QF01/0408-4.0E	Course Plan for Bachelor program - Study Plan Development and Updating Procedures/ Cyber Security Department

Study plan No.	**3**		**University Specialization**	**Cybersecurity**	
Course No.	**0133223**		**Course name**	**Data integrity and authentication**	
Credit Hours	**3**		**Prerequisite Co-requisite**	**Cryptography Theory**	
Course type	☐ MANDATORY UNIVERSITY REQUIREMENT	☐ UNIVERSITY ELECTIVE REQUIREMENTS	☐ FACULTY MANDATORY REQUIREMENT ☐ Support course family require ments	✓ Mandatory requirements	☐ Elective requirements
Teaching style	☐ **Full online learning**		✓ **Blended learning**	☐ **Traditional learning**	
Teaching model	☐ **2Synchronous: 1asynchronous**		✓ **1 face to face : 1synchronous**	☐ **3 Traditional**	

Faculty member and study divisions information (to be filled in each semester by the subject instructor)

Name	Academic rank	Office No.	Phone No.	E-mail	
Dr Farhan Farhan				**Farhan.a@zuj.edu.jo**	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**
1	[12:30_14:00] ح (ن) ث (م)	**9202**	**36**		
2	[11:00_12:30] ن (م) ر (ن)	**9204**	**44**		

Brief description

This Course provides knowledge of data integrity and authentication techniques. The following topics must be included in this Course: Authentication Strength, Password Attack Techniques, Password Storage Techniques: Cryptographic Hash Functions, Collision Resistance, Salting, and Data integrity: Message Authentication Codes(MAC), (HMAC), Digital Signatures

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	***Security+ Guide to Network Security Fundamentals,* Seventh Edition Mark Ciampa** ***Cryptography and Network Security Principles and Practice Eighth Edition Global Edition William Stallings***			
Supportive learning resources (Books, databases, periodicals, software, applications, others)	1. W. Stallings, "Cryptography and Network Security Principles and Practice", Pearson Education, 2020, 8th edition 2. Kevin D. Mitnick, Robert Vamosi - The Art of Invisibility_ The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data-Little, Brown and Company (2017) 3. William Stallings - Effective Cybersecurity_ A Guide to Using Best Practices and Standards-Addison-Wesley Professional (2018)			
Supporting websites				
The physical environment for teaching	✓ Class room	☐ labs	✓ Virtual educational platform	☐ Others

Necessary equipment and software	Data show
Supporting people with special needs	
For technical support	

Course learning outcomes (S= *Skills, C= Competences K= Knowledge,)*

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	Define the main concepts in authentication, authorization,and data integrity.	**MK1, MK2**
K2	Describe the different types of authentication credentials	**MK1, MK2**
K3	Demonstrate common attacks on passwords.	**MK1, MK2**
K4	Summarize the benefits and challenges of multifactor authentication.	**MK1, MK2**
	Skills	
S1	Contrast the concepts and techniques to achieve data integrity and Authentication	**MS2**
S2	Apply basic functions associated with storing sensitive data, such as cryptographic hash functions, salting, iteration count, password-based key derivation, and password managers	**MS1**
	Competences	
C1	Illustrate the use of cryptography to provide data integrity, such as message authentication codes, digital signatures, authenticated encryption	**MC1**

Mechanisms for direct evaluation of learning outcomes

Type of assessment / learning style	Fully electronic learning	Blended learning	Traditional Learning (Theory Learning)	Traditional Learning (Practical Learning)
First exam	0	**0**	%20	0
Second / midterm exam	%30	**%30**	%20	30%
Participation / practical applications	0	**0**	10	30%
Asynchronous interactive activities	%30	**%30**	0	0
final exam	%40	**%40**	%50	40%

Note: Asynchronous interactive activities are activities, tasks, projects, assignments, research, studies, projects, work within student groups ... etc, which the student carries out on his own, through the virtual platform without a direct encounter with the subject teacher.

