Faculty: Information Technology	
Department: Cybersecurity	**Program: Bachelor**
Academic Year: 2023/2024	**Semester: 2nd**

Course Plan

First: Course Information

Course No.: 1506344	***Course Title: Cryptography Theory***	***Credit Hours: 3***	***Theoretical: 3***	***Practical: 0***
Prerequisite No. and Title:150341 - Networks and Information security	***Section No.: 1***	***Lecture Time: 11-12 (Sun, Tue, Thu)***		
Level in JNQF	***7***			
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: Dr. Mohammad Rasmi			***Academic Rank: Associate Professor***		
Office Number: 139 A	***Extension Number: 1515***		***Email: mmousa@zu.edu.jo***		
Course Instructor					
Name: Dr. Mohammad Rasmi			***Academic Rank: Associate Professor***		
Office Number: 139 A	***Extension Number: 1515***		***Email: mmousa@zu.edu.jo***		
Office Hours:	***Sunday***	***Monday***	***Tuesday***	***Wednesday***	***Thursday***
	10:00-11:00	***-***	***10:00-11:00***	***-***	***10:00-11:00***

Third: Course Description

This course gives an introduction to 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, AES, RC4, Key distribution, Diffie–Hellman, digital signature, identification and authentication, and sharing keys. The course includes the implementation of an application or research project by students.

Fourth: Course Objectives

1. Introducing the student to understanding classical encryption techniques: Substitution, Transposition and product Ciphers.
2. Developing the student's ability to examination of conventional encryption algorithms and design principles including transposition and substitution techniques.
3. Guiding the student to understanding of the modern cryptographic techniques such as RSA, AES, RC4, Key distribution, Diffie–Hellman, digital signature, identification and authentication, and sharing keys.
4. Expanding the student's skills of analyzing and solving programming problems by breaking down problems into smaller tasks and applying algorithmic thinking to create efficient solutions.
5. Providing the student with the skills of implementation of an application or research project by students.

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**	Outline the basic and advanced uses of computer and coding concepts.	**PK1**	• Mid-term Exam • Final Exam
	K2	Identify the different types of encryption algorithms for different security needs.	**PK3**	• Mid-term Exam • Final Exam
	K3	Describe the main components of encryption systems and distinguish between symmetric and asymmetric encryption algorithms.	**PK4**	• Quizzes • Mid-term Exam • Final Exam
Skills	**S1**	Recommend approaches to build up and design encryption algorithms using the appropriate tools and programming languages.	**PS1**	• Mid-term Exam • Final Exam
	S2	Apply probability attack, cryptanalysis attack, and brute force attack to crack the encrypted data.	**PS3**	• Mid-term Exam • Final Exam
	S3	Examine the main encryption issues related to information and data protection.	**PS5**	• Quizzes • Mid-term Exam • Final Exam
Competencies	**C1**	Develop effective communication skills with the students in the proper way to deliver the required skills and providing them with knowledge about Cryptography, techniques and tools.	**PC3**	• Participation
	C2	Utilize different techniques for dealing with encryption algorithms.	**PC4**	• Participation

*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 and Network Security Principles and Practice.**		
Author: William Stallings	***Issue No.: 10th***	***Print:***	***Publication Year: 2020***
Additional Sources and Websites:	• **Keith M. Martin. Everyday Cryptography, Second Edition, Oxford University Press, 2017** • **Chapman & Hall - Introduction to Modern Cryptography (2021)** • **Sirapat - Authentication and Access Control_ Practical Cryptography Methods and Tools (2021)** • **William Easttom - Modern Cryptography Applied Mathematics for Encryption and Information Security (2021)**		
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	-Introduction: -Computer Security Concepts	Face-to-Face	Lecturing , quizzes and assignments	Textbook-ch1
2	K1	-Computer Security Concepts	Face-to-Face	Lecturing , quizzes and assignments	Textbook-ch1
3	S1, K2, K3	- Classical Cryptography and Cryptanalysis: Substitution Cipher	Face-to-Face	Lecturing , quizzes and assignments	Textbook-ch2
4	S2, K2, K3	-Transposition Cipher -Product Cipher.	Face-to-Face	Lecturing , quizzes and assignments	Textbook-ch2
5	S2, K2, K3	-Block Cipher: General View of DES Algorithm. -Stream cipher.	Face-to-Face	Lecturing , quizzes and assignments	Textbook-ch4
6	S2, K2, K3	-Public Key Cryptography: -Public Key and Secret Key cryptosystems	Face-to-Face	Lecturing , quizzes and assignments	Textbook-ch4

7	S2, K1, K2, C1	-Basic concepts in number theory and finite fields	Face-to-Face	Lecturing , quizzes and assignments	Textbook-ch2
8	S2, K1, K2	-Finding GCD, Exponentiations, Prime Numbers, Euler's Totient Function, Inverse.	Face-to-Face	Lecturing , quizzes and assignments	Textbook-ch2
Midterm Exam					
9	S3, K1, K2, C2	-Mathematical hard problems based cryptography (classifications) -Public-key exchange (Key Management) :	Face-to-Face	Lecturing , quizzes and assignments	Textbook-ch9
10	S2, K1, K2	-Diffie-Hellman Key Exchange examples -Elliptic curve Key Exchange	Face-to-Face	Lecturing , quizzes and assignments	Textbook-ch9
11	S1, S2, K2, K3	-Public-Key Encryption	Face-to-Face	Lecturing , quizzes and assignments	Textbook-ch9
12	S1, S2, K2, K3	-RSA Algorithm	Face-to-Face	Lecturing , quizzes and assignments	Textbook-ch10
13	S1, S2, K2, K3	-Rabin Algorithm	Face-to-Face	Lecturing , quizzes and assignments	Textbook-ch10
14	S1, S2, K2, K3	-ElGamal Algorithm -Steganography	Face-to-Face	Lecturing , quizzes and assignments	Textbook-ch10
Final Exam					

*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	C1	C2	
First Exam												
Second Exam												
Mid-term Exam			35	✓	✓	✓	✓	✓	✓	✓	✓	
Participation			5									
Asynchronous Activities												
Quizzes			5	✓	✓	✓				✓		
Assignments			5	✓	✓	✓				✓		
Group presentation												
Final Exam			50	✓	✓	✓	✓	✓	✓	✓	✓	
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	Dr. Mohammad Rasmi AL-Mousa		
Faculty Dean	Prof. Dr. Mohammad Hassan		