Form: Course Syllabus	**Form Number**	EXC-01-02-02A
	Issue Number and Date	2/3/24/2022/2963 05/12/2022
	Number and Date of Revision or Modification	
	Deans Council Approval Decision Number	2/3/24/2023
	The Date of the Deans Council Approval Decision	23/01/2023
	Number of Pages	06

1.	**Course Title**	**Cryptography Theory**
2.	**Course Number**	0301446
3.	**Credit Hours (Theory, Practical)**	3
	Contact Hours (Theory, Practical)	3
4.	**Prerequisites/ Corequisites**	0301342
5.	**Program Title**	B.Sc. Mathematics
6.	**Program Code**	
7.	**School/ Center**	Science
8.	**Department**	Mathematics
9.	**Course Level**	Elective Specialization requirement
10.	**Year of Study and Semester (s)**	3rd or 4th year, 1st and 2nd or summer semester
11.	**Other Department(s) Involved in Teaching the Course**	None
12.	**Main Learning Language**	English
13.	**Learning Types**	☐Face to face learning ☐Blended ■Fully online
14.	**Online Platforms(s)**	■Moodle ■Microsoft Teams
15.	**Issuing Date**	3 – 10 – 2024
16.	**Revision Date**	

17. Course Coordinator:

Name: Prof. Emad Abuosba Contact hours: 2:30 – 4 (Mon, Wed)

Office number: Math 308 Phone number: 22088

Email: eabuosba@ju.edu.jo

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 Play fair 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. Program Student Outcomes (SO's):

(To be used in designing the matrix linking the intended learning outcomes of the course with the intended learning outcomes of the program)

1. Identify, formulate, and solve broadly-defined technical or scientific problems by applying knowledge of Mathematics and Science and/or technical topics to areas relevant to the discipline.
2. Formulate or design a system, process, procedure or program to meet desired needs.
4. Communicate effectively with a range of audiences in oral or written forms and exhibit ethical and professional values.
6. Function effectively on teams that establish goals, plan tasks, meet deadlines, and analyze risk and uncertainty.

7. Utilize research methods, critical and creative thinking skills to assess and analyze information to solve problems properly, then draw valid reasoning and logical conclusions leading to true consequences.
8. Utilize techniques, skills, and modern scientific tools such as mathematical packages, statistical software, graphing calculators, and online resources necessary for professional practice.

21. Course Intended Learning Outcomes (CLO's):

(Upon completion of the course, the student will be able to achieve the following intended learning outcomes)

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

Course CLOs	The learning levels to be achieved					
	Remembering	Understanding	Applying	Analysing	evaluating	Creating
CLO 1	•					
CLO 2		•	•		•	
CLO 3				•		
CLO 4			•			
CLO 5						•

22. The matrix linking the intended learning outcomes of the course with the intended learning outcomes of the program:

Program SO's / Course CLO's	SO (1)	SO (2)	SO (3)	SO (4)	SO (5)	SO (6)	SO (7)	SO (8)
CLO (1)	•	•						
CLO (2)	•	•						
CLO (3)							•	
CLO (4)	•	•				•		•
CLO (5)				•		•		

23. Topic Outline and Schedule:

Week	Lecture	Topic	CLO/s Linked to the Topic	Learning Types (Face to Face (FF)/ Blended/ Fully Online)	Platform Used	Synchronous (S) / Asynchronous (A) Lecturing	Evaluation Methods	Learning Resources
1	1.1	Introduction	1	FF	Teams	S		Textbook
	1.2	Simple Substitution Cyphers	1	FF	Teams	A		YouTube
2	2.1	Simple Substitution Cyphers	1	FF	Teams	S		Textbook
	2.2	Cryptography before Computers	2	FF	Teams	A		YouTube
3	3.1	Cryptography before Computers	2	FF	Teams	S		Textbook
	3.2	Cryptography before Computers	2	FF	Teams	A		YouTube
4	4.1	Project 1	2	FF	Teams	S	Project	Textbook
	4.2	Project 1	2	FF	Teams	S		Textbook
5	5.1	Symmetric and Asymmetric Ciphers	3	FF	Teams	A		YouTube
	5.2	Public Key Cryptography	3	FF	Teams	S		Textbook
6	6.1	Discrete Log Problem	3	FF	Teams	A		YouTube
	6.2	Diffie Hellman Key Exchange	3+4	FF	Teams	S		Textbook
7	7.1	ELGamal Cryptosystem	3+4	FF	Teams	A		YouTube
	7.2	Collision Algorithm	3+4	FF	Teams	S		Textbook
8	8.1	Pohling Hellman Algorithm	3+4	FF	Teams	A		YouTube
	8.2	Project 2	2+5	FF	Teams	S	Project	Textbook
9	9.1	Project 2	2+5	FF	Teams	S		Textbook
	9.2	**Midterm**	1-5	FF	Teams	S	Exam	Textbook
10	10.1	Integer Factorization	3	FF	Teams	S		Textbook
	10.2	Primality Testing	3	FF	Teams	A		YouTube
11	11.1	RSA Cryptosystem	3+4	FF	Teams	S		Textbook
	11.2	Digital Signature	3+4	FF	Teams	A		YouTube
12	12.1	Hash Functions	3+4	FF	Teams	S		Textbook
	12.2	Project 3	2+4+5	FF	Teams	S	Project	Textbook
13	13.1	Project 3	2+4+5	FF	Teams	S		Textbook
	13.2	Reports Discussion	5	FF	Teams	S	Oral Exam	Open Sources
14	14.1	Reports Discussion	5	FF	Teams	S	Oral Exam	Open Sources
	14.2	Reports Discussion	5	FF	Teams	S	Oral Exam	Open Sources
15	15.1	Reports Discussion	5	FF	Teams	S	Oral Exam	Open Sources
	15.2	Reports Discussion	5	FF	Teams		Oral Exam	Open Sources

24. Evaluation Methods:

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

Evaluation Activity	Mark	Topic(s)	CLO/s Linked to the Evaluation activity	Period (Week)	Platform
Project 1	10	Ch. 1	1+2	4th week	On Campus
Project 2	10	Ch. 2	2+5	8th week	On Campus
Midterm Exam	20	Ch.1 + Ch. 2	1 – 5	9th week	On Campus
Project 3	10	Ch. 3	2+4+5	12th week	On Campus
Report	10		1 – 5	14th week	Teams
Final Exam	40		1 – 5		On Campus

25. Course Requirements:

Each student must have:

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

26. 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.

27. References:

A- Required book(s), assigned reading and audio-visuals:

Textbook: 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

28. Additional information:

Name of the Instructor or the Course Coordinator: **Prof. Emad A. Abuosba**	Signature: ……	Date: 3 – 10 – 2024
Name of the Head of Quality Assurance Committee/ Department: **Prof. Manal Ghanem**	Signature: ……	Date: ……
Name of the Head of Department: **Prof. Baha Alzalg**	Signature: ……	Date: ……
Name of the Head of Quality Assurance Committee/ School of Science: **Prof. Emad A. Abuosba**	Signature: ……	Date: ……
Name of the Dean or the Director: **Prof. Mahmoud I. Jaghoub**	Signature: ……	Date: ……