Arab Academy for Science and Technology & Maritime Transport
College of Computing & Information Technology

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

Course title	**Computer System Security**
Course code	**CS421**

Form no. (11A): **Knowledge and skills matrix for a course**

Course content	Week	Knowledge	Intellectual skills	Professional skills	General skills
Introduction	1	• Define security services, mechanisms and attacks. • Describe OSI security architecture.	• Differentiate between confidentiality and Integrity as security services		
Classical Encryption Techniques – Part I	2	• Demonstrate the encryption model for the classical ciphers (Caesar – monoalphabetic – Playfair – Hill)	• Distinguish between Symmetric ciphers and Asymmetric ciphers. • Apply classical encryption algorithms	• 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	Verify theory with practice
Classical Encryption Techniques – Part II	3	• Know the encryption model for the polyalphabetic cipher. • Define the steganography process	• Apply the polyalphabetic cipher on an example plaintext message • Analyze the security strengths for some classical encryption techniques		
Block Ciphers & DES	4	• Demonstrate the encryption model for the Fiestel cipher structure • Illustrate the block diagram for the DES round	• Apply a DES round on a block of bits • Analyze the Avalanche effect in DES • Recognize security problems with DES	• Design and implement an application to experiment with symmetric key encryption	Verify theory with practice

		• Demonstrate Triple DES operation			
Block cipher design principles/Block cipher modes of operation	5	• Demonstrate operation of the different block cipher modes	• Compare the different block cipher models.	• Design and implement an application to experiment with block cipher modes of operation	Verify theory with practice
Advanced encryption standard - AES	6	• Demonstrate the block diagram for AES	• Analyze the security strength of the AES key size		
7th Week Exam	7				
Intro to Number Theory	8	• Define discrete logarithm • Define Fermat's theorem • Define Euler's Theorem	• Calculate discrete logarithm • Calculate Euler's totient function		
Public key cryptography	9	• Define the principles of public-key cryptography • Demonstrate how RSA works	• calculate the public and private keys in the RSA algorithm	• Design and implement an application to experiment with public key cryptography	• Verify theory with practice
Key Distribution for Symmetric Encryption	10	• Demonstrate a key distribution scheme for symmetric encryption	• Analyze a key distribution scheme for symmetric encryption		
Key Distribution for Asymmetric Encryption	11	• Demonstrate the Diffie-Hellman key exchange algorithm	• Analyze a key distribution scheme for asymmetric encryption • Analyze Diffie-Hellman key exchange algorithm	• Design and implement an application to calculate the common session key using Diffie- Hellman key agreement protocol	• Verify theory with practice
12th Week Exam	12				
Message Authentication and Hash Functions	13	• List the authentication requirements • Describe the authentication functions	• Differentiate between a message authentication code and a hash value • Apply use of MAC and hash functions to provide message authentications		
Hash and MAC Algorithms	14	• Describe the message digest algorithm • Demonstrate the secure hash algorithm	• Distinguish between Hashing and Encryption	• Design and implement an application to experiment with MAC and hash algorithms	• Verify theory with practice

Firewalls	15	- Demonstrate Firewall Design Principles	- Identify security problems not handled by firewalls		

Course Instructor

Name:

Signature:

Head of Department

Name:

Signature: