Total No. of Questions: 6 *Total No. of Printed Pages:3*

Enrollment No.....

Faculty of Engineering / Science

End Sem (Even) Examination May-2022

CA3CO16 Network Security

Programme: BCA / BCA-MCA (Integrated) Branch/Specialisation: Computer Application

Duration: 3 Hrs. **Maximum Marks: 60**

Note: All questions are compulsory. Internal choices, if any, are indicated. Answers of Q.1 (MCQs) should be written in full instead of only a, b, c or d.

Q.1 i. What is the ethics behind training how to hack a system? **1**

(a) To think like hackers and know how to defend such attacks
(b) To hack a system without the permission
(c) To hack a network that is vulnerable
(d) To corrupt software or service using malware

ii. Which of them is not a wireless attack? **1**

(a) Eavesdropping (b) MAC Spoofing
(c) Wireless Hijacking (d) Phishing

iii. The Caesar cipher is a _____cipher that has a key of 3. **1**

(a) Transposition
(b) Additive
(c) Shift
(d) Transposition + subtraction + additive

iv. Encryption in Autokey cipher is done using _____. **1**

(a) A 5×5 table (b) A 13×2 table
(c) Vigenere table (d) A 6×6 table

v. DES follows **1**

(a) Hash Algorithm (b) Caesars Cipher
(c) Feistel Cipher Structure (d) SP Networks

vi. How many rounds does the AES-192 perform? **1**

(a) 10 (b) 12 (c) 14 (d) 16

P.T.O.

vii. Which one of the following is a cryptographic protocol used to secure HTTP connection? **1**
(a) Stream control transmission protocol (SCTP)
(b) Transport layer security (TLS)
(c) Explicit congestion notification (ECN)
(d) Resource reservation protocol

viii. A digital Signature is **1**
(a) A bit string giving identity of a correspondent
(b) A unique identification of a sender
(c) An authentication of an electronic record by trying it uniquely to a key only a sender knows
(d) An encrypted signature of sender

ix. Which of the following is not a transport layer vulnerability? **1**
(e) Mishandling of undefined, poorly defined
(b) The Vulnerability that allows "fingerprinting" & other enumeration of host information
(c) Overloading of transport-layer mechanisms
(d) Unauthorized network access

x. What layer in the TCP/IP stack is equivalent to the Transport layer of the OSI model? **1**
(a) Application (b) Host to host
(c) Internet (d) Network Access

Q.2 i. What are the three approaches to computer security? **2**
ii. What are the three fundamental principles of security management? **3**
iii. Explain any five malware attacks with suitable example. **5**
OR iv. Enlist ten different cyber-attack types. **5**

Q.3 i. Explain Homophonic substitution cipher. **2**
ii. Explain mention cipher technique using suitable examples Polygram substitution cipher, Polyalphabetic substitution cipher, and Playfair cipher. **8**
OR iii. Explain mention cipher technique using suitable examples Hill cipher, transposition techniques, Rail-Fence technique and Steganography. **8**

Q.4 i. What is symmetric and asymmetric encryption? **3**
ii. (a) Write two strength of data encryption standard (DES). **7**
(b) What is the difference between a private key and a public key?
(c) What is a block cipher?
(d) What is cipher block chaining?
OR iii. Why symmetric key cryptography alone can not resolve internet security issue? Write three differences between symmetric and symmetric key cryptography. **7**

Q.5 i. Explain RSA algorithm, with suitable example. **4**
ii. What is the relationship between VPN and Firewalls using suitable diagram? **6**
OR iii. What security vulnerabilities are addressed by VPN? Explain with suitable example. **6**

Q.6 Attempt any two:
i. Compare between Hyper Text Transfer Protocol (HTTP) and Secure Hyper Text Transfer Protocol (SHTTP). **5**
ii. Differentiate between Secure Socket Layer (SSL) and Transport Layer Security (TLS). **5**
iii. Illustrate the role of firewall and virtual private network. **5**

******

Marking Scheme
CA3CO16 Network Security

Q.1	i.	(a) To think like hackers and know how to defend such attacks		**1**
	ii.	(d) Phishing		**1**
	iii.	(c) Shift		**1**
	iv.	(c) Vigenere table		**1**
	v.	(c) Feistel Cipher Structure		**1**
	vi.	(c) 14		**1**
	vii.	(b) Transport layer security (TLS)		**1**
	viii.	(c) An authentication of an electronic record by trying it uniquely to a key only a sender knows		**1**
	ix.	(d) Unauthorized network access		**1**
	x.	(b) Host to host		**1**
Q.2	i.	Approaches to computer security		**2**
		Enlist approaches	1 Mark	
		Explanation	1 Mark	
	ii.	Three fundamental principles of security management		**3**
		Explanation- 1 Mark for each	(1 Mark*3)	
	iii.	Five malware attacks with suitable example		**5**
		Explanation- 1 Mark for each	(1 Mark*5)	
OR	iv.	Ten different cyber-attack types		**5**
		Explanation- 0.5 Mark for each	(0.5 Mark*10)	
Q.3	i.	Explain Homophonic substitution cipher.		**2**
		Explanation	2 Marks	
	ii.	Cipher technique using suitable examples		**8**
		Polygram substitution cipher	2 Marks	
		Polyalphabetic substitution cipher	2 Marks	
		Playfair cipher.	4 Marks	
OR	iii.	Cipher technique using suitable examples Hill cipher, transposition techniques, Rail-Fence technique and Steganography		**8**
		Explanation 2 Marks for each	(2 Marks*4)	
Q.4	i.	Explanation on symmetric encryption	1.5 Marks	**3**
		Explanation on asymmetric encryption	1.5 Marks	
	ii.	(a) Two strength of data encryption standard (DES).	2 Marks	**7**
		(b) Difference between a private key and a public key		
		Two difference each	2 Marks	
		(c) Block cipher		
		Explanation	2 Marks	
		(d) Cipher block chaining	1 Mark	
OR	iii.	Symmetric key cryptography		**7**
		Explanation	4 Marks	
		Three differences Explanation	3 Marks	
Q.5	i.	RSA algorithm		**4**
		Description	2 Marks	
		Example (step wise)	2 Marks	
	ii.	Relationship between VPN and Firewalls		**6**
		Explanation	4 Marks	
		Diagram	2 Marks	
OR	iii.	Security vulnerabilities are addressed by VPN		**6**
		Explanation	4 Marks	
		Diagram	2 Marks	
Q.6		Attempt any two:		
	i.	Compare between HTTP and (SHTTP		**5**
		Five differences each for 1 Mark	(1 Mark*5)	
	ii.	Differentiate SSL and TLS		**5**
		Five differences each for 1 Mark	(1 Mark*5)	
	iii.	Role of firewall and virtual private network.		**5**
		Description of firewall	2 Marks	
		Diagram	0.5 Mark	
		Description of virtual private network	2 Marks	
		Diagram	0.5 Mark	

******