Detailed Course Description - Course Plan Development and Updating Procedures/ Computer Information Systems Department	QF01/0408-3.0E

Faculty	Faculty of Science and Information Technology	Department	Computer Information Systems
Course Number	**0113353**	Course Title	**Information Security**
Number of Credit Hours	3	Pre-Requisite/Co-Requisite	Algorithms

Brief Course Description
Introduction to information security and its importance, threats and vulnerabilities of computing system, understanding of classical encryption techniques: Substitution, Transposition and Product Ciphers. Examination of conventional encryption algorithms and design principles including transposition and substitution techniques such as DES. Understanding of the modern cryptographic techniques such as RSA, Key distribution, digital signature, identification and authentication, and sharing keys. Provide basic understanding of attack types, Network security Access control methods, Firewalls, Malware, and Digital watermarking/Steganography.

	Course Goals and Learning Outcomes
Goal 1	**Understanding the basic principles for information and communication security, and be able to apply these principles to evaluate and criticize information system security properties.**
Learning Outcomes	**1.1** Cite the need for information security. **1.2** Provide basic understanding of security threats and vulnerabilities of computing system. **1.3** List and briefly describe security risks and mitigation strategies for an organization that is about to connect its network to the Internet and communicate with other companies via email. **1.4** Be able to identify the vulnerability of the Internet systems and recognize the mechanisms of the attacks, and apply them to design and evaluate counter-measure tools.
Goal 2	**Understanding the classical encryption techniques**
Learning Outcomes	**2.1** Provide basic understanding of classical encryption Techniques: Substitution, Transposition and product Ciphers. **2.2** Examine of conventional encryption algorithms and design principles including transposition and substitution techniques such as DES. **2.3** account for the cryptographic theories, principles and techniques that are used to establish security properties, analyze and use methods for cryptography, reflect about limits and applicability of methods.
Goal 3	**Presenting an overview of the basic principles of public-key cryptosystems and its mathematical hard problems.**
Learning Outcomes	**3.1** Understand the mathematical hard problem based cryptography. **3.2** Provide basic understanding of the modern encryption technique such as DH, RSA, DSA, etc. **3.3** Develop efficient algorithms for manipulating encryption techniques such as (Key distribution, digital signature, identification and authentication, and secret

	sharing keys).
Goal 4	**Presenting an overview of the basic principles of Network And Internet Security**
Learning Outcomes	**4.1** Understand network access control **4.2** Understand cloud security risks and countermeasures **4.3** Provide basic understanding of Transport-Level Security **4.4** Understand IP Security Overview
Textbook	Cryptography and Network Security Principles and Practice, William Stallings, Sixth Edition, **2014**.
Supplementary References	**1.** An Introduction to Mathematical Cryptography. **2014-** 2nd Edition by Jeffrey Hoffstein, Jill Pipher, J.H. Silverman. **2.** The Art of Invisibility: The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data Hardcover – February 14, 2017, by Kevin Mitnick, Mikko Hypponen.

Course Timeline				
Week	**Number of Hours**	**Course Topics**	**Pages (Textbook)**	**Notes**
01	**1** **1** **1**	**Introduction:** – Computer Security Concepts – Security Cycle – Security Services – Security Mechanisms – A Model for Network Security	**9,14,15,17, 20, 22**	
02/03	**1** **1** **1** **1** **1**	**Classical Cryptography and Cryptanalysis:** – Substitution Cipher – Transposition Cipher – Product Cipher – Block Cipher: General View of DES Algorithm. – Stream cipher. **Assignment!**	**28-49** **61-78**	Added topics from Ref.
03/04	**1** **1** **1** **1**	**Public Key Cryptography:** – Public Key and Secret Key cryptosystems – Basic concepts in number theory and finite fields – Finding GCD, Exponentiations, Prime Numbers, Euler's Totient Function, Inverse.	**85-112**	Added topics from Ref.
05	**1** **1**	**Hash Functions:** – Secure Hash Algorithm (SHA)	**313-339**	
05/06	**1** **1**	**Mathematical Hard Problems Based Cryptography (Classifications)**	**287-292**	Added Topics

	1 1 1	**Public-key exchange (Key Management) :** – Diffie-Hellman Key Exchange – Elliptic curve Key Exchange **Assignment!**		and examples
07/08	1 1 1 1 1	**Public-Key Encryption:** – RSA Algorithm – Rabin Algorithm – ElGamal Algorithm	**253-264, 292-**	Added Topics and examples
08/09/10	1 1 1 1 1	**Digital Signature Algorithms:** – RSADS, Digital Signature Algorithm (DSA) – Combining Algorithms	**393-400**	Added Topics and examples
10/11	1 1 1	**System Access Control:** – Password Management, Password Protection **Data Access Control:** – DAC, MAC, RBAC		Added Topics and examples
11/12/13	1 1 1 1 1	**Network Access Control and Cloud Security:** – Network Access Control – Extensible Authentication Protocol – IEEE 802.1X Port-Based Network Access Control – Cloud Computing – Cloud Security Risks and Countermeasures – Data Protection in the Cloud – Cloud Security as a Service	**495-520**	
13	1 1	**Transport-Level Security**: – Web Security Considerations – Secure Sockets Layer	**522-525**	
14	1 1 1	**Malware and Social Engineering Attacks:** – Define malware – List the different types of malware – Identify payloads of malware – Describe the types of social engineering psychological attacks – Explain physical social engineering attacks Firewall		Articles and Ref.
15/16	1 1 1	**Steganography**	**52**	Articles and Ref.
16	1 1 1	**Reviewing and Assignments Discussions**		

Detailed Course Description - Course Plan Development and Updating Procedures/ Computer Information Systems Department	QF01/0408-3.0E

Theoretical Course Evaluation Methods and Weight	Participation = 10% First Exam 20% Second Exam 20% Final Exam 50%	**Practical (Clinical) Course Evaluation Methods**	Semester Students' Work = 50% (Reports, Research, Quizzes, Etc.) Final Exam = 50%

Approved by Head Of Department		**Date of Approval**	

Extra information (to be updated every semester by corresponding faculty member)

Name of Teacher		Office Number	
Phone Number (Extension)		Email	@zuj.edu.jo
Office Hours			