جامعة المجمعة
Majmaah University

Course Specifications

Institution: College of Science at Az Zulfi

Academic Department : Department of Computer Science and Information

Programme : Computer Science and Information

Course : Cryptography and Information Security

Course Coordinator : Assoc. Prof. Hassan Aly

Programme Coordinator : Assoc. Prof. Yosry Azzam

Course Specification Approved Date : 22/ 12 / 1435 H

This form compatible with NCAAA 2013 Edition

A. Course Identification and General Information

1 - Course title :	Cryptography and Information Security	Course Code:	CSI-423
2. Credit hours :	3 (3 lecture + 1 lab)		
3 - Program(s) in which the course is offered:	Computer Science and Information		
4 – Course Language :	English		
5 - Name of faculty member responsible for the course:	Dr. Hassan Aly		
6 - Level/year at which this course is offered :	8th level/ 5		
7 - Pre-requisites for this course (if any) :	• Design and Analysis of Algorithms (CSI 321)		
8 - Co-requisites for this course (if any) :	N/A		
9 - Location if not on main campus :	College of Science at AzZulfi		

10 - Mode of Instruction (mark all that apply)

A - Traditional classroom	√	What percentage?	**80 %**
B - Blended (traditional and online)	√	What percentage?	**10 %**
D - e-learning	√	What percentage?	**10 %**
E - Correspondence		What percentage?	**……. %**
F - Other		What percentage?	**…….%**

Comments :

One-tenth of the course is presented mainly inside lab discussions on the implementation of the security protocols presented in the course.

B Objectives

What is the main purpose for this course?

The aim of this course is to facilitate understanding of the inherent strengths and limitations of cryptography, especially when used as a tool for information security. Armed with this knowledge, student should be able to make more informed decisions when building secure systems.

The course covers various aspects of symmetric and asymmetric cryptography. While some topics will be dealt with in more detail, the course will attempt to provide a broad coverage of possibly all the core areas of cryptography. The students will be expected to implement and analyze some simple cryptographic schemes and read various articles. To understand the principles of encryption algorithms; conventional and public key cryptography. To have a detailed knowledge about authentication, hash functions and application level security mechanisms. The main course objectives can be outlined in the following points:

1. Develop an understanding of information assurance as practiced in computer systems and network applications.
2. Gain familiarity with prevalent network and distributed system attacks and defenses against them.
3. Develop an understanding of cryptography, how it has evolved, and some key encryption techniques

used today.

4. Develop an understanding of security polices (such as authentication, integrity, and confidentiality), as well as protocols to implement such policies in the form of message exchanges.

Briefly describe any plans for developing and improving the course that are being implemented :

1. Using group discussion through the internet with course attending students.
2. Updating the materials of the course to cover the new topics of the field.
3. Increasing the ability of the students to implement the algorithms that are presented in the course.

C. Course Description

1. Topics to be Covered

List of Topics	No. of Weeks	Contact Hours
1. Overview: computer security concepts, the OSI security Architecture, Security attacks, Security mechanisms, Model of network security.	1	4
2. Classical Encryption Techniques: Symmetric cipher model, substitution techniques, Transposition techniques, Rotor machines.	2	8
3. Block ciphers and DES: Block cipher principles, DES, the strength of DES, Differential and linear cryptanalysis, Block cipher design principles.	2	8
4. Review of Mathematical concepts: Divisibility, Division algorithm, the Euclidean algorithm, Modular arithmetic, Groups, rings, fields. Finite Fields.	1	4
5. Advanced Encryption Standard: Finite Field Arithmetic, AES structures, AES transformation, AES key expansion.	2	8
6. Block cipher operation: Multiple and triple DES, ECB, CBC, CFB, OFB, Counter, and XTS mode of encryptions.	1	4
7. Review of Number theory concepts: prime numbers, Fermat's and Euler's theorem, testing primality, Chinese remainder theorem, Discrete logarithms.	1	4
8. Public key Cryptography and RSA: principles of public key cryptosystems, The RSA algorithm.	1	4

9. Other public key cryptosystem: DH scheme, ElGamal cryptosystem.	1	4
10. Cryptographic Hash functions: Applications of Cryptographic hash functions, simple hash functions, SHA-3, Digital signatures. Applications in authentication.	3	12

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

	Lecture	Tutorial	Laboratory	Practical	Other:	Total
Contact Hours	45	-	15	-	-	60
Credit	45	-	-	-	-	45

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

5 Hours

The private self-study of the attending student is crucial for this course. It includes:

- reading carefully the topics in the textbook or reference book,
- implementing security algorithms using C++ ,
- browsing the websites that concerned with the course,
- solving the exercises that are assigned in each chapter,
- discussing the course topics with the instructor in his office hours,

The total workload of the student in this course is then: 60 + 5 x 15 = 135 work hours.

