KOMAR UNIVERSITY OF SCIENCE AND TECHNOLOGY
(KUST)

Info Assurance & Security Course Syllabus			
Course Title	**Info Assurance & Security**		
Course Code	**INF 4330**	**No. of Credits**	**3**
Department	**E-Commerce & Info. Management departments**	**College**	**College of Business**
Pre-requisites Course Code	**Database Management Systems (INF 3315)**	**Co-requisites Course Code**	**None**
Course Coordinator(s)	**Adnan H. M. Al-Helali**		
Email	**Adnan.hadi@komar.edu.iq**	**Office No. 309**	**IP No. 123**
Other Course Teacher(s)/Tutor(s)	**None**		
Class Hours	**Sunday and Tuesday from 2:00 to 3:30 PM**		
Office Hours	**Tuesday from 10:00 to 12:00**		
Course Type	**❒ E-Commerce Requirement**		
Offer in Academic Year	**☐ Fall Semester 2015**		

COURSE DESCRIPTION

Students will learn information security basics, classical encryption, modern symmetric ciphers, confidentiality using private- key and public-key cryptosystems, message authentication and hash functions, digital signatures, and key management. Students will also use some of Internet-based security algorithms, working with email and web browsers and learn how to browse the business web sites using IPsec and Web security techniques. Coursework also illustrate and categorize the firewalls, trusted systems, malicious software threats and advanced Anti-Virus techniques

COURSE OBJECTIVES

1. Develop and understanding of information assurance as practiced in computer operating systems, distributed systems, networks and representative applications.
2. Gain familiarity with prevalent network and distributed system attacks, defenses against them, and forensics to investigate the aftermath.
3. Develop a basic understanding of cryptography, how it has evolved, and some key encryption techniques used today.
4. Develop an understanding of security policies (such as authentication, integrity and confidentiality), as well as protocols to implement such policies in the form of message exchanges.

KOMAR UNIVERSITY OF SCIENCE AND TECHNOLOGY
(KUST)

COURSE LEARNING OUTCOMES

After participating in the course, the students should be able to:

1. analyze information security attacks, services, and mechanisms
2. Create information security systems
3. Evaluate the difference between private (symmetric)-key and public (asymmetric)-key cryptosystems.
4. Illustrate some of the international private-key and public-key algorithms.
5. Applying some of the Internet based security technologies.
6. Evaluate the malicious software and advanced Anti-Virus techniques.

GUIDELINES ON GRADING POLICY

A	=	95	–	100	Points	
A–	=	90	–	94	Points	
B+	=	87	–	89	Points	
B	=	83	–	86	Points	
B–	=	80	–	82	Points	
C+	=	75	–	79	Points	
C	=	70	–	74	Points	
C–	=	65	–	69	Points	
D+	=	60	–	64	Points	(65 is the passing grade. A 100 is your goal)
D	=	55	–	59	Points	
D–	=	50	–	54	Points	
F	=	0	–	49	Points	
W	Withdrawal					
I	Incomplete					

COURSE CONTENT

Course topics include:

1. Introduction
2. Conventional Encryption/ Classical Techniques.
3. Conventional Encryption/ Modern Techniques.
4. Conventional Encryption: Algorithms.
5. Advanced Encryption Standard
6. Public Key Cryptography.
7. Message Authentication and Hash Functions.
8. Digital Signature and Authentication Protocols.
9. IP Security and Web Security techniques.
10. Malicious software and advanced Anti-Virus techniques.
11. Firewall

COURSE ASSESSMENT TOOLS

Assessment Tool	Description	Weight
Quizzes	Quizzes are scheduled as shown in the semester schedule. Students will take 4 quizzes. All the quizzes will be counted toward your final grade.	15%
Assignments and Participation	Five assignments will be conducted during the semester; each one will be given as scheduled and will be posted on Google Classroom.	20%
Midterm Exam	The midterm exam will be designed to cover the students' learning outcomes number 1, 2 and 3.	25%
Test	Students will take one test designed to cover outcomes 4 and 5.	10%
Final Exam	The final exam will be designed to cover all the students' learning outcomes for this course. The exam will be close book, no materials are allowed except the one that will be given by the instructor.	30%

COURSE TEACHING AND LEARNING ACTIVITIES

Course Teaching and Learning Activities: (short description)

Teaching Strategies

1. Lectures/Demonstrations.
2. Hands-on exercises.
3. Assignments.
4. Interactive class discussion.
5. Tests and quizzes.

Student Activities

Students must:

1. Read and comprehend the textbook material.
2. Attend all the classes and take notes on class discussions.
3. Actively participate in class discussions and activities.
4. Submit all the assignments and the project on time.
5. Pass tests and quizzes.

Textbooks:
Cryptography and network security, principles and practice, 5th edition, William Stallings, 2011.

References:

1. The Complete Reference Information Security, 2nd edition, by Mark Rhodes-Ousley, 2013.
2. Principles of Information Security, 4th edition, by Michael E. Whitman, and Herbert J. Mattord, 2012
3. Information Technology Security Hand Book, by George Sadowsky, James X. Dempsey, Alan Greenberg, Barbara J. Mack, and Alan Schwartz, 2003.

COURSE POLICY (including plagiarism, academic honesty, attendance etc.)

Attendance Policy

Students are expected to attend all the classes for the entire semester. Students are responsible for material presented in lectures. Attendance is taken at the beginning of each class. Only students with official KUST absences, family crises, and illness are excused from class. This in no way cancels any responsibility for work due or assigned during absence. The student who misses more than 10 percent of the course classes will be placed on probation.

