Kingdom of Saudi Arabia

Ministry Of Higher Education

Majmaah University

Deanship of Quality assurance

and Human Development

Course Specification

Introduction to Cryptography and information security

CIS 445-Z

(Summary)

1431/1432

Course Specification

Institution : **Majmaah University**
College/Department : **College of Science in AL-Zulfi / Computer Science& Information**

A- Course Identification and General Information

1. Course title and code**: Introduction to Cryptography and information security / CIS 445-Z**
2. Credit hours: 3
4. Name of faculty member responsible for the course : **Mohammad Al-Othman**
5. Level/year at which this course is offered**: 8 level / 4 year**
6. Co-requisites for this course (if any) : **CIS 313**
7. Location if not on main campus **: College of Science in AL-Zulfi**

B- Objectives

1. Introduce students with the importance of security for computer systems.
2. Introduction to security goals and the services of security system.
3. Explain available methods of defense.
4. Distinguish between Cryptography and Steganography.
5. Describe classical encryption techniques (Caesar, Mono-alphabetic, and poly-alphabetic ciphers)
6. Describe transposition techniques.
7. Introduce Data Encryption Standard algorithm with great details.
8. Compare between different symmetric key encryption algorithms.
9. Introduce Public-key encryption concept and detailed RSA algorithm
10. Introduce students with authentication service , IP security, and web security
11. Introduce students with malicious programs such as viruses, worms, logic bombs and Trojan horses.
12. Introduction to firewalls.

C- Course Description (Note: General description in the form to be used for the Bulletin or Handbook should be attached)

1. Topics to be Covered		
Introduction	**No Of Week**	Contact hours
Classical Encryption Techniques	2	6
Block Cipher and Data Encryption Standard	1	3
Advanced Encryption Standard	1	3
Contemporary Symmetric Ciphers	1	3
Confidentiality using symmetric encryption	1	3
Public - key encryption and RSA	2	6
Message Authentication and Hash Functions	1	3
Digital Signatures and Authentication Protocols	2	6
Network Security Practice	1	3
System Security	1	3
Projects Discussion	1	3

2. Course components (total contact hours per semester):				
Lecture: 42	Tutorial:	Laboratory:0	Practical/Field work/Internship	Other:

3. Additional private study/learning hours expected for students per week. (This should be an average: for the semester not a specific requirement in each week)

D- E-Learning Resources.

1. Required Text(s) : • **Cryptography and Network Security Principles and Practices, 5th Ed., William Stallings, Printice Hall, 2010**
2. Essential References : • **"Handbook of Applied Cryptography", by Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. CRC Press, 1996.**
3- Recommended Books and Reference Material (Journals, Reports, etc) (Attach List) • **Charles P. Pfleeger and Shari L. Pfleeger . Security in Computing. Prentice Hall, (3rd Ed. 2003), (4th Ed. 2006).**
4-.Electronic Materials, Web Sites etc
5- Other learning material such as computer-based programs/CD, professional standards/regulations

E- Assessment

Assessment Policy		
Assessment Type	**Week**	**Weight**
First Exam	**6**	**15%**
Second Exam	**12**	**15%**
Quizzes Home works and Project		**10%**
Final Exam		**60%**
Total		**100%**