Schedule of simultaneous / face-to-face encounters and their topics

Week	Subject	learning style*	Reference **
1	Introduction to Authentication	Lecture, Activity, Group work, Searching, Practical Implementation	TB ch12, ref01
2	Types of Authentication Credentials Authentication strength	Lecture, Activity, Group work, Searching, Practical Implementation	TB ch12, ref01
3	Something You Know: Passwords One-time passwords, and Knowledge-based authentication	Lecture	TB ch12, ref01
4	Password attack techniques Dictionary attack, Brute force attack, Rainbow table attack,	Lecture	TB ch12, ref01
5	Multifactor authentication Something You Have: Smartphone and Security Keys	Lecture	TB ch12, ref01
6	Something You Are: Biometrics Something You Do: Behavioral Biometrics	Lecture	TB ch12, ref01
7	Authentication Solutions Password Security salts and key stretching, Managing Passwords	Lecture, Activity, Group work, Searching, Practical Implementation	TB ch12, ref01
8	Secure Authentication Technologies Single Sign-On and federation	Lecture	TB ch12, ref01
9	Authentication Services RADIUS, or Remote Authentication Dial-In User Service, Terminal Access Control Access Control System1 (TACACS1) Kerberos authentication protocol	Lecture, Activity, Group work, Searching, Practical Implementation	TB ch12, ref01
10	review Midterm Exam	Problem solving	
11	Password storage techniques	Lecture, Activity, Group work, Searching, Practical Implementation	TB ch11, ref02
12	Applications of Cryptographic Hash Functions Message Authentication	Lecture	TB ch11, ref02
13	Digital Signatures Other Applications	Lecture, Activity, Group work, Searching, Practical	TB ch11, ref02

		Implementation	
14	Secure Hash Algorithm (SHA) SHA-512 Logic SHA-512 Round Function	Lecture, Practical implementation	TB ch11, ref02
15	Message Authentication Codes MAC		TB ch12, ref02
16	Final Exam		

*** Learning styles: Lecture, flipped learning, learning through projects, learning through problem solving, participatory learning ... etc.**
**** Reference: Pages in a book, database, recorded lecture, content on the e-learning platform, video, website ... etc.**

Schedule of asynchronous interactive activities (in the case of e-learning and blended learning)

Week	Task / activity	Reference	Expected results
During the semester	This activities was designed using the **Project-Based Learning (PBL)** approach to enhance students' understanding of **data integrity and authentication** through real-world applications.	**Useful Link** https://www.nist.gov/publications/guide-integrity-controls *NIST Guide on Data Integrity Controls*	Student groups prepare a **presentation** that explains how data integrity is maintained inside a real-time information system (example: university records system, hospital system, online banking, or e-commerce). The goal is to help students **visualize threats** to integrity and **propose controls** that preserve accuracy and consistency. Students explore concepts and technologies related to **IoT, Blockchain, and Cloud Computing**.
During the semester	Each project encourages problem-solving, collaboration, and critical thinking. Examples include *"IoT Device Authentication Using Lightweight Cryptography," "Blockchain for Data Integrity,"* and *"Zero-Trust Authentication in Cloud Systems."*	**Useful Link** https://auth0.com/learn/authentication *Auth0 Guide to Authentication and Security*	Students work in groups to create a **presentation** describing a secure authentication process for a hypothetical mobile app (e.g., health app, student portal, online shopping). The goal is to explain **how users are authenticated** and **what methods protect the login process**
2	Activity 1: Research and summarize types of authentication credentials	Supporting material	Understand different authentication types and their applications.

3	Activity 2: Analyze a case study on password attack techniques.	Supporting material	Identify common attack methods and propose defensive strategies.
7	Activity 3: Create a short presentation on password security and management.	Supporting material	Demonstrate knowledge of secure password storage techniques.
9	Activity 4: Compare different authentication services like Kerberos and RADIUS.	Supporting material	Evaluate authentication protocols and their use cases.
11	Activity 5: Apply cryptographic hash functions to store passwords securely.	Supporting material	Implement secure storage techniques using hashing and salting.
13	Activity 6: Develop a simple implementation of a digital signature in Python.	Supporting material	Show practical understanding of digital signatures and their role in ensuring data integrity.