الجامعـــــــــة الهاشـــميـــــــــة
كلية الاميـر الحسين بـــــن عبدالله الثاني لتكنولوجيا المعلـــومات

The Hashemite University
Prince Al-Hussein Bin Abdullah II Faculty for Information Technology
Department of Software Engineering

Course Syllabus
1st Semester 2012/2013

Course Title: Information System Security **Course Number:** 1003480 **Prerequisite:** 1002281	**Assessment and Course Grade:** • First Exam 20% • Second Exam 20% • Final Exam 50% • Programming Assignments (Homework) 10%, there will be about 2 assignments
Instructor: Dr. Ala Mughaid **Office NO**: IT 126 **Contact Info**: ala.mughaid@hu.edu.jo,	
Office Hours:(Sun,Tuesday,Thursday) 11-12	

Course Description

The OSI security architecture, security attacks, security mechanisms, symmetric ciphers, Classical encryption techniques, data encryption standards (DES), primary numbers, introduction to number theory, public-key cryptosystems, RSA algorithm, message authentication, digital signature, Hash function.

Textbook

Stalling, W., "Cryptography and Network Security". 4 th Ed., Prentic Hall,(2006)

Additional Reading

- William Stallings, Network Security Essentials: Applications and Standards Prentice Hall, Hardcover, Published November 1999, ISBN 0130160938.
- Bruce Schneier and John Wiley, Secrets and Lies: Digital Security in a Networked World, Published August 2000, ISBN 0471253111

Course Objectives

On successful completion of this course the students should be able to:

- Describe the risks of insufficient information protection and the need for computer security.
- Describe the threads posed to information security and discuss the more common attacks associated with those threats.
- Understand the principles and practices of cryptographic techniques.
- Compare and contrast symmetric and asymmetric encryption.
- Compare between substitutions, transposition ciphering techniques.

- Learning various data ciphering techniques.
- Apply appropriate security techniques to solve security problems.
- Implement practical security policies and describe how to assess their effectiveness.
- Explain the need of Hash functions and message authentication code.
- Describe the importance of Digital Signature in electronic documents and messages.

Course Plan

Week no.	Topic	chapters
1	**Introduction:** Defining Security What is modern Cryptography Security Attacks Security Mechanisms.	
2 and 3	**Classical Encryption Techniques.** Symmetric Cipher model. Substitution Techniques. Transposition Techniques.	
4 and 5	**Block Ciphers and Data Encryption Standards.** Block Cipher Principles. The Data Encryption Standard. The strength of DES. Multiple Encryption and Triple DES.	
First Exam		
6	**Introduction to Number Theory** Prime Numbers. Fermat's and Euler's Theorem.	
Programming assignment 1		
7 and 8	**Public-Key Cryptography and RSA.** Principles of Public-key Cryptosystems. The RSA Algorithm.	
9	**Key Management**	
Second Exam		
10 and 11	**Message Authentication and Hash Functions**. Authentication Requirements. Authentication Functions. Message Authentication Codes. Hash Function.	
Programming assignment 2		
12 and 13	**Digital Signatures and Authentication Protocols** Digital Signatures Authentication Protocols. Digital Signatures Standard.	
14 and 15	**Hash Algorithm** Secure Hash Algorithm.	
Final Exam		