UNIVERSITY OF BAHRAIN

College of Information Technology

Quality Assurance Office

جامعة البحرين

كلية تقنية المعلومات

مكتب ضبط الجودة

Course Information Form (*QAO-1*)

Code	ITCS412	Title	Cryptography and Network Security	Credit Hours	3-2-3
Pre-requisites		ITCS251&ITCE311	Web	http://groups.yahoo.com/group/itcs412/	

Course Instructor	Email	Office Hours	Course Coordinator
Hesham al-Ammal	hesham@itc.uob.bh	UT 10am-11am	Dr. Hesham al-Ammal

Course Objectives

The aim of this course is to provide a basic understanding of the various cryptographic techniques, their strengths and weaknesses, as well as their application to the security and integrity of computer systems and networks. The course also exposes the student to the threats and vulnerabilities associated with IT and the associated countermeasures.

Course Description

Introduction to basic concepts in public and symmetric cryptography, authentication, and general data security issues. Historical perspective of cryptography including some classical encryption techniques, cryptanalysis, and steganography. Symmetric key encryption methods. Public-key encryption methods. Hash functions and authentication protocols. Access control, firewalls, and network security. Viruses and intruders. Social implications of security problems and ethical issues.

Learning Outcomes

On successful completion of this course, students will be able to:

1. **Understand** the principles and practices of **cryptographic techniques** and their role in network and data security.
2. **Describe** efficient basic number-theoretic **algorithms necessary for cryptography**.
3. **Describe** some modern **private-key cryptosystems**.
4. **Identify** the features of **modern encryption techniques** and when to use them.
5. **Describe** at least one **public-key cryptosystem** including necessary complexity-theoretic assumptions for its security.
6. **Understand** a variety of generic **security threats and vulnerabilities**; and the dangers posed by different types of attacks.
7. **Identify** and analyze particular **security problems** for different aspects of a computer system and apply appropriate security **techniques to solve them**;
8. **Understand** the **tradeoffs** involved in producing a security solution (through examples of existing security applications);
9. **Understand** the effects of security risks on society and the **ethical responsibility** of the IT professional toward e-security.

Textbook

William Stallings, ***Cryptography and Network Security: Principles and Practices***, 3rd Edition, Prentice Hall, NJ.

Course Assessments

Mid-Term Exams	Lab Assignments	Quizzes	Project	Final Exam
40%	10%	10%	-	40%

Test Dates

Mid-Term Exam	Final Exam
MT1: Wed. 2/11/2006 at 10am, MT2:Wed. 28/12/2006 at 10am	23 Jan. 2007 at 8:30 – 10:30

General Notes

- Exam dates are final. No makeup exams.
- Test points will be carried forward to the final exam for students with valid approved absence reasons.
- Each assignment has a fixed due date, late submission will be subject to a 10% per day penalty.

Course Weekly Breakdown (*QAO-2b*)

Week	Date	Topics Covered	Lab. Assignments
1	17/9 19/9 21/9	**Introduction: What is cryptography?** **Historical Context for Cryptography** **1.1-1.6: Security services, attacks and mechanisms**	
2	24/9 26/9 28/9	**2.1-2.2: Conventional Encryption: Classical Techniques** **3.1- 3.3: Block Ciphers and DES**	Lab1: Introduction to Ethical Hacking + Footprinting and Scanning
3	1/10 3/10 5/10	**3.4-3.5: Block Ciphers and DES (cont.)** **Chapter 4. Finite Fields** **Chapter 5. AES**	Lab2: Sniffers and Denial of Service Attacks
4	8/10 10/10 12/10	**Chapter 5. AES (cont.)**	
5	15/10 17/10 19/10	**6.1-6.3: Brief Overview of Contemporary Ciphers**(handout)	Lab3: Encryption and Confidentiality
6	22/10 24/10 26/10	**9.1- 9.3: Public Key Cryptography**	
7	29/10 31/10 2/11	**9.1- 9.3: Public Key Cryptography (cont.)**	*Midterm Exam 1 (2/11/2006 at 10am)*
8	5/11 7/11 9/11	**10.1 Key Management**	Lab4: Buffer overflow, backdoors and trojans (ncat)
9	12/11-6/11		
10	19/11 21/11 23/11	**11.1-11.5 Message Authentication and Hash Functions**	Lab5: Wireless networks security
11	26/11 28/11 30/11	**15.1 e-mail Security (PGP)**	Lab6: Hacking web servers and web applications
12	3/12 5/12 7/12	**17.1-17.3 Web Security**	Lab7: Trojans, Viruses and Worms
13	10/12 12/12 14/12	**18.1-18.3 Mal Software**	
14	17/12 19/12 21/12	**19.1-19.2 Intruders and Viruses**	
15	24/12 26/12 28/12	**20.1-20.2 Firewalls**	*Midterm Exam 2(28/12/2006 at 10am)*
16	31/12 2/1 4/1	**20.2 Firewalls**	
17	7/1 9/1	**Review**	