1.	Course title	Cryptography
2.	Course number	**1911241**
3.	Credit hours (theory, practical)	3
	Contact hours (theory, practical)	3
4.	Prerequisites/corequisites	Discrete (1901101) + Principles of Security (1911194)
5.	Program title	Cyber security
6.	Year of study and semester (s)	First year (Fall) 2022/2023
7.	Final Qualification	Bachelor's degree
8.	Other department (s) involved in teaching the course	None
9.	Language of Instruction	English
10.	Date of production/revision	September, 2022 / February, 2023
11.	Required/ Elective	Required

12. Course Coordinator:

Dr. Oraib AbuAlganam
Office numbers:
Phone number:
Email addresses: o.Abualganam@ju.edu.jo

13. Other instructors:

Dr. Ahmad Al Hwaitat
Office numbers:
Phone number:
Email addresses: o.hwaitat@ju.edu.jo

14. Course Description:

This course introduces cryptography algorithms and mechanisms including: symmetric key algorithms such as AES and 3DES, public key algorithms such as RSA and ECC, digital signature, hash functions and MAC. The course provides security analysis to the algorithms as well

15. Course aims and outcomes:

A- Aims:

Goal:

The main goal of this course is to provide students with required mathematical knowledge of symmetric and asymmetric cipher techniques. Moreover, provide students with basic security requirements that should be considered in designing phase.

Objectives:

- *Describe the fundamental concepts of encryption theory and information hiding.*
- *Describe modern private-key cryptosystems and ways to cryptanalyze them.*
- *Understand the modern encryption (stream and block) cipher techniques such as (RC4, DES, AES).*
- *Understand other block cipher operations such as (3DES, ECB, CBC).*
- *Understand the public-key cryptography such as RSA and ECC*
- *Understand message authentication code and hash functions.*
- *Implement and cryptanalyze complete protocol using SPAN AVISPA.*
- *Key Distribution and Management and X.509 certificates.*

ABET Outcomes

CAC-1: Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions.

CAC-2: Design, implement, and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline.

B- Intended Learning Outcomes (ILOs): Upon successful completion of this course students will be able to …

A-Knowledge and understanding: with the ability to …

A1) Learn the basic concepts involved with cyber security of functions.
A2) Understand the issues related to cybersecurity.
A3) Understanding the importance of having secure network using cryptography.
A4) Describe the fundamental concepts of encryption theory and information hiding.
A5) Describe modern private-key cryptosystems and ways to cryptanalyze them.

B- Intellectual skills: with the ability to …

B1) Distinguish between symmetric and asymmetric encryption.
B2) Analyze and compare between the advantages and disadvantages of different encryption techniques.
B3) Classify different types of security attacks.

C- Subject specific skills – with ability to …

C1) Understand the modern encryption technique such as (DES, AES).
C2) Understand other block cipher operations such as (3DES, ECB, CBC).
C3)Understand the public-key cryptography such as RSA and ECC
C4) Understand message authentication code and hash functions.

D- Transferable skills – with ability to

D1) Implement and cryptanalyze complete protocol using SPAN AVISPA.
D2) Key Distribution and Management and X.509 certificates

16. Topic Outline and Schedule:

Topic	Week	ILOs	ABET Outcomes	TLA (teaching, learning and Assessment)
1.Quick Revision for Number Systems	1	---	-	
2. Introduction to Cryptography	2	A1-A2-A3-A4	-	
3. Classical Encryption Techniques • Caesar Cipher. • Monoalphabetic Cipher • Play fair Cipher. • Hill Cipher. • Polyalphabetic Cipher (Vigenere Cipher) • Rail fence cipher • Route cipher	3,4	A4- B1-B2	**CAC-1**	
4. Modern Encryption Techniques • Stream cipher (RC4)	5	C1-B2	**CAC-1**	
5. Modern Encryption Techniques • AES Block Cipher Operation • SDES, DES and 3DES	6	C2-B2	**CAC-1**	
Midterm Exam				
6. **Public key Cryptography** • Terminology Related to Asymmetric Encryption. • Pre RSA . • RSA.	7	C3	**CAC-1**	
7. Public key Cryptography • Diffie-Hellman Algorithm.	8	C3-B2	**CAC-1**	

8. SPAN AVISPA **Cryptography data integrity algorithm** • Message Authentication Functions • SHA-512	9,10	B3-C4-D1	**CAC-2**		
Key Management and Distribution **X.509** certificates	11,12	D2	**CAC-2**		
Final	13				

1. Evaluation Methods and Course Requirements (Optional):

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

There will be several assessment methods of evaluation the performance of the students such as class participation, grading the quizzes; assignments; conducting the midterm, short test and the final exam.

2. Course Policies:

A- Attendance policies:
Deliberate abstention from attending **1911241** *classes and any other similar acts will lead to student deprivation from the course according to the UJ regulations*

B- Absences from exams and handing in assignments on time:

If you miss the midterm, then a makeup exam will not be provided unless you submit a valid absence excuse, within three days from the midterm, to your lecturer. This excuse must be signed and stamped from the UJ hospital in order to be valid. If your lecturer accepts the excuse then you will be able to take the makeup. You need to follow up the departmental announcements regarding the makeup date and time. Please note that the lecturer may either accept or reject your excuse based on UJ regulations

C- Health and safety procedures:

N/A

D- Honesty policy regarding cheating, plagiarism, misbehavior:

All students in this course must read the University policies on plagiarism and academic honesty
http://registration.ju.edu.jo/RegRegulations/Forms/All_Regulations.aspx

E- Grading policy:

- *Midterm Exam:*	*30%*
- *Quizzes, assignments and Tasks*	*20%*
- *Final Exam:*	*50%*

F- Available university services that support achievement in the course:

N/A

G- Statement on Students with disabilities

Students with Disabilities: Students with disabilities who need special accommodations for this class are encouraged to meet with the instructor and/or their academic advisor as soon as possible. In order to receive accommodations for academic work in this course, students must inform the course instructor and/or their academic advisor, preferably in a written format, about their needs no later than the 4th week of classes.

3. Required equipment:

- Virtual Box
- SPAN AVISP
- OpenStego tool

4. References:

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

- Cryptography and Network Security: Principles and Practice, William Stallings, 7th Edition, 2017

B. Recommended books, materials, and media:

- Cryptography: Theory and Practice, Third Edition, Douglas R. Stinson, CRC Press, 2006.
- Introduction to Cryptography with Coding Theory, Trappe & Washington, Prentice Hall, 2005.
- Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. Van Orschot, Scott A. Vanstone, CRC Press.
- Heys' tutorial on linear and differential cryptanalysis.

C. **Additional information:**

YouTube videos are presented to support the learning process

Date: 2/10/2022

Name of Course Coordinator: Dr. Oraib AbuAlganam Signature:

Head of curriculum committee/Department: ---------- Signature: ----------

Head of Department: ---------- Signature: ----------

Head of curriculum committee/Faculty: ---------- Signature: ----------

Dean: ---------- -Signature: ----------

Copy to:
Head of Department
Assistant Dean for Quality Assurance
Course File