جـامعـة الـزيـتـونـــة 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.	**1**		**University Specialization**		**Cybersecurity**	
Course No.	**0125244**		**Course name**		**Cryptography**	
Credit Hours	**3**		**Prerequisite Co-requisite**		**Principles of Cybersecurity**	
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	
Hani Mahmoud Almimi	Assistant Prof.			Hani.mimi@zuj.edu.jo	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**

Brief description

This course gives an introduction to Cryptography and its importance, understanding classical encryption Techniques: Substitution, Transposition and product Ciphers, Examination of conventional encryption algorithms and design principles including transposition and substitution techniques such as DES, understanding of the modern cryptographic techniques such as RSA, Key distribution, digital signature, identification and authentication, and sharing keys. A survey of symmetric encryption, including classical and modern algorithms, are provided. The emphasis is on the two most important algorithms, the Data Encryption Standard (DES) and the Advanced Encryption Standard (AES). This course also covers the most crucial stream encryption algorithm, RC4, and the critical topic of pseudorandom number generation—a survey of public-key algorithms, including RSA (Rivest-Shamir-Adelman).

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	William Stallings, Cryptography and Network Security Principles and Practice 7th-Edition-
Supportive learning resources (Books, databases, periodicals, software, applications, others)	1- Chapman & Hall - Introduction to Modern Cryptography (2021) 2- Sirapat - Authentication and Access Control_ Practical Cryptography Methods and Tools (2021) 3- William Easttom - Modern Cryptography Applied Mathematics for Encryption and Information Security (2021)
Supporting websites	

The physical environment for teaching	✓ Class room	□ labs	✓ Virtual educational platform	□ Others
Necessary equipment and software	Data show Any Programming language (C++ preferred)			
Supporting people with special needs				
For technical support				

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

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	Knowledge of basic coding terms and concepts	
K2	Know, explain and compare types of encryption algorithms	
K3	Knowledge of methodologies and techniques used to protect data	
K4	Know and explain the main components of encryption systems and distinguish between symmetric and asymmetric encryption algorithms	
	Skills	
S1	Apply probability attack, cryptanalysis attack, and brute force attack to crack the encrypted data.	
S2	Clarify common encryption vulnerabilities and threats	
S3	Implement and Designing encrypting algorithms using programming languages	
S4	Clarify the main concepts in cryptography.	
	Explain the main encryption issues related to information and data protection	
	Competences	
C1	Independently manage tasks related to cryptography	
C2	Work collaboratively and constructively	
C3	Have the ability to lead and entrepreneurially perform a wide range of tasks responsibly	
C4	Make constructive decisions in situations that require self-reliance	
	Learn and innovate independently	

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	**%20**	0
Second / midterm exam	%30	%30	**%20**	30%
Participation / practical applications	0	0	**10**	30%

Asynchronous interactive activities	%30	%30	**0**	0
final exam	%40	%40	**%50**	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 **
1/2	Introduction: Computer Security Concepts Security Cycle Security Services Security Mechanisms A Model for Network Security	lecture	9,14,15,17, 20, 22
3	Classical Cryptography and Cryptanalysis: Substitution Cipher Transposition Cipher Product Cipher	Lectures, Problem solving	28-49 61-78
4/5	Block Cipher: General View of DES Algorithm. Stream cipher. Public Key Cryptography: Public Key and Secret Key cryptosystems	Lectures Problem solving	85-112
6	Basic concepts in number theory and finite fields Finding GCD, Exponentiations, Prime Numbers, Euler's Totient Function, Inverse.	Lectures	85-112
7	Hash Functions: Secure Hash Algorithm (SHA) **First Exam**	Lectures, Problem solving	313-339
8/9	Mathematical hard problems based cryptography (classifications) Public-key exchange (Key Management) : Diffie-Hellman Key Exchange examples	Lectures, Problem solving	287-292

	Elliptic curve Key Exchange		
10	Public-Key Encryption: RSA Algorithm	Lectures, Problem solving	253-264
11	Rabin Algorithm ElGamal Algorithm	Lectures, Problem solving	264-292
12/13	Digital Signature Algorithms: RSADS, Digital Signature Algorithm (DSA) Combining Algorithms	Lectures, Problem solving	393-400
14	Steganography	Lectures, Problem solving Group project	52
15	Revision		
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			
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			