Jordan University of Science and Technology

Faculty of Computer & Information Technology

Cybersecurity Department

CY261 Cryptography - JNQF Level: 7

First Semester 2023-2024

Course Catalog
3 Credit Hours. This course covers basic concepts in cryptography, including encryption/decryption, sender authentication, data integrity, non-repudiation, attack classification (ciphertext-only, known plaintext, chosen plaintext, chosen ciphertext), symmetric cryptography (i.e. DES and AES) and asymmetric cryptography (i.e. RSA), information-theoretic security (one-time pad, Shannon Theorem), key exchange and digital signatures.

Text Book	
Title	Cryptography and Network Security: Principles and Practice,
Author(s)	William Stallings
Edition	7th Edition
Short Name	Main Textbook
Other Information	SBN 10:1-292-15858-1, ISBN 13: 978-1-292- 15858-7

Course References

Short name	Book name	Author(s)	Edition	Other Information
Ref #1	Handbook of Applied Cryptography,	Menezes, Oorschot and Vanstone	1st Edition	CRC Press

Instructor	
Name	**Dr. Qasem Abu Al-Haija**
Office Location	-
Office Hours	Sun : 09:30 - 10:30 Sun : 11:30 - 12:30 Mon : 09:30 - 10:30 Mon : 10:30 - 11:30 Tue : 09:30 - 10:30 Thu : 09:30 - 10:30

Email	qsabuhaija@just.edu.jo

Class Schedule & Room
Section 1: Lecture Time: Sun, Tue, Thu : 08:30 - 09:30 Room: C3013 Section 2: Lecture Time: Sun, Tue, Thu : 10:30 - 11:30 Room: SF12

Prerequisites		
Line Number	**Course Name**	**Prerequisite Type**
902331	MATH233 Probability & Statistics (For Computer Sciences Students)	Prerequisite / Study
1761120	SE112 Introduction To Object- Oriented Programming	Prerequisite / Study
821123	HSS112SE Introduction To Object- Oriented Programming	Prerequisite / Study
822331	HSS233MATH Probability & Statistics (For Computer Sciences Students)	Prerequisite / Study

Tentative List of Topics Covered		
Weeks	**Topic**	**References**
Weeks 1, 2	Course Overview + Introduction to Cryptography	**Ch. 01** From **Main Textbook**
Weeks 3, 4	Introduction to Number Theory	**Ch. 02** From **Main Textbook**
Weeks 5, 6	Classic Encryption Technique	**Ch. 03** From **Main Textbook**
Weeks 7, 8, 9	Symmetric Key Encryption	**Ch. 04 to Ch. 07** From **Main Textbook**
Weeks 10, 11	Public Key Encryption	**Ch. 09+Ch. 10** From **Main Textbook**
Week 12	Cryptographic Hash Function	**Ch. 11** From **Main Textbook**
Week 13	Message Authentication Codes	**Ch. 12** From **Main Textbook**
Weeks 14, 15	Public Key Digital Signatures	**Ch. 13** From **Main Textbook**

Mapping of Course Outcomes to Program Outcomes and NQF Outcomes	Course Outcome Weight (Out of 100%)	Assessment method
Identify the basic cryptographic concepts and functionalities including symmetric ciphers, asymmetric encryption, digital signatures, hash functions, and others. [1SO1] [1L7K1]	25%	
Use the fundamental techniques of number theory and modular arithmetic in problem-solving. [1SO1] [1L7S1]	10%	

Apply various cryptographic techniques to secure data and communications, including both classical and modern encryption algorithms. [1SO2] [1L7S3]	40%	
Design and implement modern cryptosystems for secure data transmission and authentication. [1SO3] [1L7C1]	10%	
Analyze the security of cryptographic systems, identifying potential vulnerabilities and understanding common attacks on cryptographic systems. [1SO1] [1L7S2]	15%	

Relationship to Program Student Outcomes (Out of 100%)				
SO1	SO2	SO3	SO4	SO5
50	40	10		

Relationship to NQF Outcomes (Out of 100%)				
L7K1	L7S1	L7S2	L7S3	L7C1
25	10	15	40	10

Policy	
Grading Policy	1st Exam: 20% 2nd Exam: 20% Project: 10% Quizzes: 10% Final Exam: 40%

Date Printed: 2023-10-21