The University of Jordan
School of Engineering
Department of Computer Engineering
Fall Term – A.Y. 2021-2022

Course:	Information and Network Security – 0907520 (3 Cr)
Catalog Data:	This course covers topics including basics of computer security, Cryptography, Cryptology, Cryptanalysis, Encryption, Decryption, stream cipher, block cipher, symmetric encryption, asymmetric encryption, active attacks, passive attacks, DES, 3DES, AES, RSA, Hash functions, authentication, data integrity, and preserving confidentiality.
Prerequisites by Course:	Computer Networks (0907422)
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 Princibles 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.
Course Website:	ramzi.ucoz.com
Schedule & Duration:	15 Weeks, 45 lectures, 50 minutes each (including exams).
Minimum Student Material:	Text book, class handouts, instructor keynotes, calculator and access to apersonal 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.[7] 3. Decide when to use symmetric and when to use asymmetric encryption.[7] 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. [7]

Course Topics:

Introduction
Basic Classical Cryptography
Mono-Alphabetic cryptanalysis example
One Time pad
DES
AES
Modes of Encryption
Data Integrity
Public Key Encryption (RSA)
Diffie and Hellman Key Exchange
User Authentication
Web Security
Anonymity
LAN Security
PGP, SSL, and IPSec

Assessments: Project, Presentation, and Exams.

Grading policy:

Midterm Exam	30%
Project	10%
Quiz	10%
Final Exam	50%

Instructors:

Dr. RamziSaifan
r.saifan@ju.edu.jo
Office Hours: Sun, Tue, Thu 10:30 – 11:30

Program Outcomes (PO)

1	an ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics
2	an ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors
3	an ability to communicate effectively with a range of audiences
4	an ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts
5	an ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives
6	an ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions
7	an ability to acquire and apply new knowledge as needed, using appropriate learning strategies.

Last Updated: OCT10, 2021