College of Engineering

Department of Computer Engineering

Course Syllabus/Specification

Course Code and title	**ECCE 501: Introduction to Information Security**
Weight:	**(3 - 0 - 3)**
Prerequisite:	**None**
NQF Level Allocated	**8** **NQF Notional Hours / Credits: 120/12**
Description:	This course will cover the most important features of computer security, including topics such as cryptography, software security, malicious software, and network security. After completing this course, students will be able to analyze, design, and build secure systems of moderate complexity.
Objectives:	The objectives of the course are to : 1. Overview various computer security threats and countermeasures to that threats. 2. Gain understanding of software and operating system security. 3. Implement symmetric-key (shared secret key) and asymmetric-key (public-private key) encryption. 4. Design and imply the concepts of Internet Security Protocols and Standards. 5. Write and formulate access control polices of users for a given system. 6. Perform IT Security management and risk assessment 7. Formulate a computer and network security strategy.

SEMESTER:	First	**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 a critical knowledge and understanding of properties, techniques, concepts, principles and theories relating to security services	**Knowledge**: Theoretical understanding [Level 9]
A2	**Contemporary Trends, Problems and Research**: Gain a ***critical*** understanding of research methods/investigation techniques to shed light of current threats and countermeasures with respect to computer security	**Knowledge**: Theoretical Understanding [Level 9]
A3	**Professional Responsibility**: understand *detailed knowledge* of the role cryptography as a tool for deploying security software"	**Knowledge**: Theoretical Understanding. [Level 9]

B. Subject-Specific Skills		NQF Descriptor/ Level
B1	**Problem Solving**: Perform ***advanced*** calculations with respect to computer security	**Knowledge**: Practical application [Level 9]
B2	**Modeling and Design**: ***Demonstrate creativity and*** design a computer based security system to address a range of security problems (software, operating system and networks)	**Skills**: Generic problem solving & Analytical Skills [Level 9] **Knowledge**: Practical application [Level 9]
B3	**Application of Methods and Tools**: apply ***advanced*** security tools and techniques to encrypt/decrypt messages with a focus on cryptographic algorithms such as DES, AES and RSA"	**Skills**: Communication, ICT and Numeracy [Level 9]

C. Thinking Skills		NQF Descriptor/ Level
C1	**Analytic**: ***Critically*** analyze the scale of threats with respect to software, operating system and networks to evaluate the effectiveness of countermeasures.	**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 effectively with persons and specialists and be able to make formal presentation in the area of computer security.	**Skills**: Communication, ICT and Numeracy [Level 9]
D2	**Teamwork and Leadership**: Work effectively as a member of a project team and demonstrate understanding of individual responsibility within the team	**Competence**: Autonomy, Responsibility and Context [Level 9]
D4	Ethical and Social Responsibility: Emphasis on personal and organizational ethics and accept accountability for conducting independent learning according to ethical and social norms in the field of computer 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	-
3	3	0	A1,A3, B1, C1,D2	**Overview of asymmetric ciphers:** Public-Key Cryptosystems and RSA	Lecture, Group Discussion	-
4	3	0	A1,A3,C1, D4	**Block Cipher Operation:** ECB, CFM, OFM, CM, and XTS-AES Mode	Lecture	-
5	3	0	A1,A3,C1, D4	**Cryptographic data integrity:** Hash Function, MAC, Digital Signatures	Lecture	**Assignment 1**
6	3	0	A1,B1,B2, B3,D1,D2	**Tutorial Session:** Problem Solving and Software Demonstration	Group Discussion	-
7	3	0	A1,A3,B1, C1,D1,D4	**Mutual Trust:** Key Management and User Authentication	Lecture	**Test1** A1, B1, C1
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	-
9	3	0	A1,A2,A3, C1,D4	**Network and Internet Security:** Web Security Consideration, Secure Sockets Layer, Transport Layer Security, HTTPS, SSH	Lecture	-
10	3	0	A1,B1,B2, B3,D1,D2	**Tutorial Session:** Problem Solving and Software Demonstration	Group Discussion	-

11	3	0	A1,A2,A3, B1,C1,D4	**Network and Internet Security:** Wireless Security, Mobile Device Security, IEEE 802.11i	Lecture, Group Discussion	-
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	-
13	3	0	A1,A2,A3, B1,C1,D4	**Network and Internet Security:** IP Security overview and Policy, Encapsulating Security Payload, Combining Security Associations	Lecture, Group Discussion	**Test 2** A1, B1, C1
14, 15	3	0	A2,A3,D1, D2, D4	**Research Assignment Presentation**	Group Discussion	**Research assignment** A2,A3,D1, D2, D4
16			A1,B1,C1, C2	**Final Examinations**		**Written Exam** A1,B1,C1, C2

TEACHING MATERIALS:

TEXTBOOK(S):	William Stalling & Laurie Brown 'Computer Security Principles and Practices' , 4rd Edition, Pearson, 2018
HANDOUT(S):	Material provided in eLearning (Moodle)
REFERENCE(S):	Texts: . Stallings, "Cryptography and Network Security: Principles & Practice", 8th edition, Pearson, 2019. Behrouz A. Forouzan 'Cryptography and Network Security' McGraw-Hill International Edition, 2008. Articles/Research papers: 1. Ammar Aldallal, "Exploring DOM-Based Cross-Site Scripting", International Conference on Recent Advancess in Engineering and Technology (ICRAET), Berlin, Germany, 3-4 Oct. 2017, pp.1-4. 2. 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 3. 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. 4. 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. 5. Larry Greenemeier, 'Fact or Fiction: Encryption Prevents Digital Eavesdropping' , Scientific Americain,July 15, 2013

	http://www.scientificamerican.com/article.cfm?id=fact-fiction-encryption-prevents-digital-eavesdropping 6. G. Richard Newell and Tim Morin, 'The Right and Wrong Way to Implement Cryptographic Algorithms in Embedded Electronic Systems' , EDN Network, March 2013, http://www.edn.com/design/systems-design/4410267

Assessment:

Method of Assessment	Description	Learning Outcomes	Weighting
Test (2)	Two tests of one hour each covering topics discussed in class up to week (6) & week (12). First test is worth 20% and the second 15%.	A1, B1, C1	35%
Programming Project (Assignment 1)	The first project is individual where each student has to implement/apply a security system from those discussed in the class.	A1, A2, B1,B2, B3, D1	10%
Research Assignment	The second project is a group project where each group has to write a research project about one of the security topics covered in class Students may use the articles from the reference list as references for their project)	A2,A3,D1, D2,D4	15%
Final Exam:	A two-hour final exam consisting of problem solving and essay questions. The exam covers all the topics in the course syllabus.	A1, B1, C1, C2	40%
Exercises	Selective practice questions from the textbook	B1	*Formative Assessment
Oral Participation	Questions and discussion during the lecture	A1, D1	*Formative Assessment
Overall:			**100%**

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