الجامعة الأهلية
AHLIA UNIVERSITY
BAHRAIN

COLLEGE OF ENGINEERING
DEPARTMENT OF TELECOMMUNICATION ENGINEERING
COURSE SYLLABUS/ SPECIFICATION

Course Code and title	**ECTE 537: Network Security**
Weight:	**(3 - 0 - 3)**
Prerequisite:	**None**
NQF Level Allocated	**9** **NQF Notional Hours / Credits: 120/12**
Description:	This course covers advanced topics in IT security spanning Network security including: Security at the Application Layer, Security at the Transport Layer, Security at the Network Layer, and general aspects in Mobile ad-hoc networks security.
Objectives:	1. To provide student with an overview of modern symmetric and asymmetric cryptosystems. 2. To explore advanced techniques in cryptographic data integrity and mutual trust. 3. To discuss various approaches in network and internet security in detail

SEMESTER:	Second	**ACADEMIC YEAR:**	2019-2020
INSTRUCTOR:	Dr. Ammar Sami Al-Dallal		
OFFICE TEL.:	17298999 Ext. 8914		
EMAIL:	aaldallal@ahlia.edu.bh		

Intended Learning Outcomes (ILOs)

A. Knowledge and Understanding		**NQF Descriptor/ Level**
A1	Concepts and Theories: Demonstrate knowledge and understanding of concepts and theories related to network security, encipherment, and mutual trust.	**Knowledge**: Theoretical understanding [Level 9]
A2	Contemporary Trends, Problems and Research: Demonstrate an informed and critical awareness of network security problems, research issues and technological advancements.	**Knowledge**: Theoretical Understanding [Level 9]
A3	Professional Responsibility: Demonstrate cognizance of and adhere to the professional and legal standards as a network user/consumer.	**Knowledge**: Theoretical Understanding. [Level 9]

B. Subject-Specific Skills	**NQF Descriptor/ Level**

B1	Problem Solving: Identify and evaluate network security problems; plan, design, and implement appropriate solutions related to encipherment, mutual trust, and corresponding implementation layer.	**Knowledge**: Practical application [Level 9]
B2	Modeling and Design: Model and design security system/component in order to illustrate one or combination of the following concepts: encipherment, data integrity, mutual trust, and internet security.	**Skills**: Generic problem solving & Analytical Skills [Level 9] **Knowledge**: Practical application [Level 9]
B3	Application of Methods and Tools: Use effectively one of the available simulation software (MATLAB, Sage, OPNET, or Cisco Packet Tracer) to implement various methods and tools related to encipherment, mutual trust, and network security such as AES, ECB, CFM, CBC, OFM, key distribution techniques, and user authentication.	**Skills**: Communication, ICT and Numeracy [Level 9]

C. Thinking Skills		**NQF Descriptor/ Level**
C1	Analytic: Evaluate the benefits, complexity, and challenges of the discussed methods and tools related to encipherment, mutual trust, and network security.	**Skills**: Generic problem solving & Analytical Skills [Level 9]
C2	**Synthetic**: ***Identify*** and integrate a range of security solutions to address computer security threats.	**Skills**: Generic problem solving & Analytical Skills [Level 9]

D. General and Transferable Skills (Other Skills Relevant to Employability and Personal Development)		**NQF Descriptor/ Level**
D1	Communication: Express and communicate ideas cogently, persuasively and effectively, in written and oral form, to a diverse range of audiences and stakeholders through written test, final examination, group assignment, and research project.	**Skills**: Communication, ICT and Numeracy [Level 9]
D2	Teamwork and Leadership: Work effectively as a member/leader of a team of technical people who may plan, design, implement, manage, monitor and evaluate a security system/protocol.	**Competence**: Autonomy, Responsibility and Context [Level 9]
D4	Ethical and Social Responsibility: Demonstrate awareness of, and adhere to, ethical and societal responsibilities in the area of network security.	Context [Level 9] **Knowledge**: Theoretical understanding [Level 9]

Course Structure (Outline)

Week	Hours		ILOs	Topics	Teaching Method	Assessment Method
	Lec.	Lab				
1	3	0	A1,A3,D4	**General Introduction:** Security Attacks, Services, Mechanisms	Lecture	-
2	3	0	A1,A3, B1, C1,D2	**Overview of symmetric ciphers:** Traditional, DES, and AES	Lecture, Group Discussion	Test1 (week 6)/ Exercise 1* Oral Participation*

