جامعة الزيتونة الأردنية

Al-Zaytoonah University of Jordan

Course Syllabus

According to JORDAN National Qualification Framework (JNQF)

Course Name: Mathematics in Cyber Security

Course Number: 0101375

General Course Information:

Course Title	Mathematics in Cyber Security
Course Number	0101375
Credit Hours	3 credit hours
Education Type	Traditional learning
Prerequisites/Co-requisites	-
Academic Program	Bachelor
Program Code	…
Faculty	Faculty of Science and Information Technology
Department	Mathematics
Level of Course	3
Academic Year /Semester	2024/2025 1st-Semester
Awarded Qualification	BSc
Other Department(s) Involved in Teaching the Course	-
Language of Instruction	English
Date of Production	2024-2025
Date of Revision	November 2024

Course Coordinator:

Coordinator's Name	
Office No.	
Office Phone Extension Number	
Office Hours	
E-mail	

Other Instructors:

Instructor Name	
Office No.	
Office Phone Extension Number	
Office Hours	
Email	

Course Description *(English/Arabic)*:

English	This course introduces students to the essential mathematical concepts underpinning modern cybersecurity. The course covers foundational topics such as logic, number theory, modular arithmetic, probability, and graph theory, demonstrating their relevance in real-world security applications. Students will learn how these mathematical principles are applied in encryption, network security, error detection, and data integrity, forming the basis for secure information systems. The course progresses from basic concepts to applications, including how prime numbers support encryption, modular arithmetic's role in secure communication, and how probability aids in risk assessment.
Arabic	تقدم هذه الدورة للطلاب المفاهيم الرياضية الأساسية التي تدعم الأمن السيبراني الحديث. وتغطي الدورة مواضيع أساسية مثل المنطق ونظرية الأعداد والحساب المعياري والاحتمالات ونظرية الرسم البياني، مع توضيح أهميتها في تطبيقات الأمن في العالم الحقيقي. سيتعلم الطلاب كيفية تطبيق هذه المبادئ الرياضية في التشفير وأمان الشبكة واكتشاف الأخطاء وسلامة البيانات، وتشكيل الأساس لأنظمة المعلومات الآمنة. تتقدم الدورة من المفاهيم الأساسية إلى التطبيقات، بما في ذلك كيفية دعم الأعداد الأولية للتشفير ودور الحساب المعياري في الاتصالات الآمنة وكيف تساعد الاحتمالات في تقييم المخاطر.

Textbook: *Author(s), Title, Publisher, Edition, Year, Book website.*

Eric Lehman, F. Thomson Leighton, and Albert R. Meyer, Mathematics for Computer Science, Samurai Media Limited, England, 2017.

References: *Author(s), Title, Publisher, Edition, Year, Book website.*

William Stallings, Cryptography and Network Security: Principles and Practice, Pearson Education Limited, England, 2017.

Course Educational Objectives (CEOs):

CEO1	Develop Mathematical Foundations
CEO2	Apply Mathematics to Cybersecurity Problems
CEO3	Enhance Problem-Solving Skills
CEO4	Prepare for Advanced Cybersecurity Studies

Intended Learning Outcomes (ILO's):

Intended learning outcomes (ILOs)		**Relationship to CEOs**	**Contribution to PLOs**	**Bloom Taxonomy Levels***	**JNQF Descriptors****
K	Knowledge and understanding				
1. ILO1-k	Students will demonstrate an understanding of foundational mathematical concepts, including number theory, modular arithmetic, probability, and logic, and recognize their applications in cybersecurity.	CEO1	PLO1-k	Remembering	K
2. ILO2-k	Students will understand how mathematical principles are applied to various cybersecurity functions, such as encryption, data integrity, and network security, and appreciate the importance of these concepts in protecting information.	CEO2	PLO2-k	Understanding	K
S	Intellectual skills				
3. ILO3-s	Students will develop the ability to apply mathematical methods, such as modular arithmetic and prime number theory, to solve real-world cybersecurity challenges, including encryption and data protection.	CEO3	PLO5-s	Analysing	S
4. ILO4-s	Students will be able to critically analyze cryptographic algorithms and evaluate their security, using mathematical reasoning to assess strengths and weaknesses in protecting data.	CEO3	PLO6-s	Applying	S
5. ILO5-s	Students will develop the skill to use probability and combinatorics to model and assess security risks,	CEO3	PLO7-s	Creating	S

	helping them make informed decisions about potential vulnerabilities in cybersecurity systems.				
C	Subject specific skills				
6. ILO6-c	Students will acquire the skill to implement and analyze basic cryptographic methods, such as symmetric and asymmetric encryption, hashing, and error detection techniques, using mathematical principles to secure data and communications effectively.	CEO1-CEO4	PLO9-c	Applying	C