Make-up Policy

Because all examinations are announced in advance a zero will be assigned to any missed examination unless a student has a legitimate acceptable reason, such as illness, for not being able to take the examination during all the days when the examination was announced.

Academic Dishonesty

Any type of dishonesty (plagiarism, copying another's test or home-work, etc) will NOT be tolerated. Students found guilty of any type of academic dishonesty are subject to failure in this course, plus further punishment by the University Consul.

Deadlines/Due Dates

Recognizing that a large part of professional life is meeting deadlines, it is necessary to develop time management and organizational skills. Failure to meet the course deadlines will result in penalties.

GUIDELINES FOR SUCCESS

1. Work both independently and in groups of your study of peers, who can help you understanding the course material.
2. Pay a full attention in the class when your instructor explain the lesson, if you understand 70% directly from the instructor, then the 30% will be just practice exercises.
3. Understanding more than memorizing will help you a lot in passing exams.
4. Working many problems beyond the assigned homework will help mastering.
5. Ask a question when something is not clear.

6. Finally, attend every lecture and getting missed material is your responsibility.

E-MAIL ETIQUETTE OF COMMUNICATION

Please note the following in regards to e-mail communication:

1. It is your responsibility to update your Komar-email address daily for course updates. Faculty will not be able to contact you if you fail to have an email address and you could potentially miss important information about the course.
2. Email will only be answered if it comes from Komar-email address. Faculty will not respond to unprofessional email addresses.
3. Mail should have a subject heading which reflects the content of the message.
4. Your message should begin with an appropriate salutation, including the name of the person being addressed, and end with thanks followed by your full name of the sender.
5. Emails that do not follow the above guidelines, or are written in an unprofessional and / or disrespectful manner as well as anonymous emails will not be addressed.
6. Failure to check e-mail or Google classroom may result in you missing important assignments and subsequently affect your grade.

CELL PHONES

All cell phones are expected to be switched to vibrating mode if available and turned off completely if this feature is not an option. Disruption of class due to a cell phone will not be tolerated and the student will be asked to leave class. All other electronic equipment that the faculty member deems not essential to the provision of academic learning is prohibited from being used in class.

REVISIONTO THE SYLLABUS

This syllabus is subject to change. It is the duty of the instructor to inform students of changes in a timely fashion after approval of Quality Assurance Office (QAO).

KOMAR UNIVERSITY OF SCIENCE AND TECHNOLOGY
(KUST)

Course calendar: Please check the academic calendar for 2015/2016 (Subject to Change)

Lecture	Beg/End Dates	Topics (Chapters)	Course Requirements
1	28 Sep – 1 Oct 2015	**1. Introduction** • Information Security Concepts • Attack, services, and Mechanisms • Security Attacks • Security Services • A Model for network Security	
2	4 – 8 Oct 2015	**2. Conventional Encryption/ Classical Techniques** • Symmetric Cipher Model • Substitution Techniques • Transposition Techniques • Steganography	**Assignment #1**
3	11 – 15 Oct 2015	**3. Conventional Encryption/ Modern Techniques** • Block Cipher Principles • The Data Encryption Standard (DES)	**Quiz #1**
4	18 – 22 Oct 2015	**5. Advanced Encryption Standard** • A DES Example • The Strength of DES	**Assignment #2**
5	25 – 29 Oct 2015	**9. Public-Key Cryptography and RSA** • Principles of Public-Key Cryptosystems • The RSA Algorithm	
6	1 – 5 Nov 2015	**9. Public-Key Cryptography and RSA** • Principles of Public-Key Cryptosystems The RSA Algorithm	**Assignment #3**
7	8 – 12 Nov 2015	**11. Cryptographic Hash Functions** • Applications of Cryptographic Hash Functions • Two Simple Hash Functions • Hash Functions Based on Cipher Block Chaining • Secure Hash Algorithm (SHA)	**Quiz #2**
	15 – 19 Nov 2015	**Midterm Exam**	

8	22 – 26 Nov 2015	**12. Message Authentication Codes** • Message Authentication Requirements • Message Authentication Functions • Message Authentication Codes • Security of MACs	
9	29 Nov – 3 Dec 2015	**13. Digital Signatures** • Digital Signature • Digital Signature Standard (DSS)	**Assignment #4**
10	6 – 10 Dec 2015	• 14. Key Management and Distribution • Symmetric Key Distribution Using Asymmetric Encryption Distribution of Public Keys • X.509 Certificates • Public Key Infrastructure	
12	13 – 17 Dec 2015	**16. Web Security** • Transport-Level Security • Secure Sockets Layer (SSL) • Transport Layer Security (TLS) • HTTPS	**Quiz #3**
13	20 – 24 Dec 2015	**19. IP Security** • IP Security Overview • IP Security Policy • Encapsulating Security Payload • Internet Key Exchange	**Assignment #5** **Test #1**
	27 – 31 Dec 2015	**New Year Holiday**	
14	3 – 7 Jan 2015	**21. Malicious Software** • Types of Malicious Software • Viruses • Virus Countermeasures • Worms • Distributed Denial of Service Attacks	**Quiz #4**
15	10 – 14 Jan 2015	**22. Firewalls** • The Need for Firewalls • Firewall Characteristics • Types of Firewalls • Firewall Basing • Firewall Location and Configurations	
16	17 – 21 Jan 2015	**review**	
		Final Exam	

KOMAR UNIVERSITY OF SCIENCE AND TECHNOLOGY
(KUST)