Jordan University of Science & Technology		
Faculty of Computer & Information Technology		
Year: 2015/2016	**Department of Network Engineering and Security**	Semester: Second

Course Information	
Course Title	Cryptography and Network Security
Course Number	NES 452
Prerequisites	NES 451 – Basics of Information System Security NES 312 – Fundamentals of Computer Networks
Course Website	http://elearning.just.edu.jo
Coordinator	
Instructor	Dr. Baha' A. Alsaify
E-mail	baalsaify@just.edu.jo
Office Location	N1-L0
Office Phone	7201000 ext. 22396
Office Hours	TBA
Assistants	TBA

Catalog Description

Introduction to the principles of number theory and the practice of network security and cryptographic algorithms. Topics include: Divisibility and the Greatest Common Divisor, Euclidean Algorithm, modular arithmetic and discrete logarithm, Primes, primality testing, Chinese Remainder Theorem. Conventional or Symmetric Cryptography (Rijndael, AES family), Modes of operation, Public or Asymmetric Cryptography (RSA), key management and exchange, hash functions (MD5, SHA family, HMAC), digital signatures, certificates and authentication protocols (X.509, DSS, Kerberos), electronic mail security (PGP), web security and protocols for secure electronic commerce (IPSec, SSL/TLS, SET).

Text Book	
Title	Cryptography and Network Security
Author(s)	Behrouz A. Forouzan
Publisher	McGraw-Hill Higher Education
Edition / Year	First Edition / 2008
Book Website	http://highered.mheducation.com/sites/0072870222/index.html
References	Cryptography and Network Security, Sixth Edition, William Stalling, 2013

Assessment Policy		
Assessment	**Date**	**Weight**
First Exam	During the 5th or 6th week	15%
Second Exam	During the 11th or 12th week	15%
Quizzes/Assignments		10%
Project		20%
Final Exam	During the 16th week	40%
Total		100%

Course Objectives	**Weight**
This course is designed to help students:	
1. Be familiar with fundamentals of cryptography	10%
2. Be familiar with different secure protocols and algorithms	35%
3. Be familiar with network security threats and countermeasures	25%
4. Be familiar with network security designs and systems using available secure solutions (such as PGP, SSL, and IPSec).	20%
5. Be familiar with advanced security issues and technologies	10%

Teaching & Learning Methods
▪ Class lectures, lecture notes and assignments are designed to achieve the course objectives. ▪ Students are expected to read the material as detailed in the text, complete the assignments on time and participate in class. ▪ Course web page is an essential part of the course.

Learning Outcomes		
Related Objective(s)	**This course requires the student to demonstrate the following:**	**Reference(s)**
1	1. An understanding of the fundamental building blocks of modern block ciphers.	Ch.5
2, 3	2. An understanding of some of the most popular block ciphers (such as AES)	Ch.6, Ch.7
2, 3	3. The ability to encrypt long messages using the different modes of operation available (ECB, CBC, OFB, CFB, CTR)	Ch.8
1	4. An understanding of the prime numbers, primality testing, modular arithmetic, the concepts of factorization, and the Chinese remainder theorem.	Ch.9
2, 3	5. The ability to understand the concepts of Asymmetric ciphers along with some of the most common algorithms (such as RSA).	Ch.10
2	6. Understand and differentiate between MDC and MAC	Ch.11
2, 3, 5	7. The ability to understand hash functions and their attacks and how to apply them to long messages using different models.	Ch.12
2, 3	8. The ability to apply and use digital signatures in the most effective way along with the understanding of the attacks that can be launched on digital signatures.	Ch.13
2, 5	9. The understanding of the importance of key distribution centers such as Kerberos.	Ch.15
4	10. The understanding of some of the security issues at the application layer (Email security and PGP).	Ch.16
4	11. The understanding of some of the security issues at the transport layer (SSL/TLS).	Ch.17
4	12. The understanding of some of the security issues at the Network layer (IPsec).	Ch.18
5	13. The understanding of Secure Electronic Transaction (SET) protocol	handouts

Course Content		
Week	**Topics**	**Chapter(s) in Text**
1,2	▪ Introduction to Modern Symmetric-Key Ciphers	5
3,4	▪ Data Encryption Standard	6
5,6	▪ Advanced Encryption Standard	7
7	▪ Encipherment Using Modern Symmetric-Key Ciphers	8
8,9	▪ Asymmetric-Key Encipherment	9,10
10,11,12,13	▪ Integrity, Authentication, and Key Management	11,12,13, and 15
14,15	▪ Network Security	16, 17, and 18
16	▪ Secure Electronic e-commerce	handout

Essential Notes	
Exams	▪ May include: Definitions, True/False, Multiple-Choice, Analysis and Descriptive formats. ▪ Use only your own tools: calculator, pens and ruler ▪ Instructions on the first page of the exam are quite important.

	▪ Not abiding by the rules is a reason for dismissal from the exam.

Additional Notes	
Makeups	▪ Makeup exam should not be given unless there is a valid excuse.
Drop Date	▪ Last day to drop the course is before the 12th week of the current semester.
Cheating	▪ Standard JUST policy will be applied.
Attendance	▪ Excellent attendance is expected. ▪ According to the JUST policy, a student will receive the grade of ZERO (35%) “failed for absence” if he misses more than 20% of the classes. ▪ Attendance will be taken by calling the names or passing a sign-up sheet. ▪ If you miss a class, it is your responsibility to find out about any announcements or assignments you may have missed.
Workload	▪ Average work-load student should expect to spend is 6 hours/week.
Graded Exams	▪ Graded exam papers will be returned within a week.
Participation	▪ Participation in the class will positively affect your performance. ▪ Disruption and side talks will possibly result in dismissal from class. ▪ No eating or chewing gums are allowed in class.