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

Study plan No.	**2022-2023**		**University Specialization**		**Cyber Security**		
Course No.	**0125347**		**Course name**		**Secure Communication Protocols (SCP)**		
Credit Hours	**3**		**Prerequisite Co-requisite**		**Computer networks(2)**		
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**		✓**2 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. Manal Abd aljabbar Mizher	**Assistant Prof.**	**118**		**m.mizher@zuj.edu.jo**	
Division number	**Time**	**Place**	**Number of students**	**Teaching style**	**Approved model**
1	**12.30:2 Sun Tue**	**9250**		**Traditional**	

Brief description

1) SCP is: A communication protocol that provides the appropriate **confidentiality**, **authentication**, **non-repudiation, access control,** and **content-integrity protection (***between communication sides***).**
2) The OSI Security Architecture (ITU-T X.800).
3) This course aims to give an introduction of secure communication protocols. By completing this course, students should be able to:
   - Practice secure communication protocols (e.g. HTTPS, SSH, SSL/TLS, IPsec, VPN, L2TP, PPP and RADIUS protocols).
   - Illustrate common attacks on various communication protocols and how to protect against them.

Learning resources

Course book information (Title, author, date of issue, publisher ... etc)	1. Cryptography and network security principles and practice, William Stallings, 8 edition, 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.
Supportive learning resources	1. CCNA Security 210-260 Certification Guide: Build your knowledge of network security and pass your CCNA Security exam (210-260)

(Books, databases, periodicals, software, applications, others)				
Supporting websites				
The physical environment for teaching	☐ Classroom	✓ labs	☐ Virtual educational platform	☐ Others
Necessary equipment and software				
Supporting people with special needs				
For technical support	**E-learning and Open Educational Center. Computer Center**			

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

No.	Course learning outcomes	The associated program learning output code
	Knowledge	
K1	Understand the fundamentals of secure protocols (SCPs)	
K2	Learn about famous (SCPs) and The OSI Security Architecture	
K3	Understand the differences between SCPs depending on the kinds of network types	
	Skills	
S1	Using Cisco Packet Tracer	
S2	Programming SCP using Python libraries and additional tools like OpenSSL etc.	
	Competencies	
C1	Awareness and realization about the robustness of networks that used SCPs, and the different possible attacks on SCP.	

Mechanisms for direct evaluation of learning outcomes

Type of assessment/learning	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%
Home works and quizzes	%30	**%20**	0	0
final exam	%40	**%50**	%50	40%

Note: Asynchronous interactive activities are activities, tasks, projects, assignments, research, studies, projects, and 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.

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

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

Week	Subject	learning style*	Reference **
1	- Recap (Network 2) - Introduction to SCP	**Lecture**	
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	**Lecture**	
3	Security Protocols in the **Application Layer:** - HTTP and its implementation in Python	**Lecture + Lab**	
4	- HTTPS and its differences from HTTP - HTTPS implementation in Python	**Lecture + Lab**	
5	- Cisco Packet Tracer	**Lab**	
6	- Telnet and SSH - SSH implementation	**Lecture + Lab**	
7	Security Protocols in **Transport Layer:** SSL/TLS	**Lecture + Lab**	
8	Implementation of SSL/TLS		
9	- Attacks on TLS: Downgrade Attacks, Certificate Forgery, Implications of Stolen Root Certificates, Certificate Transparency - SSL-TLS Prevention Vulnerabilities	**Lecture**	
10	Security Protocols in **Internet/Network Layer:** - Recap IP - IPsec - Comparison between IP and IPsec	**Lecture + Lab**	
11	Security Protocols in **Internet/Network Layer:** - VPN	**Lecture + Lab**	
12	Security Protocols in **Data Link Layer:** L2TP, PPP	**Lecture + Lab**	
13	Security Protocols in **Data Link Layer:** RADIUS	**Lecture + Lab**	
14	**Privacy-Preserving Protocols:**	**Lecture + Lab**	

	Mixnet, Tor		
15	Introduce security Protocols for: - **Multimedia Streaming** - **Mobile Communications** - **5G networks and IoT** - **Cloud** - **Wi-Fi**	**Students presentations**	
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.**