



Date: 9 / 12 / 2015

Updated 2018

Course Specification

A- Affiliation

Relevant program:	Computer Science
Department offering the program:	Mathematics
Department offering the course:	Mathematics
Academic year/level:	Fourth level / Second 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:
Cryptography	466 MC	Fourth level / Second Semester
Teaching Hours: 42 h	Lectures:	Tutorial: —
	2h/week	
	Practical:	Total: 3 h/week
	2h/week	

C - Professional information

1 – Course Learning Objectives:

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

Studying how to design coding system. Know how coding system work. Studying some important codes. Apply effectively information technology relevant to the field.

2 - Intended Learning Outcomes (ILOS)

a - Knowledge and understanding:

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

- a1. Identify the ability of the student to design coding system.
- a2. To know how coding system works.
- a3. Define number systems and how to create new codes.

b - Intellectual skills:

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

- b1. Confirm students in some related courses.
- b2. Design discussion concerning assigned problems



b3. Construct mental ability for the student

c - Practical and professional skills:

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

- c1. Show techniques and tools considering scientific ethics.
- c2. Analyze problems using a range of formats and approaches.
- c3. Show the concepts and methods of computer science, mathematics, and statistics to the solution of the real problems in professional practice.

d - General skills:

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

- d1. Communication with others, set tasks and solve problems on scientific basis.
- d2. Working in groups effectively, manage time, collaborate and communicate with others positively.
- d3. Time management to Analysis of results
- d4. Lifelong learning.

3 – Contents			
Topic	Lecture hours	Tutorial hours	Practical hours
Overview and Introduction to Cryptography	2	-	2
Mathematical Background	2	-	2
Mathematical Background	2	-	2
Symmetric Cryptosystems	2	-	2
Stream Ciphers	2	-	2
Block Ciphers	2	-	2
Mid-Term Examination and Feistel Ciphers	2	-	2
Multiple Encryption	2	-	2
DES/AES	2	-	2
Hash Functions	2	-	2
More on Hash Functions	2	-	2
Data Integrity, Authentication, MAC	2	-	2
Asymmetric Cryptosystems	2	-	2
Algorithmic Number Theory	2	-	2
Total hours	28	-	28



4 - Teaching and Learning methods:

Intended Learning Outcomes			Lecture	Presentations & Movies	Discussions & Seminars	Practical	Problem solving	Brainstorming
Knowledge & Understanding	a1	Identify the ability of the student to design coding system.	✓	✓	✓	✓		
	a2	To know how coding system works.	✓	✓		✓		
	a3	Define number systems and how to create new codes.	✓	✓	✓	✓		
Intellectual Skills	b1	Confirm students in some related courses.	✓	✓	✓	✓	✓	
	b2	Design discussion concerning assigned problems.	✓	✓	✓			
	b3	Construct of mental ability for the student						✓
Practical and professional skills	c1	Show techniques and tools considering scientific ethics.			✓	✓		
	c2	Analyze problems using a range of formats and approaches.			✓	✓	✓	
	c3	Show the concepts and methods of computer science, mathematics, and statistics to the solution of the real problems in professional practice.	✓		✓	✓	✓	
General Skills	d1	Communication with others, set tasks and solve problems on scientific basis.	✓		✓	✓	✓	✓
	d2	Working in groups effectively, manage time, collaborate and communicate with others positively.	✓		✓	✓	✓	
	d3	Time management to Analysis of results.		✓	✓	✓		
	d4	life long learning.	✓			✓	✓	

5- Students' Assessment Methods and Grading:

Tools:	To Measure	Time schedule	Grading
Mid-Term Exam	a1,a2,a3,c2,c3,d1,d4	Week 7	14 %
Oral exam	a1,a2,a3,b2,d3,d4	Week 15	14 %
Practical exams	a1,a2,a3,b2,c1,c2,c3,d3,d2	Week 15	24 %
Written exam	a1,a2,a3,c2,c3,d1,d4	Week 16	48 %
Total			100 %



6- Course Matrix

Topic	Knowledge and understanding			Intellectual skills			Practical and professional skills			General skills			
	a1	a2	a3	b1	b2	b3	c1	c2	C3	d1	d2	d3	d4
Overview and Introduction to Cryptography	x												x
Mathematical Background		x					x						
Mathematical Background			x						x			x	
Symmetric Cryptosystems						x							
Stream Ciphers										X			
Block Ciphers					X								
Mid-Term Examination and Feistel Ciphers							x						
Multiple Encryption	x		x	x			x	x				X	
DES/AES											x		
Hash Functions													x
More on Hash Functions						x							x
Data Integrity, Authentication, MAC	x							x			x		
Asymmetric Cryptosystems												X	
Algorithmic Number Theory				x					x				x

7- List of references:

7-1 Course notes

- Notes approved by Math. Department.

7-2 Required books.

- Paar, C. and Pelzl, J. (2010). *Understanding cryptography*. Berlin: Springer.

7-3 Recommended books.

- Ferguson, N., Schneier, B. and Kohno, T. (2012). *Cryptography Engineering*. Chichester: John Wiley & Sons, Inc.

7-4 Periodicals, Web sites, etc.

- <http://www.brighthub.com/computing/smb-security/articles/80137.aspx> [Accessed 29 Oct. 2015].
- <http://www.tutorialspoint.com/cryptography> [Accessed 29 Oct. 2015].
- <https://www.cs.auckland.ac.nz/~pgut001/tutorial> [Accessed 29 Oct. 2015].

8- Facilities required for teaching and learning:

- Data Show Device
- Whiteboard

Course coordinator: Dr. Mosab abd el-hameed hassaan

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

Date : 9 / 12 /2015

Updated 2018