Faculty of Science & Information Technology

Department: Computer Science

COURSE SYLLABUS

Short Description
Student's Copy

One copy of this course syllabus is provided to each student registered in this course. It should be kept secure and retained for future use.

I. Course Information

1.	Course Title	:	**Practical Aspects of Information Security**
2.	Course Code	:	1306755
3.	Credit Hours	:	3
4.	Prerequisite	:	None
5.	Corequisite	:	None

2. Instructor Information

1.	Instructor	:	Dr. Khaled W. Mahmoud
2.	Office	:	214D
3.	Phone	:	ext(1417)
4.	Email	:	**k.w.mahmoud@zu.edu.jo**
5.	Office Hours		**Sun, Tue, Thu, 1- 2 Mon, Wed : 12:30 -2:00**

3. Class Time and Place

1.	Class Days and Time	:	Sun 4-7 P M
2.	Class Location	:	304 H
3.	Lab Days and Time	:	------
4.	Lab Location	:	------

4. Course Policies

University regulations are applied to this course, regarding Class Attendance; Punctuality, Exam, Makeup Exams; Absence with permission; Penalties for Cheating; and Policies for Assignment and Projects. Students should be aware of all those in addition to other rules and regulations.

5. Resources

Main Reference Text Book:

Charles P. Pfleeger and Shari Lawrence Pfleeger. 2006. *Security in Computing (4th Edition)*. Prentice Hall PTR, Upper Saddle River, NJ, USA.

Additional Reference (s):

1. William Stallings 2002. *Cryptography and Network Security: Principles and Practice (3 rd).* Pearson Education
2. Kaufman, Perlman & Speciner, *Network Security*, Prentice-Hall, Englewood Cliffs, NJ, 1995. ISBN 0-13-061466-1
3. Schneier, B., *Applied Cryptography*, John Wiley, NY, NY, 1996. ISBN: 0-4711-1709-9

6. Course Description and Purpose

1. **Practical Aspects of Information Security – 3 Credits.**
2. **The purpose of this course is to**
   - Provide a practical survey of both the principles and practice of cryptography and network security.
   - Deals with the practice of network security
   - Study cryptology and applications of cryptography to problems in computer systems and networks.

3. **Course Description:**
   Exploration of the techniques of modern cryptography and its application to real-world problems, including common algorithms and protocols used to secure and validate electronic documents, messages and e-commerce secure system design, access control, and protection. Malware: computer viruses, spyware, and key-loggers. Low level software security: buffer overflow and similar attacks. Web security: Cross-site scripting and SQL injection attacks. Network security: protocols (TCP, DNS, SMTP, SSH, TLS and routing), Network worms and bot-nets.

7. Course Learning Outcomes

Upon successful completion of this course, the learner should be able to:

- Understand the principles and practices of cryptographic techniques.
- Understand a variety of generic security threats and vulnerabilities, and identify and analyze particular security problems for a given application.
- Understand the design of security protocols and mechanisms for the provision of security services needed for secure networked applications.
- Be familiar with current research issues and directions of network security.

8. Methods of Teaching

The methods of instruction may include, but are not limited to:

1. Lectures
2. Discussion and problem solving
3. Brainstorming
4. Individual assignments
5. Case Study
6. Asking students to give a presentation in a specific subject or problem related to the course
7. Lecturing using PowerPoint Presentations, mixed with discussion with students
8. Asking students to prepare a term paper about a subject or a problem related to the course, and discuss it in the class.

9. Course Learning Assessment/Evaluation

The following methods of learning assessment will be used in this course:

	Assessment	Weight	Description
a	2 Tests - Mid Exam - Final Exam	30% 40%	- Multiple choice questions - True/False - Short answers - Essay Questions - Problem solving - Explanations
b	Actives such as Quizzes	10%	- Multiple choices questions - True /False - Short answers - Problem solving
c	Assignments Research proposal	10%	- Asking students to prepare a term paper about a subject or a problem related to the course, and discuss it in the class
d	Presentations/participation	10%	- Student participation - Course portfolio
	Total	100%	

Note: The details for the above methods of assessment are presented below:

(a) Tests

Test	Weight %	CLO	Due Date
Mid	30%	1-5	Week 6
Final	40%	1-12	Week 16
Total	70%	12	

(b) Quizzes

Method+	Weight	CLO	Focus & Scope	Due Date
Quizzes	10%	Every Chapter	To be defined by instructor	To be defined
Total	10%			

(c) Assignments

Assignment	Weight	CLO	Scope & Focus	Due Date
Assignments	10%	1-3	Ch2, Ch3, Ch5, Ch6, Ch7, Ch8, ch11. ch12	after finish every Chapter

(d) Participation

Method	Weight	CLO	Focus & scope	Due Date
Participation & Presentation	10%	**	Student contribution and cooperation Course portfolio	All weeks
Total	10%			

10. Course Schedule/Calendar

Wk No.	Topic	Assignments/ workshops due date	Reference in the textbook	CLO
1	Overview			
2	Classical Encryption Technique			
3	Block Cipher, DES and AES			
4	Block Cipher Operation			
5	Public Key Cryptography and RSA			
6	Other Public-Key Cryptosystems			
7	Mid Exam			
8	Cryptographic Hash Functions Message authentication code (MAC) Digital Signatures			
9	Key Management and Distribution			
10	User Authentication			
11	Transport-Level Security Secure Sockets Layer (SSL)			
12	Wireless Security			
13	|Email Security			
14	IP Security			
15				
16	Final Test			

Special Equipment or Supplies

Personal Computer