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

	NQF Learning Domains And Course Learning Outcomes	Course Teaching Strategies	Course Assessment Methods
1.0	**Knowledge**		
1.1	Assess the implications of cryptography in terms of privacy, security, and ethical issues.	Lectures Lab demonstrations Case studies Individual presentations	Written Exam Homework assignments Lab assignments Class Activities Quizzes
1.2	Evaluate and compare encryption standards and techniques.		
1.3	define the basic terminology , notation, and concepts of computer security.		
2.0	**Cognitive Skills**		
2.1	Compile, integrate and appraise various methods of encryption information.	Lectures Lab demonstrations Case studies Individual presentations Brainstorming	Written Exam Homework assignments Lab assignments Class Activities Quizzes Observations
2.2	Measure and determine appropriate encryption standards and techniques to suite specific business and technological needs.		
3.0	**Interpersonal Skills & Responsibility**		
3.1	Analyze strengths and weaknesses in different systems.	Small group discussion Whole group discussion Brainstorming Presentation	Written Exam Homework assignments Lab assignments Class Activities Quizzes
3.2	Design security protocols and methods to solve specified security problem.		
4.0	**Communication, Information Technology, Numerical**		
4.1	work cooperatively in a small group environment.	Small group discussion Whole group discussion Brainstorming Presentation	Observations Homework assignments Lab assignments Class Activities
4.2	keep your computer safe from different threats.		
5.0	**Psychomotor**		
5.1	**..**	....	....

5. Schedule of Assessment Tasks for Students During the Semester:

	Assessment task	Week Due	Proportion of Total Assessment
1	First written mid-term exam	6	15%
2	Second written mid-term exam	12	15%
3	Presentation, class activities, and group discussion	Every week	10%
4	Homework assignments	After each chapter	10%
5	Implementation of presented protocols	Every two weeks	10%
6	Final written exam	16	40%
7	Total		100%

D. Student Academic Counseling and Support

Office hours: Sun: 10-12, Mon. 10-12, Wed. 10-12
Office call: Sun. 12-1 and Wed 12-1

Email: h.haly@mu.edu.sa
Mobile: 0538231332

E. Learning Resources

1. List Required Textbooks :

- W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, Six Edition. 2013.

2. List Essential References Materials :

- C. Kaufman, Radia Perlman, Mike Speciner, Network Security, Private Communication in a PublicWorld, Prentice Hall, 2002

3. List Recommended Textbooks and Reference Material :

- Journal of cryptology.

4. List Electronic Materials :

- www.iacr.org

5. Other learning material :

- Video and presentation are available with me

F. Facilities Required

1. Accommodation

- Classroom and Labs as that available at college of science at AzZulfi are enough.

2. Computing resources

- Smart Board

3. Other resources

- N/A

G Course Evaluation and Improvement Processes

1 Strategies for Obtaining Student Feedback on Effectiveness of Teaching:

- Questionnaires (course evaluation) achieved by the students and it is electronically organized by the university.
- Student-faculty management meetings.

2 Other Strategies for Evaluation of Teaching by the Program/Department Instructor :

- Discussion within the staff members teaching the course

- Departmental internal review of the course.

3 Processes for Improvement of Teaching :

- Periodical departmental revision of methods of teaching.
- Monitoring of teaching activates by senior faculty members.
- Training course.

4. Processes for Verifying Standards of Student Achievement

- Reviewing the final exam questions and a sample of the answers of the students by others.
- Visiting the other institutions that introduce the same course one time per semester.
- Watching the videos of other courses by international institutions.

5 Describe the planning arrangements for periodically reviewing course effectiveness and planning for improvement :

- Course evaluation
- Exam evaluation
- Improvement plan

Course Specification Approved
Department Official Meeting No (6) Date 22 / 12 / 1435 *H*

Course's Coordinator		**Department Head**	
Name :	Hassan Aly	***Name :***	Yosry Azzam
Signature :	....	***Signature :***	....
Date :	22/ 12 / 1435 *H*	***Date :***	…./ … / …… *H*