Science & IT
Faculty of Science & IT

جامعــة الـزيتونـــة الأردنيــة
Al-Zaytoonah University of Jordan
كلية العلوم وتكنولوجيا المعلومات
Faculty of Science and Information Technology

" عراقة وجودة"
"Tradition and Quality"

QF01/0408-4.0E	**Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department**

Study plan No.	**2024/2025**		**University Specialization**		**Cybersecurity**	
Course No.	**0133222**		**Course name**		**Cryptography Theory**	
Credit Hours	**3**		**Prerequisite Co-requisite**			
Course type	□ MANDATORY UNIVERSITY REQUIREMENT	□ UNIVERSITY ELECTIVE REQUIREMENTS	□ FACULTY MANDATORY REQUIREMENT	□ Support course family requirements	□ ✓Mandatory requirements	□ Elective requirements
Teaching style	□ Full online learning		□ ✓Blended learning		□ Traditional learning	
Teaching model	□ 2Synchronous: 1asynchronous		□ 2 face to face : 1synchronous		□ 3 Traditional	

Faculty member and study divisions information (to be filled in each semester by the subject instructor)

Name	**Academic rank**	**Office No.**	**Phone No.**	**E-mail**	
Mohammad Alia	**Professor**	**321**		**dr.m.alia@zuj.edu.jo**	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**

Brief description

This course offers a comprehensive introduction to information security and cryptography, emphasizing their critical role in modern computing. It begins with an exploration of classical encryption techniques, including substitution, transposition, and product ciphers, providing a detailed understanding of conventional encryption algorithms and their design principles. Particular attention is given to symmetric encryption, focusing on widely adopted algorithms such as the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES), alongside stream encryption techniques.

Modern cryptographic methodologies are also a key focus, with in-depth coverage of RSA encryption, RSA digital signatures (RSADS), and Diffie-Hellman (DH) secure key exchange. The course further examines the essential topic of pseudorandom number generation and provides an extensive survey of public-key encryption algorithms, highlighting RSA as a cornerstone of modern cryptography.

In addition to these foundational topics, the course introduces students to advanced techniques such as digital watermarking and steganography, offering insights into their practical applications in data security and information concealment. By combining theoretical knowledge with practical examples, this course equips students with the skills and understanding needed to navigate and contribute to the evolving field of cryptography and information security.

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	1. William Stallings, Cryptography and Network Security Principles and Practice 8th-Edition-2023
Supportive learning resources	2. Handbook of applied cryptography, Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, 2011 3. Chapman & Hall - Introduction to Modern Cryptography (2021)

(Books, databases, periodicals, software, applications, others)	4. Sirapat - Authentication and Access Control_ Practical Cryptography Methods and Tools (2021) 5. William Easttom - Modern Cryptography Applied Mathematics for Encryption and Information Security (2021)
Supporting websites	6. https://www.youtube.com/ 7. https://aws.amazon.com/ar/security/opensource/cryptography/
The physical environment for teaching	☐ ✓Class room ☐ labs ☐ Virtual educational platform ☐ Others
Necessary equipment and software	8. https://www.cryptool.org/en/cto/ 9. https://www.openstego.com/
Supporting people with special needs	
For technical support	**E-learning and Open Educational Center. Computer Center**

Course learning outcomes (S= *Skills, C= Competences K= Knowledge,)*

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	Knowledge of basic cryptology terms and concepts	**2**
K2	Know and explain the main components of encryption systems and distinguish between symmetric and asymmetric encryption algorithms	**2**
K3	Know and explain the concepts of number theory	**2**
	Skills	
S1	Apply cryptanalysis attack and brute force attack to crack the encrypted data.	**7**
	Analyze, evaluate, and implement DH protocol, RSA and ElGamal algorithms, and RSADS digital signatures.	**9**
	Competences	
C1	Solve complex problems in cryptography related to key generation, encryption, decryption, and secure communication using both classical and modern algorithms.	**11**
C2	Integrate and apply cryptographic and security concepts to ensure data confidentiality, integrity, and authentication in real-world scenarios, including designing secure systems and protocols.	**11**

Mechanisms for direct evaluation of learning outcomes

Type of assessment / learning style	Fully electronic learning	Blended learning	Traditional Learning (Theory Learning)	Traditional Learning (Practical Learning)
First exam	0	**0**	0	0
Second / midterm exam	%30	**%30**	%30	%30
Participation / practical applications	0	**0**	0	0

Asynchronous interactive activities	%30	**%30**	%30	%30
final exam	%40	**%40**	%40	%40

Note: Asynchronous interactive activities are activities, tasks, projects, assignments, research, studies, projects, work within student groups ... etc, which the student carries out on his own, through the virtual platform without a direct encounter with the subject teacher.

Schedule of simultaneous / face-to-face encounters and their topics

Week	Subject	learning style*	Reference **
1	Introduction: Computer Security Concepts Security Cycle Security Services Security Mechanisms A Model for Network Security	face-to-face	1+3+4
2	Classical Cryptography and Cryptanalysis: Substitution Cipher Transposition Cipher	face-to-face	1+3+4
3	Classical Cryptography and Cryptanalysis: Product Cipher	face-to-face	1+3+4
4	Block Cipher: General View of DES Algorithm. Stream cipher. Public Key Cryptography: Public Key and Secret Key cryptosystems	face-to-face	1
5	Basic concepts in number theory and finite fields Finding GCD, Exponentiations,	face-to-face	1+2
6	Prime Numbers, Euler's Totient Function, Inverse.	face-to-face	1+2
7	Mathematical hard problems based cryptography (classifications) Public-key exchange (Key Management)	face-to-face	1+2+5
8	**Midterm Exam**		
9	Diffie-Hellman Key Exchange examples Elliptic curve Key Exchange	face-to-face	1+2
10	Public-Key Encryption: RSA Algorithm	face-to-face	1+2
11	ElGamal Algorithm	face-to-face	1+2
12	Hash Functions: Secure Hash Algorithm (SHA)	face-to-face	1+2+5
13	Digital Signature Algorithms: RSADS, Digital Signature Algorithm (DSA)	face-to-face	1+2
14	Steganography	face-to-face	1+6+9
15	Discussion and Revision	face-to-face	
16	**Final Exam**		

*** Learning styles: Lecture, flipped learning, learning through projects, learning through problem solving, participatory learning ... etc.**

**** Reference: Pages in a book, database, recorded lecture, content on the e-learning platform, video, website ... etc.**

Schedule of asynchronous interactive activities (in the case of e-learning and blended learning)

Week	Task / activity	Reference	Expected results
1	information Security		1+7
2	Caesar Cipher Implementation		1+6+8
3	Vernam Cipher Implementation		1+6+8
4	S-DES		1+6+8
5	DH		1+2+8
6	RSA		1+2+8
7	Steganography		6+9