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

Study plan No.	**2024/2025**		**University Specialization**		**Cybersecurity**		
Course No.	0133326		**Course name**		Secure Communication Protocols		
Credit Hours	**3**		**Prerequisite Co-requisite**		Network Security		
Course type	☐ MANDATORY UNIVERSITY REQUIREMENT	☐ UNIVERSITY ELECTIVE REQUIREMENTS	☐ FACULTY MANDATORY REQUIREMENT	☐ Support course family requirements	☐ ✓ **Mandatory requirements**	☐ Elective requirements	
Teaching style	☐ **Full online learning**		☐ Blended learning		☐ ✓ Traditional learning		
Teaching model	☐ 2Synchronous: 1asynchronous		☐ 2 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. Ahmad Alshanty	**assistant professor**	**226**		**a.alshanty@zuj.edu.jo**	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**

Brief description

In the rapidly evolving of digital communication, the need for robust and reliable security measures has become paramount. The Secure Communication Protocols course provides a comprehensive exploration of contemporary security protocols, their inherent properties, and their practical application. This course covers a wide spectrum of essential topics about the theoretical foundations and practical implementation of secure communication protocols. In addition, the knowledge and skills necessary to design, evaluate, and implement secure communication solutions, contributing to the protection of sensitive data and the integrity of digital interactions.

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	**Orzach, Y., & Khanna, D. (2022). *Network Protocols for Security Professionals: Probe and identify network-based vulnerabilities and safeguard against network protocol breaches*. Packt Publishing Ltd.**			
Supportive learning resources (Books, databases, periodicals, software, applications, others)	***1. Cryptography and network security principles and practice, William Stallings, 8 edition, Pearson (June 6, 2022)*** ***2. Design and Analysis of Security Protocol for Communication. Goyal, Dinesh, et al., eds. John Wiley & Sons, 2020.*** ***3. Network security essentials: applications and standards. Stallings, William. USA: Pearson, 2017.*** ***4. Internet Security Protocols: Protecting IP Traffic 1st Edition, Prentice Hall; 1st edition (July 24, 2000)***			
Supporting websites	https://www.catonetworks.com/network-security/network-security-protocols/			
The physical environment	☐ **Class**	☐ ✓ labs	☐ **Virtual**	☐ Others

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

for teaching	**room**		**educational platform**	
Necessary equipment and software	**Cisco Packet tracer, Wireshark**			
Supporting people with special needs				
For technical support	**E-learning and Open Educational Center. Computer Center**			

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

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	Learn about famous (SCPs) and The OSI Security Architecture	**3**
K2	Explain Information Security Protocols.	**1**
K3	Identify the fundamental strategies of developing and tracing information Security protocols.	**3**
	Skills	
S1	Explore the functionality of Information security Protocols components, Architecture, and the interaction between them.	**6**
	Competences	
C1	Analyze the Information security Protocols challenges and proposed solutions.	**11**
C2	Design and implement information Security protocols.	**12**

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**	0	0
Second / midterm exam	%30	**%30**	%30	%30
Participation / practical applications	0	**0**	0	0
Asynchronous interactive activities	%30	**%30**	%30	%30
final exam	%40	**%40**	%40	%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	Recap (Network 2) and introduce the concept of protocol	Face to Face	Cryptography and network security principles and practice, William Stallings,

