Faculty: Information Technology	
Department: Cybersecurity	**Program: Master**
Academic year:	**Semester:**

Course Plan

First: Course Information

Course No: 1506769	***Course Name: Advanced Topics in Cryptography***	***Credit Hours: 3***	***Theoretical:3***	***Practical:0***
Prerequisite No. and Title:		***Section No.:***	***Lecture Time:***	
Level in JNQF	***9***			
Type Of Course:	☐ ***Obligatory University Requirement*** ☐ ***Elective University Requirement*** ☐ ***Obligatory Faculty Requirement*** ☐ ***Elective Faculty Requirement*** ■ ***Obligatory Specialization Requirement*** ☐ ***Elective Specialization Requirement*** ☐ ***Ancillary course***			
Type of Learning:	■ ***Face-to-Face Learning*** ☐ ***Blended Learning (2 Face-to-Face + 1 Asynchronous)*** ☐ ***Online Learning (2 Synchronous+ 1 Asynchronous)***			

Second: Instructor's Information

Course Coordinator:			
Name:	***Academic Rank:***		
Office Number:	***Extension Number:***	***Email:***	
Course Instructor:			
Name:	***Academic Rank:***		
Office Number:	***Extension Number:***	***Email:***	
Office Hours:	***Sunday Monday Tuesday Wednesday Thursday***		

Third: Course Description

Master the secret language of secure information with Advanced Cryptography. Go beyond basic ciphers to explore powerful algorithms like elliptic curves and homomorphic encryption. Develop the skills to break cryptosystems, analyze real-world protocols, and stay ahead of the curve with cutting-edge research. Design secure solutions for the digital age, from communication channels to blockchain security. This course is for cryptography enthusiasts who want to unlock the secrets and code the future of information protection.

Fourth: Course Objectives

1. Master complex cryptographic primitives: RSA, AES, Elliptic curves, homomorphic encryption, multiparty computation.
2. Sharpen cryptanalysis skills: Break cryptosystems, understand vulnerabilities, develop countermeasures.
3. Analyze real-world cryptographic protocols: Identify security flaws, discuss best practices.
4. Stay current with cutting-edge research: Quantum-resistant cryptography, blockchain security, privacy-preserving computation.
5. Apply cryptography to solve practical problems: Design, implement, analyze cryptosystems in real-world scenarios.

Fifth: Learning Outcomes

Level descriptor according to (JNQF)	*CILOs Code*	*CILOs* If any CLO will not be assessed in the course, mark NA.	*Associated PILOs Code* *Choose one PILO for each CILO**	*Assessment method* *Choose at least two methods*
Knowledge	**K1**	Recall the mathematical foundations of advanced cryptographic primitives (elliptic curves, lattices, homomorphic encryption).	PK1	Mid-term Exam Final Exam
	K2	Relate different cryptographic mechanisms (symmetric/asymmetric, hash functions, signatures) to their specific security goals (confidentiality, integrity, non-repudiation).	PK1	Mid-term Exam Final Exam
	K3	Tell the historical development of cryptography and its impact on major societal and technological advancements.	PK2	Mid-term Exam Final Exam
Skills	**S1**	Apply advanced cryptographic algorithms to protect real-world data and systems.	PS2	Mid-term Exam Final Exam
	S2	Construct secure cryptographic protocols based on specific security requirements.	PS3	Mid-term Exam Final Exam
	S3	Compare the strengths and weaknesses of different cryptographic approaches and select the most appropriate one for a given scenario.	PS3	Mid-term Exam Final Exam
	S4	Develop and implement cryptographic tools and libraries using appropriate programming languages and frameworks.	PS4	Mid-term Exam Final Exam
	S5	Analyze the computational		Mid-term

		complexity and resource requirements of advanced cryptographic algorithms.	PS5	Exam Final Exam
Competencies	**C1**	Collaborate effectively with other students on cryptographic research projects and problem-solving activities.	PC1	Participation Project
	C2	Exhibit leadership in technical discussions and presentations related to advanced cryptography.	PC2	Participation Project

*CILOs: Course Intended Learning Outcomes; PILOs: Program Intended Learning Outcomes; For each CILO, the PILO could be the same or different.

