Course Specification

A- Affiliation

Relevant program: Computer Science
Department offering the program: Mathematics
Department offering the course: Mathematics
Academic year/level: Fourth level/ First Semester
Date of specifications approval: 9 /12 / 2015, No. (390) and updated 10/1/2018 meeting no.(419).

B - Basic information

Title:	Code:	Year/level:
Computer security techniques	453MC	Fourth level/ First Semester
	Lectures: 2h/week	Tutorial: —
	Practical: —	Total: 2 h/week

C - Professional information

1 – Course Learning Objectives:

At the end of this course, the students must be able to:

The "Computer Security Techniques" course is a fourth year undergraduate course that introduces students to the subject of Information Security from the technical point of view. The purpose of this course is to help students in learning the principles of computer information security in general and of constructing secure systems in particular. It familiarizes students with the aspects of information security: security attacks, security mechanisms, and security services. Since cryptographic techniques underlie many of the security mechanisms in use, this course covers the development, use and management of such techniques. It also introduces authentication techniques, access control mechanisms, and how security assurance is achieved on computer networks.

2 - Intended Learning Outcomes (ILOS)

a - Knowledge and understanding:

At the end of this course, the students must be able to:

a1- To know the principles of computer and information security and describe the types of attacks and malicious code that may be used against a computer system; threats and countermeasures

a2- Describe similarities and differences among various symmetric and public key cryptographic techniques.

a3- Explain discretionary , mandatory, and role-based access control models.

a4-Determine Technologies and concepts used for providing secure communications channels, secure internetworking devices, and network medium and describe the risk assessment techniques and the types of security policies.

a5- Describe the role and types of intrusion detection systems, firewalls, and physical security concepts.

b - Intellectual skills:

At the end of this course, the students must be able to:

b1- Hypothesize the information security needs of an organization

b2- Organize security threats to networked systems and make decisions regarding network security practice.

c - Practical and professional skills:

At the end of this course, the students must be able to:

c1-Examine Implement cryptography algorithms and technique.

d - General skills:

At the end of this course, the students must be able to:

d1- Communication with others to Discuss high awareness of how to protect data and resources from disclosure, to guarantee the authenticity of data and messages and to protect computer systems from network-based attacks.

d2- Using internet to Develop research skills and extend professional knowledge to clarify problems and take responsibility for furthering own learning.

3 – Contents

Topic	Lecture hours	Tutorial hours	Practical hours
Overview of Information Security-	2	-	-
Attackers and their attacks	2		
Security Basics	2	-	-
Traditional Symmetric-Key Ciphers	2		
Modern Symmetric-Key Ciphers	2	-	-
Asymmetric Key Cryptography.	2		
Revision and Mid term	2		
Message Integrity and Authentication	2	-	-
Hash Functions and Digital Signature.	2		
Entity Authentication	2	-	-
Key Management	2		
Securing the Network Infrastructure.	2		
Operational Security	2	-	-
Security Policies and Procedures	2		
Total hours	28	-	-

4 - Teaching and Learning methods:

Intended Learning Outcomes		Lecture	Presentations & Movies	Discussions & Seminars	Problem solving	Brain storming
Knowledge & Understanding	a1. To know the principles of computer and information security and describe the types of attacks and malicious code that may be used against a computer system; threats and counter measures.	✓		✓		
	a2. Describe similarities and differences among various symmetric and public key cryptographic techniques.	✓		✓		✓
	a3. Explain discretionary, mandatory and role-based access control models.	✓		✓		
	a4. Determined Technologies and concepts used for providing secure communications channels secure internetworking devices, and network medium and describe the risk assessment techniques and the types of security policies.	✓		✓		
	a5. Describe the role and types of intrusion detection systems, firewalls, and physical security concepts.	✓		✓		✓
Intellectual Skills	b1. Hypothesize the information security needs of an organization.	✓	✓		✓	
	b2. Organize security threats to networked systems and make decisions regarding network security practice.	✓			✓	
Practical and professional skills	c1. Examine Implement cryptography algorithms and techniques.	✓			✓	
General Skills	d1. Communication with others to Discuss high awareness of how to protect data and resources from disclosure, to guarantee the authenticity of data and messages and to protect computer systems from network-based attacks.	✓	✓	✓		✓
	d2. Using internet to Develop research skills and extend professional knowledge to clarify problems and take responsibility for furthering own learning.		✓	✓		

5- Students' Assessment Methods and Grading:			
Tools:	To Measure	Time schedule	Grading
Mid-Term Exam	a1- a2- a3- a4- a5- b1- b2- b3- c1- c2	Week 7	14 %
Oral exam	a1- a2- a3- a4- a5- b1- b2- b3- d1- d2	Week 15	14 %
Practical exams	a3, c1, d2	Week 15	24%
Written exam	a1- a2- a3- a4- a5- b1- b2- b3- c1- c2	Start of the sixteenth week	48 %
Total			100 %

6-Course matrix

Topic	Knowledge and understanding						Intellectual skills		Practical and professional skills	General skill	
	a1	a2	a3	a3	a4	a5	b1	b2	c1	d1	d2
Overview of Information Security-				x	x						
Attackers and their attacks				x			x	X			
Security Basics		x									
Traditional Symmetric-Key Ciphers			X	x				X			X
Modern Symmetric-Key Ciphers	x		X			x	x		x	x	
Asymmetric Key Cryptography.	x					x					
Revision and Mid term				x				X			X
Message Integrity and Authentication		x			x		x			x	
Hash Functions and Digital Signature.									X		
Overview of Information Security-								x			
Attackers and their attacks				x		x		x			
Entity Authentication	x	x		x							X
Key Management		x							x	x	X
Securing the Network Infrastructure.		x		x					x		
Operational Security			X						x		
Security Policies and Procedures								x		x	

7- List of references:

7-1 Course notes

- Notes approved by Math. Department.

7-2 Required books.

- B. A. Forouzan, Cryptography & Network Security: McGraw-Hill, Inc., 2007.

- S. William and W. Stallings, Cryptography and Network Security, 4/E: Pearson Education India, 2006.

7-3 Recommended books.

- A. Conklin, G. White, C. Cothren, D. Williams, and R. L. Davis, Principles of computer security: security+ and beyond: McGraw-Hill, Inc., 2004.

- C. P. Pfleeger and S. L. Pfleeger, Security in computing: Prentice Hall Professional Technical Reference, 2002.

7-4 Periodicals, Web sites, etc.

http://its.ucsc.edu/security/training/intro.html

8- Facilities required for teaching and learning:

Black board, white board and data show.

Course coordinator: **Dr. Yasser Maher**

Head of the Department: **Prof. Dr. Abdel Kareem Soliman**

Date: 9 / 12 /2015 Updated 2018