứu tài liệu tham khảo [2] - chương 2.
6	2.2.4. Tấn công với bản rõ đã biết trên hệ mật Hill 2.2.5. Thám mã hệ mã dòng xây dựng trên LFSR Bài thực hành số 6	02	02	[1] [2]	- Nghiên cứu tài liệu [1] - chương 2 mục 2.2.4 - 2.2.5 - Nghiên cứu tài liệu tham khảo [2] - chương 2. - Nghiên cứu bài thực hành số 6.
7	<b>Kiểm tra giữa học phần</b> Bài thực hành số 7	02 KT	02	[1] [2]	- Nghiên cứu tài liệu [1] - chương 2. - Nghiên cứu tài liệu tham khảo [2], chương 2. <b>Sinh viên làm bài kiểm tra giữa học phần.</b>
8	<b>Chương 3. Chuẩn mã dữ liệu DES</b> <b>Mục tiêu chương:</b> - Giải thích được nguyên tắc hoạt động của mã dữ liệu DES: thuật toán, hoán vị khởi đầu,	02	02	[1] [2]	- Nghiên cứu tài liệu [1] - chương 3 mục 3.1 - 3.5. - Nghiên cứu tài liệu tham khảo [2] - chương 3.

TT	Nội dung giảng dạy	Lý thuyết	Thực hành	Tài liệu đọc trước	Nhiệm vụ của sinh viên
	<p>khóa chuyển đổi, hoán vị mở rộng, hộp thay thế S, hộp hoán vị P, hoán vị cuối cùng, giải mã DES, phần cứng và phần mềm thực hiện DES, sự an và các chế độ hoạt động của DES.</p> <p>- Phân tích được bản rõ, bản mã, phương pháp tạo khóa, mã hóa, giải mã, thám mã DES.</p> <p>- Áp dụng vào thực hành cài đặt mã DES trong bảo mật thông tin.</p> <p><b>Nội dung cụ thể:</b></p> <p>3.1. Giới thiệu chung về DES</p> <p>3.2. Mô tả thuật toán</p> <p>3.3. Hoán vị khởi đầu</p> <p>3.4. Khóa chuyển đổi</p> <p>3.5. Hoán vị mở rộng</p> <p>Bài thực hành số 8</p>				<p>- Nghiên cứu bài thực hành số 8.</p>
9	<p>3.6. Hộp thay thế S</p> <p>3.7. Hộp hoán vị P</p> <p>3.8. Hoán vị cuối cùng</p> <p>Bài thực hành số 9</p>	02	02	[1] [2]	<p>- Nghiên cứu tài liệu [1] - chương 3, mục 3.6 - 3.8</p> <p>- Nghiên cứu tài liệu tham khảo [2] chương 3.</p> <p>- Nghiên cứu bài thực hành số 9.</p>
10	<p>3.9. Giải mã DES</p> <p>3.10. Phần cứng và phần mềm thực hiện DES</p> <p>3.11. Sự an toàn của DES</p> <p>Bài thực hành số 10</p>	02	02	[1] [2]	<p>- Nghiên cứu tài liệu [1] - chương 3, mục 3.9 - 3.11</p> <p>- Nghiên cứu tài liệu tham khảo [2] - chương 3.</p>

TT	Nội dung giảng dạy	Lý thuyết	Thực hành	Tài liệu đọc trước	Nhiệm vụ của sinh viên
					- Nghiên cứu bài thực hành số 10.
11	3.12. Tranh luận về DES 3.13. DES trong thực tế 3.14. Các chế độ hoạt động của DES Bài thực hành số 11	02	02	[1] [2]	- Nghiên cứu tài liệu [1] - chương 3 mục 3.12 - 3.14 - Nghiên cứu tài liệu tham khảo [2] - chương 3. - Nghiên cứu bài thực hành số 11.
12	<b>Chương IV. Mật mã công khai</b> <b>Mục tiêu chương:</b> - Giải thích được nguyên tắc hệ mật mã khóa công khai, hệ mật mã RSA, hệ mật mã Rabin, hệ mật mã Elgamal và các hệ tương tự, các hệ mật mã dựa trên các bài toán NP-đầy đủ. - Phân tích được bản rõ, bản mã, phương pháp mã hóa, giải mã, thám mã hệ công khai. - Phân biệt được các hệ công khai so với hệ bí mật. - Áp dụng hệ mật mã công khai vào thực hành cài đặt chương trình thử nghiệm. <b>Nội dung cụ thể:</b> 4.1. Giới thiệu về hệ mật mã khóa công khai 4.2. Hệ mật RSA 4.2.1. Thuật toán RSA	02	02	[1] [2]	- Nghiên cứu tài liệu [1] - chương 4 mục 4.1 - 4.2. - Nghiên cứu tài liệu tham khảo [2] - chương 4. - Nghiên cứu bài thực hành số 12.

TT	Nội dung giảng dạy	Lý thuyết	Thực hành	Tài liệu đọc trước	Nhiệm vụ của sinh viên
	4.2.2. Một số thuật toán triển khai trong RSA 4.2.3. Độ an toàn của hệ mật RSA Bài thực hành số 12				
13	4.3. Hệ mật mã Rabin 4.4. Hệ mật Elgamal và các hệ tương tự 4.5. Các hệ mật mã dựa trên các bài toán NP- đầy đủ Bài thực hành số 13	02	02	[1] [2]	- Nghiên cứu tài liệu [1] - chương 4 mục 4.3 - 4.5. - Nghiên cứu tài liệu tham khảo [2] - chương 4. - Nghiên cứu bài thực hành số 13.
14	<b>Chương V. Các sơ đồ chữ ký số</b> <b>Mục tiêu chương:</b> - Giải thích được sơ đồ chữ ký số, sơ đồ chữ ký RSA, Sơ đồ chữ ký Elgamal, sơ đồ chữ ký không phủ định được, hàm băm và chữ ký số. - Phân tích được bản rõ, bản mã, phương pháp mã hóa, giải mã hệ chữ ký và hàm băm. - Áp dụng sơ đồ chữ ký số vào thực hành cài đặt chương trình thử nghiệm. <b>Nội dung cụ thể:</b> 5.1. Định nghĩa sơ đồ chữ ký số 5.2. Sơ đồ chữ ký RSA 5.3. Sơ đồ chữ ký ELGAMAL Bài thực hành số 14	02	02	[1] [2]	- Nghiên cứu tài liệu [1] – chương 5 mục 5.1 - 5.3. - Nghiên cứu tài liệu tham khảo [2] - chương 5. - Nghiên cứu bài thực hành số 14.

TT	Nội dung giảng dạy	Lý thuyết	Thực hành	Tài liệu đọc trước	Nhiệm vụ của sinh viên
15	5.4. Sơ đồ chữ ký không phủ định được 5.5. Hàm băm và chữ ký số Bài thực hành số 15	02	02	[1] [2]	- Nghiên cứu tài liệu [1] - chương 5, mục 5.4 - 5.5. - Nghiên cứu tài liệu tham khảo [2] - chương 5. - Nghiên cứu bài thực hành số 15.

Hải Dương, ngày 14 tháng 8 năm 2018

KT. HIỆU TRƯỞNG  
PHÓ HIỆU TRƯỞNG



TS. Nguyễn Thị Kim Nguyễn

KT. TRƯỞNG KHOA  
PHÓ TRƯỞNG KHOA

Trần Duy Khánh

TRƯỞNG BỘ MÔN

Phạm Văn Kiên