			8 edition, Pearson (June 6, 2022)
2	History and Generations of Security Protocols (The OSI Security Architecture: •Security attack: Passive, Active. •Security mechanism: •Security service: CIA, Access control, non-repudiation •Definition of Ports	Face to Face	Cryptography and network security principles and practice, William Stallings, 8 edition, Pearson (June 6, 2022)
3	Security Protocols in the Application Layer	Face to Face	Design and Analysis of Security Protocol for Communication. Goyal, Dinesh, et al., eds. John Wiley & Sons, 2020.
4	HTTPS and its differences from HTTP	Face to Face	Orzach, Y., & Khanna, D. (2022). Network Protocols for Security Professionals: Probe and identify network-based vulnerabilities and safeguard against network protocol breaches. Packt Publishing Ltd.
5	Security protocols for Emails (PGP)	Face to Face	Orzach, Y., & Khanna, D. (2022). Network Protocols for Security Professionals: Probe and identify network-based vulnerabilities and safeguard against network protocol breaches. Packt Publishing Ltd.
6	Security Protocols in Transport Layer	Face to Face	Orzach, Y., & Khanna, D. (2022). Network Protocols for Security Professionals: Probe and identify network-based vulnerabilities and safeguard against network protocol breaches. Packt Publishing Ltd.
7	Socket secure layer/ Transport layer security SSL/TLS	Face to Face	Orzach, Y., & Khanna, D. (2022). Network Protocols for Security Professionals: Probe and identify network-based vulnerabilities and safeguard against network protocol breaches. Packt Publishing Ltd.
8	Midterm Exam		
9	Implementation of SSL/TLS (SSL-TLS Prevention Vulnerabilities)	Face to Face	Orzach, Y., & Khanna, D. (2022). Network Protocols for Security Professionals: Probe and identify network-based vulnerabilities and safeguard against network

			protocol breaches. Packt Publishing Ltd.
10	Attacks on TLS: Downgrade Attacks, Certificate Forgery, Implications of Stolen Root Certificates, Certificate Transparency	Face to Face	Orzach, Y., & Khanna, D. (2022). Network Protocols for Security Professionals: Probe and identify network-based vulnerabilities and safeguard against network protocol breaches. Packt Publishing Ltd.
11	Security Protocols in Internet/Network Layer: Recap IP IPsec Comparison between IP and IPsec	Face to Face	Orzach, Y., & Khanna, D. (2022). Network Protocols for Security Professionals: Probe and identify network-based vulnerabilities and safeguard against network protocol breaches. Packt Publishing Ltd.
12	Security Protocols in Internet/Network Layer: Virtual Private Network (VPN) configuration	Face to Face	Orzach, Y., & Khanna, D. (2022). Network Protocols for Security Professionals: Probe and identify network-based vulnerabilities and safeguard against network protocol breaches. Packt Publishing Ltd.
13	Security Protocols in Data Link Layer: L2TP, PPP	Face to Face	Orzach, Y., & Khanna, D. (2022). Network Protocols for Security Professionals: Probe and identify network-based vulnerabilities and safeguard against network protocol breaches. Packt Publishing Ltd.
14	Security Protocols in Data Link Layer: RADIUS	Face to Face	Orzach, Y., & Khanna, D. (2022). Network Protocols for Security Professionals: Probe and identify network-based vulnerabilities and safeguard against network protocol breaches. Packt Publishing Ltd.
15	Cisco Packet Tracer: application layer's protocols configuration and analysis, VPN configuration	Face to Face	Packet Tracer and Alternative Lab Solutions
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)

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

Week	Task / activity	Reference	Expected results
1	Applications protocols implementations/ Exploring the implementation and configuration of the most popular application protocols HTTP, DHCP and DNS by using packet tracer.	Cisco IOS LISP Application Note Series: Lab Testing Guide Version 3.0 -2022	understanding the implementation and configuration of three application protocols HTTP, DHCP and DNS
2	Virtual Private Networks (VPNs)/ providing security to shared public networks such as the Internet.	Cisco Secure Firewall Management Center Device Configuration Guide, 7.4 Chapter Title Remote Access VPN	explain the effect of the configured VPN, on the network traffic and reflect this on the concept of ipSec protocols
3	Capture Network Traffic with Wireshark /examine the incoming and outgoing traffic using Wireshark	Cisco lab guide 7.4 Chapter Title Capture Network Traffic with Wireshark	detailed view of all incoming and outgoing network packets, showing communication between devices, protocols used, and any unusual or suspicious traffic patterns for analysis of network performance and security.
4			
5			
6			
7			
8			