University/Academy: Arab Academy for Science and Technology & Maritime Transport
Faculty/Institute: College of Computing and Information Technology
Program: Computer Science

Form No. (12)
Course Specification

1- Course Data

Course Code:	Course Title:	Academic Year/Level:
CS421	Computer System Security	Year 4 / Semester 8
Specialization:	**No. of Instructional Units:** 2 hrs lecture 2 hrs lab	**Lecture:**

2- Course Aim	The course is an introduction to computer and network security. The course encompasses the study of security mechanisms for secrecy, integrity, and availability. Topics include basic cryptography and its applications, security in computer networks and distributed systems and control and prevention of viruses and other rogue programs. In addition, hands-on experience will be provided through a series of programming assignments.
3- Intended Learning Outcome:	
a- Knowledge and Understanding	**Students will be able to demonstrate knowledge of:** **K13.** Use high-level programming languages. **K15.** Interpret and analyzing data qualitatively and/or quantitatively. **K18**. Understand the fundamental topics in Computer Science, including hardware and software architectures, software engineering principles and methodologies, operating systems, compilers, parallel and distributed computing, systems and software tools. • Define security services, mechanisms and attacks. • Describe OSI security architecture. • Demonstrate the encryption model for the classical ciphers (Caesar – monoalphabetic – Playfair – Hill) • Know the encryption model for the polyalphabetic cipher. • Define the steganography process • Demonstrate the encryption model for the Fiestel cipher structure • Illustrate the block diagram for the DES round • Demonstrate Triple DES operation • Demonstrate operation of the different block cipher modes • Demonstrate the block diagram for AES • Define discrete logarithm • Define Fermat's theorem • Define Euler's Theorem • Define the principles of public-key cryptography • Demonstrate how RSA works • Demonstrate a key distribution scheme for symmetric encryption

	• Demonstrate the Diffie-Hellman key exchange algorithm • List the authentication requirements • Describe the authentication functions • Describe the message digest algorithm • Demonstrate the secure hash algorithm • Demonstrate Firewall Design Principles
b- Intellectual Skills	**By the end of the course, the student acquires high skills and an ability to understand:** **I10.** Define traditional and nontraditional problems, set goals towards solving them, and. observe results. **I11.** Perform comparisons between (algorithms, methods, techniques...etc). **I13.** Identify attributes, components, relationships, patterns, main ideas, and errors. **I18.** Solve computer science problems with pressing commercial or industrial constraints. • Differentiate between confidentiality and Integrity as security services • Distinguish between Symmetric ciphers and Asymmetric ciphers. • Apply classical encryption algorithms • Apply the polyalphabetic cipher on an example plaintext message • Analyze the security strengths for some classical encryption techniques • Apply a DES round on a block of bits • Analyze the Avalanche effect in DES • Recognize security problems with DES • Compare the different block cipher models. • Calculate discrete logarithm • Calculate Euler's totient function • calculate the public and private keys in the RSA algorithm • Analyze a key distribution scheme for symmetric encryption • Analyze a key distribution scheme for asymmetric encryption • Analyze Diffie-Hellman key exchange algorithm • Differentiate between a message authentication code and a hash value • Apply use of MAC and hash functions to provide message authentications • Distinguish between Hashing and Encryption • Identify security problems not handled by firewalls

c- Professional Skills	**By the end of the course the student will have the ability to:** **P11.** Perform independent information acquisition and management, using the scientific literature and Web sources. **P15.** Evaluate systems in terms of general quality attributes and possible tradeoffs presented within the given problem. **P18.** Identify any risks or safety aspects that may be involved in the operation of computing equipment within a given context. • Design and implement an application to calculate a ciphertext using classical encryption algorithms • Design and implement an application to demonstrate brute force attack on Caesar cipher • Design and implement an application to experiment with symmetric key encryption • Design and implement an application to experiment with block cipher modes of operation • Design and implement an application to experiment with public key cryptography • Design and implement an application to calculate the common session key using Diffie- Hellman key agreement protocol • Design and implement an application to experiment with MAC and hash algorithms

d- General Skills	**Students will be able to:** **G1.** Demonstrate the ability to make use of a range of learning resources and to manage one's own learning. **G3.** Show the use of information-retrieval. **G5.** Exhibit appropriate numeracy skills in understanding and presenting cases involving a quantitative dimension. **G8.** Demonstrate an appreciation of the need to continue professional development in recognition of the requirement for life-long learning.
4- Course Content	

1	Identify threats to computer systems
2	Outline security attacks and countermeasures
3	Master classical and modern encryption techniques
4	Experiment with authentication protocols
5	Outline application layer security (E-mail and Web Security)
6	Experiment with system security (Firewalls and Intrusion Detection)
7	Outline main components of a security policy

5- Teaching and Learning Methods	Lectures, Labs, Projects, Individual study & self-learning.
6- Teaching and Learning Methods for Students with Special Needs	• Students with special needs are requested to contact the college representative for special needs (currently Dr Hoda Mamdouh in room C504) • Consulting with lecturer during office hours. • Consulting with teaching assistant during office hours. • Private Sessions for redelivering the lecture contents. • For handicapped accessibility, please refer to program specification.
7- Student Assessment:	
a- Procedures used:	Exams and Group Projects
b- Schedule:	Week 7 exam Project Week 16Final exam
c- Weighing of Assessment:	7th week exam 20% 7th week lab quiz 10% Project 20% Lab work 10% Final exam 40%
8- List of References:	
a- Course Notes	From the Moodle on www.aast.edu

b- Required Books (Textbooks)	W. Stallings, *Cryptography and Network Security*.4th Edition, Prentice Hall, 2006.
c- Recommended Books	1. William Stallings, *Network Security Essentials: Applications and Standards*, 3rd Edition, Prentice Hall, 2007 2. Charles P. Pfleeger and Shari Lawrence Pfleeger, *Security in Computing*, 4th Edition, prentice Hall, 2007
d- Periodicals, Web Sites, ..., etc.	

Course Instructor: **Head of Department:**

Sign **Sign**