The University of Jordan

Accreditation & Quality Assurance Center

Course Syllabus

Course Name: Cryptography Theory

مركز الاعتماد وضمان الجودة
ACCREDITATION & QUALITY ASSURANCE CENTER

Course Syllabus

1	**Course title**	**Cryptography Theory**
2	**Course number**	0301446
3	**Credit hours**	3
	Contact hours (theory, practical)	3
4	**Prerequisites/corequisites**	0301342
5	**Program title**	B.Sc. Mathematics
6	**Program code**	
7	**Awarding institution**	The University of Jordan
8	**School**	Science
9	**Department**	Mathematics
10	**Course level**	Elective Specialization requirement
11	**Year of study and semester (s)**	3rd or 4th year, 1st and 2nd or summer semester
12	**Other department (s) involved in teaching the course**	None
13	**Main teaching language**	English
14	**Delivery method**	On line
15	**Online platforms(s)**	■Moodle ■Microsoft Teams ☐Skype☐Zoom ☐Others……
16	**Issuing/Revision Date**	10th Oct, 2022

17 Course Coordinator:

Name:Prof. Emad Abuosba	Contact hours: 2:30 – 4 (Mon, Wed)
Office number:308	Phone number: 22088
Email: eabuosba@ju.edu.jo	

مركز الاعتماد وضمان الجودة
ACCREDITATION & QUALITY ASSURANCE CENTER

18 Other instructors:

Name: Office number: Phone number: Email: Contact hours: Name: Office number: Phone number: Email: Contact hours:

19 Course Description:

As stated in the approved study plan. Classical Cryptosystems such as: Shift ciphers, Affine ciphers, The Vigenere cipher, Substitution ciphers, The Playfair cipher, ADFGX cipher, and Block ciphers. One-time pad, Pseudo-Random Bit Generation, and Linear feedback shift register. World War II ciphers such as: Enigma and Lorenz. Public key cryptosystems, The RSA, Primality testing and attack on RSA, The ELGamal Public key cryptosystem. Symmetric block cipher systems such as: DES and Rijndael. Digital Signatures such as: RSA signatures, The ELGamal signature scheme, and Hash functions. Elliptic curves and elliptic curves cryptosystems. (If time permit)

20 Course aims and outcomes:

A- Aims:

This course will introduce the students to the field of cryptography theory. The main aims of this course are:

1. The students are aware of the idea of cryptography and the various applications of it.
2. The students encrypt and decrypt messages using various kinds of cryptosystems.
3. The students conduct simple attacks on the classical cryptosystems.
4. The students use softwares to perform encrypting and decrypting messages.

B- Students Learning Outcomes (SLOs):

Upon successful completion of this course, students will be able to:

SLOs / SLOs of the course	SLO (1)	SLO (2)	SLO (3)	SLO (4)	SLO (5)	SLO (6)	SLO (7)	SLO (8)
1 Outline the procedure of different kinds of cryptosystems	●	●						
2 Choose suitable cryptosystem to encrypt a message	●	●						
3 Prove mathematically the security of a given cryptosystem							●	
4 Use Mathematica to encrypt and decrypt messages	●	●				●		●
5 Work in team to write a report on a cryptosystem and deliver it to his colleges				●		●		

21 . Topic Outline and Schedule:

Week	Lecture	Topic	Student Learning Outcome	Learning Methods (Face to Face/Blended/ Fully Online)	Platform	Synchronous/ Asynchronous Lecturing	Evaluation Methods	Resources
1	1.1	Introduction	1	On Line	Microsoft Teams		Homework	Text Book
	1.2	Simple Substitution Cyphers	1	On Line	Microsoft Teams		Homework	Text Book
	1.3	Simple Substitution Cyphers	1	On Line	You Tube		Homework	Text Book
2	2.1	Cryptography before Computers	1,2	On Line	Microsoft Teams		Homework	Text Book
	2.2	Cryptography before Computers	1,2	On Line	Microsoft Teams		Homework	Text Book
	2.3	Cryptography before Computers	1,2	On Line	You Tube		Homework	Text Book
3	3.1	Cryptography before Computers	1,2	On Line	Microsoft Teams		Homework	Text Book
	3.2	Cryptography before Computers	1,2	On Line	Microsoft Teams		Homework	Text Book
	3.3	Symmetric and Asymmetric Ciphers	1,2	On Line	You Tube		Homework	Text Book
4	4.1	**Homework**						
	4.2	Public Key Cryptography	3,4	On Line	Microsoft Teams		Midterm	Text Book
	4.3	Discrete Log Problem	3,4	On Line	Microsoft Teams		Midterm	Text Book
5	5.1	Discrete Log Problem	3,4	On Line	You Tube		Midterm	Text Book
	5.2	Diffie Hellman Key Exchange	3,4	On Line	Microsoft Teams		Midterm	Text Book
	5.3	Diffie Hellman Key Exchange	3,4	On Line	Microsoft Teams		Midterm	Text Book
6	6.1	ELGamal Cryptosystem	3,4	On Line	You Tube		Midterm	Text Book

