The University of Jordan
School of Engineering
Department of Computer Engineering
Fall Term – A.Y. 2025 - 2026

Course:	Advanced Networks and Systems Security – 0907748 (3 Cr)
Catalog Data:	Review of Computer Networks. Number Theory and Field Arithmetic. Sources of Network Threats. Data Encryption: Cryptography and Ciphering. Risk Management. Key Management. Protocols and Algorithms of Security Systems. Email and Web Security and Firewalls. Performance Evaluation of Security Systems.
Prerequisites by Course:	None
Prerequisites by topics:	Students are assumed to have had sufficient knowledge pertaining to computer networks.
Textbook:	Introduction to computer security / Michael Goodrich, Roberto Tamassia. Harlow : Pearson Education ; 2014
References:	Cryptography and Network Security Principles and Practice, 6th ed., by William Stallings, Pearson Education, Inc., 2014. Network Security Essentials: Applications and Standards, 6th ed., by William Stallings, Pearson Education, Inc., 2016.
Schedule & Duration:	15 Weeks, 15 lectures, 150 minutes each (including exams).
Minimum Student Material:	Text book, class handouts, instructor keynotes, calculator and access to a personal computer and internet.
Minimum College Facilities:	Classroom with whiteboard and projection display facilities, library, and computational facilities.
Course Objectives:	By the end of this course, the student should be familiar with the basics of security and the main components and algorithms of the security triad; these are confidentiality, integrity, and authentication. Also, the student should know the differences between symmetric and asymmetric encryption algorithms.
Course Outcomes and Relation to ABET Program Outcomes:	Upon successful completion of this course, a student should be able to: 1. Understand the basic and most commonly used symmetric encryption algorithms. 2. Decide which security algorithm and which security component are needed to attain a specific security function. 3. Decide when to use symmetric and when to use asymmetric encryption. 4. Decide for a given situation, what are existing vulnerabilities and what is the suitable security solution most suitable. 5. Learn and use new security protocols and tools.

Course Topics:

Introduction
Basic Classical Cryptography
Mono-Alphabetic cryptanalysis example
One Time pad
DES
AES
Modes of Encryption
Data Integrity
Public Key Encryption (RSA)
User Authentication
Email Security
Web Security
IP sec
LAN Security
Web WiFi Security
Denial-of-Service Attacks

Assessments: Project, Presentation, and Exams.

Grading policy:

Midterm Exam	30%
Assignments and Project	30%
Final Exam	40%

Instructors:

Dr. Ramzi Saifan
r.saifan@ju.edu.jo
Office Hours: Sun, Tue, Thu 11:30 – 12:30