Total No. of Questions: 6 *Total No. of Printed Pages:2*

Enrollment No......................................

Faculty of Science / Engineering
End Sem Examination May-2024
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. Assume suitable data if necessary. Notations and symbols have their usual meaning.

Q.1 i. Which of the following principles is violated if the computer system is not accessible? **1**
(a) Confident ability (b) Availability
(c) Access control (d) Authentication

ii. Which of the following attacks is a passive attack? **1**
(a) Masquerade (b) Modification of message
(c) Denial of service (d) Traffic analysis

iii. Hill cipher is an example of ____________. **1**
(a) Mono-alphabetic cipher (b) Substitution cipher
(c) Transposition cipher (d) Encrypted lock

iv. What is the process of hiding text within an image called? **1**
(a) Steganography (b) Encryption
(c) Spyware (d) Keystroke logging

v. DES encrypts blocks of _______ bits. **1**
(a) 32 (b) 64 (c) 56 (d) 128

vi. The 4×4 byte matrices in the AES algorithm are called- **1**
(a) States (b) Words (c) Transitions (d) Permutations

vii. Public key system is useful because________. **1**
(a) It uses two keys
(b) There is no key distribution problem as public key can be kept in a commonly accessible database
(c) Private key can be kept secret
(d) It is a symmetric key system

viii. In RSA, $\Phi(n)$ = _______ in terms of p and q. **1**
(a) (p)/(q) (b) (p)(q) (c) (p-1)(q-1) (d) (p+1)(q+1)

ix. VPN is abbreviated as __________. **1**
(a) Visual Private Network (b) Virtual Protocol Network
(c) Virtual Private Network (d) Virtual Protocol Networking

x. A proxy firewall filters at _________. **1**
(a) Physical layer (b) Data link layer
(c) Network layer (d) Application layer

Q.2 i. What do you mean by data integrity and data confidentiality? **2**

ii. What are the different security services in computer security? **3**

iii. Explain the different models of network security in details. **5**

OR iv. What do you mean by attack in network security? Explain different types of active attacks. **5**

Q.3 i. Differentiate between block cipher and stream cipher. **3**

ii. In the playfair cipher suppose the key is “MONARCHY”, plaintext “hide the gold in the tree stump” what is the cipher text? **7**

OR iii. Explain encryption and decryption by using Vernam cipher if plain text and key is given below- **7**
Plain text: all the best
Key: RANCHOBABA

Q.4 i. What are the different modes of block cipher? Explain any two modes. **4**

ii. Explain data encryption standard. What happens inside s-boxes in DES? **6**

OR iii. What are the differences between DES and AES? **6**

Q.5 Attempt any two:

i. How does the RSA algorithm work? Explain RSA encryption with the help of an example. **5**

ii. What are the principle elements of a public-key cryptosystem? **5**

iii. What is digital signature? How can confidentiality be achieved in digital signature? **5**

Q.6 Attempt any two:

i. What do you mean by IP Security? **5**

ii. Explain Secure Socket Layer (SSL). **5**

iii. What is Secure HyperText Transfer Protocol (SHTTP)? **5**

*****

Marking Scheme
Network Security (T) - CA3CO16 (T)

Q.1	i	b) Availability		**1**
	ii	d)Traffic analysis		**1**
	iii	b) Substitution cipher		**1**
	iv	a) Steganography		**1**
	v	b) 64		**1**
	vi	a) States		**1**
	vii	b) There is no key distribution problem as public key can be kept in a commonly accessible database		**1**
	viii	c) (p-1) (q-1)		**1**
	ix	c) Virtual Private Network		**1**
	x	d) Application layer		**1**
Q.2	i.	1+1		**2**
	ii.	3 services		**3**
	iii.	Models 1, 3 marks + model 2, 2 marks		**5**
OR	iv.	2+3		**5**
Q.3	i.	3 Marks		**3**
	ii.	Process	4 Marks	**7**
		Final cipher	3 Marks	
OR	iii.	Encryption 4 marks, decryption 3 marks		**7**
Q.4	i.	2+2		**4**
	ii.	4+2		**6**
OR	iii.	each different 1 marks		**6**
Q.5	i.	2+3		**5**
	ii.	each element 1 marks		**5**
OR	iii.	2+3		**5**
Q.6				
	i.	3 marks theory+2 marks diagram		**5**
	ii.	3 marks theory+2 marks diagram		**5**
	iii.	3 marks theory+2 marks diagram		**5**

******