Jordan University of Science and Technology

Faculty of Computer & Information Technology

Network Engineering And Security Department

NES452 Cryptography And Network Security

First Semester 2020-2021

Course Catalog

3 Credit Hours. 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
Edition	1st Edition
Short Name	Ref#1
Other Information	

Course References

Short name	Book name	Author(s)	Edition	Other Information
Ref#2	Cryptography and Network Security	William Stallings	8th Edition	

Instructor

Name	**Dr. Raed Bani-Hani**
Office Location	E1L3
Office Hours	Sun : 10:00 - 11:30 Mon : 11:30 - 13:30 Tue : 10:00 - 11:30 Wed : 11:30 - 12:30
Email	rbanihani@just.edu.jo

Instructor	
Name	**Prof. Eyad Taqieddin**
Office Location	E1L3
Office Hours	Sun : 11:00 - 12:30 Mon : 11:00 - 12:00 Tue : 11:00 - 12:30 Wed : 11:00 - 12:30 Thu : 11:00 - 12:30
Email	eyadtaq@just.edu.jo

Class Schedule & Room

Section 1:
Lecture Time: Sun, Tue : 08:30 - 10:00
Room: منصة الكترونية

Section 2:
Lecture Time: Sun, Tue : 11:30 - 13:00
Room: منصة الكترونية

Section 4:
Lecture Time: Sun, Tue : 08:30 - 10:00
Room: منصة الكترونية

Teaching Assistant

Shefa' Mubarak(Sections 1, 2, 4)

Prerequisites

Line Number	Course Name	Prerequisite Type
1753120	NES312 Fundamentals Of Computer Networks	Prerequisite / Study
1754510	NES451 Basics Of Information System Security	Prerequisite / Study

Tentative List of Topics Covered

Weeks	Topic	References
Weeks 1, 2	Mathmatics of Cryptography	**ch's 2, 4** From **Ref#1**
Week 3	Introduction to Modern Symmetric-Key Ciphers	**ch5** From **Ref#1**
Week 4	Advanced Encryption Standard	**ch7** From **Ref#1**
Weeks 5, 6	Encipherment Using Modern Symmetric-Key Ciphers	**ch8** From **Ref#1**
Weeks 6, 7	Asymmetric-Key Encipherment	**ch's 9, 10** From **Ref#1**
Weeks 8, 9, 10, 11	Integrity, Authentication, and Key Management	**ch's 11, 12, 13, and 15** From **Ref#1**
Weeks 12, 13, 14	Network Security	**ch's 16, 17, and 18** From **Ref#1**

Mapping of Course Outcomes to Program Student Outcomes	Course Outcome Weight (Out of 100%)	Assessment method
Understand basic concepts of number theory (divisibility, modular arithmetic, and congruence) [1SO1]	10%	First Exam, Quizzes, Final Exam
Understand the basics of algebraic structure (Groups, Rings, fields, and finite fields) and concepts of modular and polynomial arithmetic [1SO1]	13%	First Exam, Final Exam
Understand the fundamental building blocks of modern block ciphers. [1SO1]	14%	First Exam, Final Exam
Understand the most popular modern symmetric block ciphers and their modes of operation [1SO1, 1SO2]	10%	First Exam, Final Exam
Understand the prime numbers, primality testing, the concepts of factorization, and exponentiation [1SO1]	5%	Quizzes, Final Exam
Explain the concepts of asymmetric ciphers along with some of the most common algorithms (such as RSA) [1SO1]	10%	Final Exam
Explain hash functions and MAC their attacks and how to apply them to long messages using different models [1SO1, 1SO2]	10%	Final Exam
Describe the use of digital signatures in the most effective way along with the understanding of the attacks that can be launched on them [1SO1, 1SO2]	6%	Quizzes, Final Exam
Understand the importance of key distribution centers such as Kerberos. [1SO2]	2%	Quizzes
Explain selected security protocols at the application layer (such as Email security and PGP). [1SO2]	8%	Final Exam
Explain selected security protocols at the transport layer (such as SSL/TLS). [1SO2]	5%	Quizzes, Final Exam
Explain selected security protocols at the Network layer (such as IPsec). [1SO2]	7%	Final Exam

Relationship to Program Student Outcomes (Out of 100%)						
SO1	SO2	SO3	SO4	SO5	SO6	SO7
65	35					

Evaluation	
Assessment Tool	**Weight**
First Exam	30%
Quizzes	20%
Final Exam	50%

Policy

Exams	1. May include: Definitions, True/False, Multiple-Choice, Analysis and Descriptive formats. 2. Use only your own tools: calculator, pens and ruler 3. Instructions on the first page of the exam are quite important. 4. Not abiding by the rules is a reason for dismissal from the exam.
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	1. Excellent attendance is expected. 2. 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. 3. Attendance will be taken by calling the names or passing a sign-up sheet. 4. 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	1. Participation in the class will positively affect your performance. 2. Disruption and side talks will possibly result in dismissal from class. 3. No eating or chewing gums are allowed in class.

Date Printed: 2021-02-22