Sixth: Learning Resources

Main Reference:	Cryptography: Theory and Practice Chapman & Hall/CRC		
Author: Douglas R. Stinson, Maura Paterson, and Alice Silverberg	***Issue No.:*** 4	***Print: CRC***	***Publication Year: 2018***
Additional Sources and Websites:	• Cryptography Engineering: Design Principles and Practical Applications by Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno John Wiley & Sons 2010 (2nd edition)		
Teaching Type:	***Classroom*** ■ ***Laboratory*** ▭ ***Workshop*** ☐ **MS Teams** ☐ **Moodle** ■		

Seventh: Course Structure

Week	Course Intended Teaching Outcomes (CILOs)	Topics	Teaching Procedures*	Teaching Methods**	References***
1	K1, K2, S1 S2	**Course Overview** Review of basic cryptography concepts, Classical Cryptography Security models and notions of security Computational complexity theory and cryptography Cryptanalysis and attacks on cryptographic algorithms and protocols	Face-to-Face	Lecturing with active participation	---------
2	K1, K2, K3, S1 S2	**Symmetric Key Cryptography** Block ciphers and stream ciphers Modes of operation	Face-to-Face	Lecturing with active participation	Chapter 2

		Key management			
3	K1, K2, K3, S1, S2, S3 S5	**Public Key Cryptography** RSA Diffie-Hellman key exchange	Face-to-Face	Lecturing with active participation	Chapter 3
4	K1, K2, K3, S1, S2, S3 S5	**Public Key Cryptography** Elliptic curve cryptography Other public key cryptosystems	Face-to-Face	Lecturing with active participation	Chapter 5
5	K1, K2, K3, S3 S5 C2, C3	**Hash Functions** Properties of hash functions Construction of hash functions Applications of hash functions	Face-to-Face	Lecturing with active participation	Chapter 6
6	K1, K2, K3, S1, S2, S3 S5	**Digital Signatures** Signature schemes Digital signature algorithms Cryptographic Protocols	Face-to-Face	Lecturing with active participation	Chapter 6
7	K1, K2, K3, S3 S5	**Key exchange protocols** Authenticated encryption protocols Secure communication protocols Other cryptographic protocols	Face-to-Face	Lecturing with active participation	Chapter 7
8	K1, K2, K3, S3 S5	**Zero-Knowledge Proofs** Zero-knowledge protocols and their	Face-to-Face	Lecturing with active participation	Chapter 7

		importance. Examples: Schnorr, Fiat-Shamir, and zk-SNARKs.			
Midterm Exams					
9	K1, K2, K3, S3 S5	**Homomorphic encryption** its use in secure computation. Fully homomorphic encryption (FHE) and its applications.	Face-to-Face	Lecturing with active participation	Chapter 7
10	K1, K2, K3, S1	**Real-World Applications** Secure communication, cloud security, and IoT.	Face-to-Face	Lecturing with active participation	Chapter 7
11	K1, K2, K3, S3 S5	**Real-World Applications** Case studies and practical implementations.	Face-to-Face	Lecturing with active participation	Chapter 7
12	K1, K2, K3, S1 S2, S3 S5	**Emerging Trends** Quantum-resistant cryptography.	Face-to-Face	Lecturing with active participation	Chapter 8
13	K1, K2, K3, S1, S3 S5	**Research Topics** Advanced cryptographic research directions.	Face-to-Face	Lecturing with active participation	Chapter 8
14	K1, K2, K3, S1, S5 C1, C2	**Project Presentation**	Face-to-Face	Lecturing with active participation	Chapter 8
Final Exams					

*Teaching procedures: (Face-to-Face, synchronous, asynchronous). ** Teaching methods: (Lecture, video….).
*** Reference: (Pages of the book, recorded lecture, video….)

Eighth: Assessment Methods

Methods	Online Learning	Blended Learning	Face-To-Face Learning	Specific Course Output to be assessed. **If any CILO will not be assessed in the course, mark NA.									
				K1	K2	K3	S1	S2	S3	S4	S5	C1	C2
First Exam													
Second Exam													
Mid-term Exam			30	✓	✓	✓	✓	✓	✓	✓	✓		
Participation												✓	✓
Asynchronous Activities													
Quizzes													
Assignments			30									✓	✓
Group presentation												✓	✓
Final Exam			40	✓	✓	✓	✓	✓	✓	✓	✓		
Total out of 100			100										

Ninth: Course Policies

- All course policies are applied to all teaching patterns (online, blended, and face-to-face Learning) as follows:
  a. Punctuality.
  b. Participation and interaction.
  c. Attendance and exams.
- Academic integrity: (cheating and plagiarism are prohibited).

Approval	Name	Date	Signature
Head of Department			
Faculty Dean			