Jordan University of Science and Technology

Faculty of Computer & Information Technology

Network Engineering And Security Department

NES751 Advanced Cryptography
Second Semester 2023-2024

Course Catalog
3 Credit Hours. This course covers advanced aspects of cryptography based on a formal and theoretical approach. Topics covered include: number theory concepts, Exponentiation methods, Chinese remainder theorem, Polynomials and finite fields, Factoring and generating prime numbers, primality testing, discrete logarithm, birthday problem, secure hash functions, attacks on hash functions, digital signature and their attacks, pseudorandom generators, and Zero-knowledge proofs.
Teaching Method: On Campus

Text Book	
Title	A Graduate Course in Applied Cryptography
Author(s)	Dan Boneh and Victor Shoup
Edition	4th Edition
Short Name	Textbook
Other Information	

Course References

Short name	Book name	Author(s)	Edition	Other Information
Old textbook	Understanding Cryptography: A Textbook for Students and Practitioners	Christof Paar, Jan Pelzl	1st Edition	
Ref #1	Cryptography and network Security	Wiliam Stallings	7th Edition	

Instructor	
Name	**Prof. Basheer Al-Duwairi**
Office Location	C5L2

Office Hours	Sun : 12:00 - 13:30 Mon : 11:30 - 13:00 Tue : 11:00 - 13:00 Wed : 09:00 - 10:00
Email	basheer@just.edu.jo

Class Schedule & Room
Section 1: Lecture Time: Wed : 11:30 - 14:30 Room: LAB

Tentative List of Topics Covered		
Weeks	**Topic**	**References**
Weeks 1, 2	Review of cryptography and basic number theory	
Week 3	Stream ciphers and Pseudorandom Number Generation (PRNG)	
Week 4	Current Modes of Operation (CTR, CCM, GCM, XTS-AES, FPE)	
Week 5	More Number theory (Finite Fields, discrete log, Primality testing, CRT, solving linear and square root mod n)	
Weeks 6, 7	RSA Performance and implementation (speed-up techniques, fast exponentiation, padding, attacks)	
Week 8	Elgamal Encryption Scheme	
Week 9	Elliptic Curve Cryptography	
Week 10	Digital Signature Algorithms	
Week 11	Birthday problem and Hash functions	
Week 12	Special Topics in Info Sec and Crypto: Blockchain Technology	
Week 13	Special Topics in Info Sec and Crypto: Birthday problem and Hash functions	
Week 14	Special Topics in Info Sec and Crypto: Zero-Knowledge proofs	
Week 15	Special Topics in Info Sec and Crypto: Side Channels Attacks	
Week 16	Special Topics in Info Sec and Crypto: Quantum Resistant Cryptography	

Mapping of Course Outcomes to Program Outcomes	Course Outcome Weight (Out of 100%)	Assessment method
Learn and apply knowledge of advanced topics/algorithms in number theory related to modern cryptography	25%	
Identify the performance characteristics and limitation of practical use of the main cryptographic algorithms.	25%	
Demonstrate the understanding of different cryptographic attacks.	25%	

Relationship to Program Student Outcomes (Out of 100%)													
SO1	SO2	SO3	SO4	SO5	SO6	SO7	MSO1	MSO2	MSO3	MSO4	MSO5	MSO6	MSO7

Policy	
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.
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

Date Printed: 2024-03-17