	6.2	ELGamal Cryptosystem	3,4	On Line	Microsoft Teams		Midterm	Text Book
	6.3	Collision Algorithm	3,4	On Line	Microsoft Teams		Midterm	Text Book
7	7.1	Collision Algorithm	3,4	On Line	You Tube		Midterm	Text Book
	7.2	Pohling Hellman Algorithm	3,4	On Line	Microsoft Teams		Midterm	Text Book
	7.3	Pohling Hellman Algorithm	3,4	On Line	Microsoft Teams		Midterm	Text Book
8	8.1	**Midterm**		On Campus				
	8.2	Integer Factorization	3,4	On Line	You Tube		Quiz	Text Book
	8.3	Integer Factorization	3,4	On Line	Microsoft Teams		Quiz	Text Book
9	9.1	Integer Factorization	3,4	On Line	Microsoft Teams		Quiz	Text Book
	9.2	Primality Testing	3,4	On Line	You Tube		Quiz	Text Book
	9.3	Primality Testing	3,4	On Line	Microsoft Teams		Quiz	Text Book
10	10.1	RSA Cryptosystem	3,4	On Line	Microsoft Teams		Quiz	Text Book
	10.2	RSA Cryptosystem	3,4	On Line	You Tube		Quiz	Text Book
	10.3	RSA Cryptosystem	3,4	On Line	Microsoft Teams		Quiz	Text Book
11	11.1	**Quiz # 1**		Moodle				
	11.2	Elliptic Curves	3,4	On Line	Microsoft Teams		Quiz	Text Book
	11.3	Elliptic Curves	3,4	On Line	You Tube		Quiz	Text Book
12	12.1	Elliptic Curves	3,4	On Line	Microsoft Teams		Quiz	Text Book
	12.2	Digital Signature	3,4	On Line	Microsoft Teams		Quiz	Text Book
	12.3	Digital Signature	3,4	On Line	You Tube		Quiz	Text Book
13	13.1	Digital Signature	3,4	On Line	Microsoft Teams		Quiz	Text Book
	13.2	Hash Functions	3,4	On Line	Microsoft Teams		Quiz	Text Book
	13.3	Hash Functions	3,4	On Line	You Tube		Quiz	Text Book
14	14.1	**Quiz # 2**		Moodle	Microsoft Teams			

	14.2	Reports Discussion	5	On Campus			Oral Exam	
	14.3	Reports Discussion	5	On Campus			Oral Exam	
15	15.1	Reports Discussion	5	On Campus			Oral Exam	
	15.2	Reports Discussion	5	On Campus			Oral Exam	
	15.3	Reports Discussion	5	On Campus			Oral Exam	

22 Evaluation Methods:

Opportunities to demonstrate achievement of the SLOs are provided through the following assessment methods and requirements:

Evaluation Activity	Mark	Topic(s)	SLOs	Period (Week)	Platform
Quiz #1	10		8		Moodle
Quiz #2	10		8		Moodle
Report	10		4,6		On Campus
Midterm	30		1,2,7		On Campus
Final Exam	40		1,2,7		On Campus

23 Course Requirements

Each student must have:

- Computer
- Internet connection
- Webcam
- MATHEMATICA package
- Account on Microsoft Teams

مركز الاعتماد وضمان الجودة
ACCREDITATION & QUALITY ASSURANCE CENTER

24 Course Policies:

The course will be given on line during the Fall Semester. Lectures will be recorded and downloaded on a special channel on Microsoft Teams. Every week there will be two meetings using Microsoft Teams. We will use extensively MATHEMATICA package to solve numerical problems.

A- Attendance policies: Students must attend all the meetings on Microsoft Teams, the student will fail the course if he doesn't attend 4 meetings without a prior permission.

B- Absences from exams and submitting assignments on time: Students must attend all the exams, student with acceptable excuse will have an average of the other exams

C- Health and safety procedures:

D- Honesty policy regarding cheating, plagiarism, misbehavior: Cheating is strictly prohibited, any cheating in the exams or the home works will be assigned zero mark.

E- Grading policy: Quizzes will be multiple choice questions, while home works would be essay questions. The exams would be essay questions.

F- Available university services that support achievement in the course: We will use the E-learning and the JU-Exam system platforms, but if we have troubles, then we will use google meet and google forms platforms.

25 References:

A- Required book(s), assigned reading and audio-visuals:
Text Book: J. Hoffstein, J. Pipher and J. Silverman: An Introduction to Mathematical Cryptography, 2008, Springer
B- Recommended books, materials and media:
Wade Trappe and Lawrence C. Washington: Introduction to Cryptography with Coding Theory, 2nd edition, Prentice Hall

26 Additional information:

Name of Course Coordinator: Prof. Emad Abuosba Signature: ---------- Date: 10-10-2022
Head of Curriculum Committee/Department: Prof. Ahmad Al Zghoul-- Signature: ----------
Head of Department: -Prof. Manal Ghanem - Signature: -M. Ghanem
Head of Curriculum Committee/Faculty: ---------- Signature: ----------
Dean: Mahmoud Jaghoub Signature: ----------