3	3	0	A1,A3, B1, C1,D2	**Overview of asymmetric ciphers:** Public-Key Cryptosystems and RSA	Lecture, Group Discussion	Test1 (week 6) / Exercise2*
4	3	0	A1,A3,C1, D4	**Block Cipher Operation:** ECB, CFM, OFM, CM, and XTS-AES Mode	Lecture	Test1 (week 6) / Exercise 3*
5	3	0	A1,A3,C1, D4	**Cryptographic data integrity:** Hash Function, MAC, Digital Signatures	Lecture	Test1
6	3	0	A1,B1,B2, B3,D1,D2	**Tutorial Session:** Problem Solving and Software Demonstration	Tutorial/ software demo/Group Discussion	Test2 (week 12)/Quiz 2
7	3	0	A1,A3,B1, C1,D1,D4	**Mutual Trust:** Key Management and User Authentication	Lecture	Group project Oral Participation* / Test2 (week 12)
8	3	0	A1,A2,A3, C1,D4	**Network and Internet Security:** Network Access Control, Cloud Security Risks and Countermeasures, Cloud security as a Service	Lecture	Test2 (week 12) Exercise 4*
9	3	0	A1,A2,A3, C1,D4	**Network and Internet Security:** Web Security Consideration, Secure Sockets Layer, Transport Layer Security, HTTPS, SSH	Lecture	Test2 (week 12)/ Final Written Exam (week 16) Exercise 5*
10	3	0	A1,B1,B2, B3,D1,D2	**Tutorial Session:** Problem Solving and Software Demonstration	Tutorial/ software demo/Group Discussion	Test2/ Final Written Exam (week 16)
11	3	0	A1,A2,A3, B1,C1,D4	**Network and Internet Security:** Wireless Security, Mobile Device Security, IEEE 802.11i	Lecture, Group Discussion	Final Written Exam (week 16) Quiz 3
12	3	0	A1,A2,A3, B1,C1,D4	**Network and Internet Security:** Pretty Good Privacy, S/MIME, Domain Keys Identified Mail	Lecture, Group Discussion	Final Written Exam (week 16)
13	3	0	A1,A2,A3, B1,C1,D4	**Network and Internet Security:** IP Security overview and Policy, Encapsulating Security Payload	Lecture, Group Discussion	Final Written Exam (week 16)
14	3	0	A1,A2,A3, B1,C1,D4	**Network and Internet Security:** Combining Security Associations	Lecture, Group Discussion	Final Written Exam (week 16)
15	3	0	A1, A2, C1, D1,D2, D4	**Research Assignment Presentation**	Group Discussion	**Research assignment**
16	2					**Final Exam** A1,B1,C1

TEACHING MATERIALS:

TEXTBOOK(S):	W. Stallings, "Cryptography and Network Security: Principles & Practice", 7th edition, Pearson, 2017.
HANDOUT(S):	Material provided in eLearning (Moodle)

REFERENCE(S):	Books: 1. "Applied Cryptography and Network Security", 17th International Conference, ACNS 2019, Bogota, Colombia, June 5–7, 2019, Proceedings, Editors: Deng, R.H., Gauthier, V., Ochoa, M., Yung, M. (Eds.) 2. (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide 8th Edition, Kindle Edition, by Mike Chapple (Author), James Michael Stewart (Author), Darril Gibson (Author), 2018. 3. Articles/Research papers: 4. Ammar Aldallal, "Exploring DOM-Based Cross-Site Scripting", International Conference on Recent Advances in Engineering and Technology (ICRAET), Berlin, Germany, 3-4 Oct. 2017, pp.1-4. 5. Ammar Aldallal and Kashif Shabbir, "Protecting Web Applications from Cross-Site Scripting Attacks", Journal of Applied Engineering Research, volume 2017, issue 3, July – August, pp.1-21 6. Zargar, S., Joshi, J., and Tipper, D.; "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", Communications Surveys & Tutorials, IEEE, Volume: PP , Issue: 99, pp. 1 - 24, 2013. 7. M. A. Ambusaidi, X. He, P. Nanda and Z. Tan, "Building an Intrusion Detection System Using a Filter-Based Feature Selection Algorithm," in IEEE Transactions on Computers, vol. 65, no. 10, pp. 2986-2998, 1 Oct. 2016.

Assessment:

Type of Assessment		Description	Learning Outcomes	Weighting
Test		The test is one-hour Test covering topics discussed in first 7 weeks.	A1,B1,C1	25%
Research Assignment: Oral Presentation: Report:		"Each group of two students has to select a topic related to one of the specified network security to write a report, present, and discuss it in the class."	A1,A2,C1, D1,D2, D4	 5% 15%
Best 3 of 4 assignments	**Group Assignment 1**	"The class will be divided into groups, each group has to implement/simulate specific symmetric cryptographic algorithm."	B2,B3,C2, D1,D2	15%
	Group Assignment 2	"The class will be divided into groups, each group has to implement/simulate specific asymmetric cryptographic algorithm."	B2,B3,D1,D2	
	Group Assignment 3	"The class will be divided into groups, each group has to implement/simulate hash function"	B2,C2,D1,D2	
	Group	"The class will be divided into groups,	B2,C2,D1,D2	

	Assignment 4	each group has to implement/simulate specific mutual trust / network access control."		
Final Exam:		"Two-hour Final Exam consisting of essay questions. The exam will cover all the topics in the course syllabus".	A1,B1,C1	40%
			Overall:	**100%**

Admissions	
Pre-requisites	None
Minimum number of students	**5**
Maximum number of students	**20**