Course Specification

(Postgraduate Programs)

Course Title:	Networks Security Engineering
Course Code:	CE6029
Program:	Master of Science in Computer Engineering
Department:	Computer and Network Engineering
College:	College of Computer
Institution:	Umm Al-Qura University
Version:	2.0
Last Revision Date:	12/4/2025

Table of Contents

A. General information about the course:

1. Course Identification:

1. Credit hours: (3)				
2. Course type				
A.	☐University	☐College	☒ Department	☐ Track
B.	☒ Required		☐Elective	
3. Level/year at which this course is offered: (Level 2)				
4. Course General Description:				
This course provides an in-depth exploration of key concepts in networks security engineering, beginning with an introduction to security services, mechanisms, and attacks on network protocols. Students will study Symmetric and Asymmetric Cryptography, Cryptographic Hash Functions, and Authentication Protocols, along with their vulnerabilities. Key management techniques, including KDC and Kerberos, will be examined alongside essential standards such as TLS, IPsec, IKE, and PKI. Practical applications in Network Security Engineering will cover the implementation of Firewalls, Intrusion Detection Systems (IDS), VPNs, and DMZs, as well as Wireless Network Security. Students will gain the knowledge and skills necessary to design and maintain secure networks effectively.				
5. Pre-requirements for this course (if any)**:**				
Non				
6. Co-requisites for this course (if any)**:**				
Non				
7. Course Main Objective(s):				
The main objective of this course is to offer a comprehensive understanding of key issues related to network security and to equip students with th necessary practical skills to respond to security incidents.				

2. Teaching Mode: (mark all that apply)

No	Mode of Instruction	Contact Hours	Percentage
1	Traditional classroom	45	100
2	E-learning		
3	Hybrid • Traditional classroom		

No	Mode of Instruction	Contact Hours	Percentage
	• E-learning		
4	Distance learning		

3. Contact Hours: (based on the academic semester)

No	Activity	Contact Hours
1.	**Lectures**	35
2.	**Laboratory/Studio**	
3.	**Field**	
4.	**Tutorial**	
5.	**Others (specify) - Seminar**	10
	Total	45

B. Course Learning Outcomes (CLOs), Teaching Strategies and Assessment Methods:

Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
1.0	**Knowledge and understanding**			
1.1	Identify the security services and mechanisms for communication networks.	K1	Lectures, Problem solving, Case study	Exam, Quiz, Lab exercise
1.2	Recognize the cryptographic standards algorithms, techniques and protocols to secure networks.	K2		
2.0	**Skills**			
2.1	Design appropriate security architectural solutions according to the network security requirements and threats.	S1	problem-based learning, flipped classes, practical examples, open-ended, discussions, project	Practical exercises, hands-on mini porjects
2.2	Apply security models and cryptographic algorithm to to protect a given network.	S2		
2.3	Communicate effectively through a written report embodying the design,	S3		

Code	Course Learning Outcomes	Code of PLOs aligned with the program	Teaching Strategies	Assessment Methods
	implementation, evaluation of a project in network security			
3.0	**Values, autonomy, and responsibility**			
3.1	Recognize professional responsibilities and function effectively as a member or leader of a team through a project	V1 and V2	Group project and discussion sessions	Written assignments, oral presentations, and design projects. Verbal cross-questioning

C. Course Content:

No	List of Topics	Contact Hours
1	Introduction to network security (security services, mechanisms and attacks on network protocols)	6
2	Symmetric Cryptography and Asymmetric Cryptography	6
3	Cryptographic Hash functions	3
4	Authentications and Cryptographic protocols and their pitfalls	6
5	Key management and distribution (KDC and Kerberos)	6
6	Ceritifiate, TLS, IPsec, IKE and PKI	6
7	Network security engineering : Firewall, IDS, VPN and DMZ	6
8	Wireless network security	6
Total		**45**

D. Students Assessment Activities:

No	Assessment Activities *	Assessment timing (in week no)	Percentage of Total Assessment Score
1.	Midterm	8	20
2.	Final Exam	-	30
3.	Quizes and Assignments	10	20
4.	Projects	14	30

*Assessment Activities (i.e., Written test, oral test, oral presentation, group project, essay, etc.)

E. Learning Resources and Facilities:

1. References and Learning Resources:

Essential References	Network Security: Private Communication in a Public World by Charlie Kaufman, Radia Perlman, Mike Speciner, and Ray Perlner, 3nd Edition, Addison-Wesley Professional, 2022, ISBN-10: 0136643604, ISBN-13: 978-0136643609
Supportive References	Cryptography and Network Security: Principles and Practice, 7th Edition By William Stallings, Pearson, 2016, SBN-10: 0134444280, ISBN-13: 978-0134444284
Electronic Materials	The instructor may provide as per requirements.
Other Learning Materials	The instructor may provide as per requirements.

2. Educational and Research Facilities and Equipment Required:

Items	Resources
Facilities (Classrooms, laboratories, exhibition rooms, simulation rooms, etc.)	Classrooms
Technology equipment (Projector, smart board, software)	Projector
Other equipment (Depending on the nature of the specialty)	The instructor may provide as per requirements.

F. Assessment of Course Quality:

Assessment Areas/Issues	Assessor	Assessment Methods
Effectiveness of teaching	Students, Program Leaders	Indirect
Effectiveness of students' assessment	Program Leaders	Direct
Quality of learning resources	Students, Faculty	Indirect
The extent to which CLOs have been achieved	Students, Faculty, Program Leaders	Direct and Indirect
Other		

Assessor (Students, Faculty, Program Leaders, Peer Reviewer, Others (specify)

Assessment Methods (Direct, Indirect)

G. Specification Approval Data:

COUNCIL /COMMITTEE	Computer and Network Engineering Department Council
REFERENCE NO.	The 18th Session Of The Academic Year 1446
DATE	15/4/2025