Kingdom of Saudi Arabia
National Commission for
Academic Accreditation & Assessment

المملكـة العربيـة السعوديـة
الهيئـــة الوطنيـــة للتقـويـم
والاعــتــمـــاد الأكـــاديـمـــي

ATTACHMENT 5.

Kingdom of Saudi Arabia

The National Commission for Academic Accreditation & Assessment

14014604-3 Introduction to Cryptography

(CS)

Course Specifications

Institution Umm Al Qura University	Date : 16/04/2016
College/Department: College of Computers and Information Systems / Computer Science Dep.	

A. Course Identification and General Information

1. Course title and code:
14014604-3 Introduction to Cryptography

2. Credit hours: 3 (2 lecture, 2 lab,)

3. Program(s) in which the course is offered.
(If general elective available in many programs indicate this rather than list programs)
Elective course in Computer Science program.

4. Name of faculty member responsible for the course
Dr. Khaled Tarmissi

5. Level/year at which this course is offered: 5th year / level 9 or 10

6. Pre-requisites for this course (if any)
14011802-3 Discrete Structures II

7. Co-requisites for this course (if any)
N/A

8. Location if not on main campus

9. Mode of Instruction (mark all that apply)

a. traditional classroom	X	What percentage?	100
b. blended (traditional and online)		What percentage?	
c. e-learning		What percentage?	
d. correspondence		What percentage?	
f. other		What percentage?	

Comments:

B Objectives

1. What is the main purpose for this course?

Cryptography provides important tools for ensuring the privacy, authenticity, and integrity of the increasingly sensitive information involved in modern digital systems. Nowadays, core cryptographic tools, including encryption, message authentication codes, digital signature, key agreement protocols, etc., are used behind millions of daily on-line transactions. In this course, we will unveil some of the "magic" of cryptography.

2. Briefly describe any plans for developing and improving the course that are being implemented. (e.g. increased use of IT or web based reference material, changes in content as a result of new research in the field)

- use some of the web based tools and material

C. Course Description (Note: General description in the form used in Bulletin or handbook)

Course Description:
This course introduces the basic theory of cryptograph; it is an introductory course on methods, algorithms, techniques, and tools of cryptography. It includes the history of cryptography, algorithmic and mathematical aspects of cryptographic methods and protocols, such as classical ciphers and their decryption, secret-key cryptography, public-key cryptography, hash functions.

1. Topics to be Covered		
List of Topics	No. of Weeks	Contact hours
1. Introduction and Overview Classical Cryptography	2	6

2. Mathematics of Cryptography	1	3
3. More Classical ciphers :	1	3
4. Stream cipher	2	6
5. Block cipher	2	6
6. Public-key Cryptography	4	12
7. Hash Functions	1	3
8. Secret Sharing	1	3

2. Course components (total contact hours and credits per semester):

	Lecture	Tutorial	Laboratory or Studio	Practical	Other:	Total
Contact Hours	28		28			56
Credit	3					

3. Additional private study/learning hours expected for students per week. 0

4. Course Learning Outcomes in NQF Domains of Learning and Alignment with Assessment Methods and Teaching Strategy

On the table below are the five NQF Learning Domains, numbered in the left column.

First, insert the suitable and measurable course learning outcomes required in the appropriate learning domains (see suggestions below the table). **Second**, insert supporting teaching strategies that fit and align with the assessment methods and intended learning outcomes. **Third**, insert appropriate assessment methods that accurately measure and evaluate the learning outcome. Each course learning outcomes, assessment method, and teaching strategy ought to reasonably fit and flow together as an integrated learning and teaching process. (Courses are not required to include learning outcomes from each domain.)

Code #	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge**		
1.1	Students will be aware of, and be able to identify the concept of cryptography and computer security.		
1.2	Learn fundamental concepts in mathematics of cryptography.		
1.3	Understand basics of different cipher algorithm types.		
1.4			
1.5			
2.0	**Cognitive Skills**		
2.1	Ability to apply different cipher algorithm principles in the construction of crypto systems.		
2.2			
2.3			
3.0	**Interpersonal Skills & Responsibility**		
3.1	An understanding of professional, ethical, legal, security, and social issues and responsibilities		
3.2			
4.0	**Communication, Information Technology, Numerical**		
4.1	An ability to apply design and development principles in the security systems .		
4.2			
5.0	**Psychomotor**		
5.1			
5.2			

5. Map course LOs with the program LOs. (Place course LO #s in the left column and program LO #s across the top.)					
	Program Learning Outcomes				

Course LOs #	(Use Program LO Code #s provided in the Program Specifications)											
	1.1	1.2	1.3	1.4	2.1	2.2	2.3	3.1	4.1	4.2	5.1	
1.1	P											
1.2		P										
1.3		P	P									
2.1					P							
3.1					P			P				
4.1									P			

6. Schedule of Assessment Tasks for Students During the Semester

	Assessment task (e.g. essay, test, group project, examination, speech, oral presentation, etc.)	Week Due	Proportion of Total Assessment
1	Assignment 1	2	5
2	Assignment 2	4	5
3	Assignment 3	6	5
4	Assignment 4	10	5
5	Assignment 5	12	5
6	Mid Term	8	20
7	Project	9	15
8	Final Exam	16	40

D. Student Academic Counseling and Support

1. Arrangements for availability of faculty and teaching staff for individual student consultations and academic advice. (include amount of time teaching staff are expected to be available each week)

4 Office hours per week

E Learning Resources

1. List Required Textbooks Cryptography and Network Security: Principles and Practice (5th Edition), by William Stallings (Jan 2010), PEARSON, ISBN-10: 0136097049
2. List Essential References Materials (Journals, Reports, etc.) Cryptography Theory & Practice by Douglas Stinson
3. List Recommended Textbooks and Reference Material (Journals, Reports, etc) Applied Cryptography by Bruce Schneier
4. List Electronic Materials, Web Sites, Facebook, Twitter, etc. 1. Cryptography I - Stanford University | Coursera 2. Applied Cryptography and Encryption Class Online
5. Other learning material such as computer-based programs/CD, professional standards or regulations and software. https://www.cryptool.org/en/

F. Facilities Required

Indicate requirements for the course including size of classrooms and laboratories (i.e. number of seats in classrooms and laboratories, extent of computer access etc.)
1. Accommodation (Classrooms, laboratories, demonstration rooms/labs, etc.) Lecture room Computer lab
2. Computing resources (AV, data show, Smart Board, software, etc.) data show
3. Other resources (specify, e.g. if specific laboratory equipment is required, list requirements or attach list)

G   Course Evaluation and Improvement Processes

1 Strategies for Obtaining Student Feedback on Effectiveness of Teaching A student-feedback form is distributed at the end of the course
2 Other Strategies for Evaluation of Teaching by the Instructor or by the Department
3 Processes for Improvement of Teaching
4. Processes for Verifying Standards of Student Achievement (e.g. check marking by an independent member teaching staff of a sample of student work, periodic exchange and remarking of tests or a sample of assignments with staff at another institution)
5 Describe the planning arrangements for periodically reviewing course effectiveness and planning for improvement.

Name of Instructor: khaled Tarmissi

Signature: ______________________________ Date Report Completed: ____________

Name of Course Instructor ____

Program Coordinator:____

Signature: ______________________________ Date Received: ____________________