***Bloom Taxonomy Levels:**						
Level #	1	2	3	4	5	6
Level Name	Remembering	Understanding	Applying	Analysing	Evaluating	Creating
**** Descriptor (National Qualification Framework Descriptors): K: Knowledge, S: Skill, C: Competency.**						

Program Learning Outcome (PLOs):

	(PLOs)	**JNQF Descriptors****		
		K	**S**	**C**
1	Understand the Fundamental Mathematical Concepts.	√		
2	Comprehend the Principles of Cryptography.	√		
3	Grasp systematic approaches to defining and constructing models.	√		
4	Recognize the Role of Mathematics in Cybersecurity Systems.	√		
5	Analyze Modular Arithmetic in Cryptography.		√	
6	Evaluate the Security of Cryptographic Algorithms.		√	
7	Apply Probability to Cybersecurity Risk Analysis.		√	
8	Implement Cryptographic Algorithms Using Mathematical Principles.			√
9	Use Mathematical Methods for Data Integrity and Error Detection.			√

**** Descriptors according to the national qualifications framework (K: knowledge, S: skill, C: Competency)**

Weekly Schedule *(please choose the type of teaching)*

☒ **Face to Face** (F2F)

□ Hybrid *(One – To - One)*

□ Online

Schedule of Simultaneous and their Topics:

Week	**First Lecture (F2F)**	**IL**	**PLOs**	**JNQF**

		Os		Descriptors*
1	Introduction to Cybersecurity and Mathematical Foundations (**Propositional Logic**).	ILO1-k	PLO1-k	Understanding
2	Number Theory Basics (Divisibility).	ILO2-k	PLO2-k	Understanding
3	Modular Arithmetic (Modular Arithmetic).	ILO2-k	PLO2-k	Understanding
4	Introduction to Counting and Combinatorics, (Counting).	ILO3-k	PLO3-k	Understanding
5	Simple Ciphers and Encryption (review) and handouts on basic ciphers	ILO4-s	PLO5-s	Remembering
6	Probability Basics (Probability).	ILO5-s	PLO6-s	Remembering
7	Advanced Counting Methods (Permutations and Combinations).	ILO5-s	PLO7-s	Applying
Midterm Exam				
9	Public Key Cryptography and Prime Numbers Prime Numbers).	ILO5-s	PLO7-s	Remembering
10	Introduction to Graph Theory (Graphs)	ILO5-s	PLO7-s	Remembering
11	Mathematics of Network Security (Graph Theory concepts).	ILO6-c	PLO7-s	Remembering
12	Error Detection and Correction (Error Correction).	ILO6-c	PLO8-c	Understanding
13	Introduction to Boolean Algebra (Boolean Algebra).	ILO6-c	PLO9-c	Applying
14	Risk Analysis using Probability (Probability Applications).	ILO6-c	PLO9-c	Analyzing
15	Review of Mathematical Concepts for Cybersecurity (Review key topics).			
16	**Final Exam**			

* **K: Knowledge, S: Skills, C: Competency**

Teaching Methods and Assignments:

Development of ILOs is promoted through the following teaching and learning methods:

- Lecture.
- Zoom and Videos
- learning through projects.
- learning through problem solving.
- participatory learning

Course Policies:

A- Attendance policies:

The maximum allowed absences is 15% of the lectures.

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

Midterm exam can be retaken based on approval of excuse by the instructor's discretion.

Not handing assignment on time will incur penalties.

C- Academic Health and safety procedures

D- Honesty policy regarding cheating, plagiarism, and misbehaviour:

Cheating, plagiarism, misbehaviour will result in zero grade and further disciplinary actions may be taken.

E- Grading policy:

- All homework is to be posted online through the e-learning system.
- Exams will be marked within 72 hours and the marked exam papers will be handed to the students.
- Online Activities (Course Videos, Practice labs, Discussion Forums, Quizzes) 3**0%**
- Midterm 30**%**
- Final Exam 40 **%**

F- Available university services that support achievement in the course: **E-Learning Platform, Labs, Library.**

Required Equipment:

- PC / Laptop with webcam and mic
- Internet Connection
- Access to the ZUJ E-Learning Platform at https://exams.zuj.edu.jo/
- E-learning plan
- Satisfaction questionnaires for online and face-to-face learning
- Training

Assessment Tools Implemented in the Course:

- Final Exam
- Midterm Exam
- Quizzes
- Homework
- Discussion Forums
- Periodic reports for learning assessment
- Improvement plans for online or face-to-face teaching.

Responsible Persons and their Signatures:

Course Coordinator	Dr. Iqbal M. Batiha	**Completed Date**	**11/07/2024**
		Signature	iqbalbatiha

Received by (Department Head)		**Received Date**	/ /
		Signature	