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

Enrollment No.....

Faculty of Science

End Sem (Even) Examination May-2019

CA3CO16 Network Security

Programme: BCA 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. Who spread with user action? **1**
(a) Trojan (b) Virus (c) Spam (d) Adware

ii. Who hides deep with in PC? **1**
(a) Trojan (b) Virus (c) Spyware (d) Rootkits

iii. How many secret keys are needed if 100 members of club need to send secret message to each other? **1**
(a) 4950 (b) 5950 (c) 2950 (d) 3950

iv. Which is polyalphabetic cipher. **1**
(a) Ceaser (b) Affine (c) Shift (d) Playfair

v. What is the number of rounds in DES? **1**
(a) 15 (b) 16 (c) 17 (d) 18

vi. What is the number of rounds in AES-192? **1**
(a) 10 (b) 12 (c) 14 (d) 16

vii. For RSA to work, value "p" must be less than of **1**
(a) n (b) q (c) Φ(n) (d) d

viii. RSA belongs to _____ cryptography. **1**
(a) Private (b) Public
(c) Both (a) and (b) (d) None of these

ix. Firewall may be described as specified form of **1**
(a) Router (b) Bridge
(c) Operating System (d) Architecture

x. The Secure Socket layer provides **1**
(a) Encryption of message sent by both client and server
(b) Server authentication
(c) Optional client authentication
(d) All of these.

P.T.O.

Q.2 i. What is network security? **2**
ii. What do you understand by Security Goals? Explain. **3**
iii. Explain various security mechanism in relation of security services. **5**
OR iv. Explain any five malware attacks with suitable example. **5**

Q.3 i. What is character oriented and bit oriented cryptography? **2**
ii. Differentiate between homophonic substitution cipher and polygram substitution cipher. **3**
iii. Encrypt the message "this is an exercise" using multiplicative cipher with key=15. **5**
OR iv Use a hill cipher to encipher the message "we live in an insecure world". Use the following key: **5**

$$K=\begin{bmatrix}03 & 02\\ 05 & 07\end{bmatrix}$$

Q.4 i. Why does the round key generator need a parity drop permutation? **3**
ii. Draw block diagram of DES. Explain Feistel round structure in detail. **7**
OR iii. Draw block diagram of AES-128. Explain all transformation of AES-128 in detail. **7**

Q.5 i. What is Symmetric and Asymmetric Cryptography. **2**
ii. Draw and explain the block diagram of Asymmetric Cryptography. **3**
iii. Explain RSA Cryptosystem. Bob Chooses 7 and 11 as p and q. Show how alice send a plaintext "5". **5**
OR iv Explain RSA Digital signature scheme and compare it to the RSA cryptosystem. **5**

Q.6 Write short note on any two:
i. Firewalls **5**
ii. Virtual Private Networks (VPN) **5**
iii. Secure Socket Layer (SSL) **5**

******

Marking Scheme
CA3CO16 Network Security

Q.1	i.	Who spread with user action? (b) Virus	**1**
	ii.	Who hides deep with in PC? (d) Rootkits	**1**
	iii.	How many secret keys are needed if 100 members of club need to send secret message to each other? (a) 4950	**1**
	iv.	Which is polyalphabetic cipher. (d) Playfair	**1**
	v.	What is the number of rounds in DES? (b) 16	**1**
	vi.	What is the number of rounds in AES-192? (b) 12	**1**
	vii.	For RSA to work, value "p" must be less than of (c) Φ(n)	**1**
	viii.	RSA belongs to _____ cryptography. (c) Both (a) and (b)	**1**
	ix.	Firewall may be described as specified form of (a) Router	**1**
	x.	The Secure Socket layer provides (a) Encryption of message sent by both client and server	**1**
Q.2	i.	Concept of network security	**2**
	ii.	Security Goals	**3**
	iii.	Security mechanism 3 marks Relation of security services. 2 marks	**5**
OR	iv.	Any five malware attacks with suitable example 1 mark for each (1 mark * 5)	**5**
Q.3	i.	Difference character oriented and bit oriented cryptography	**2**
	ii.	Differentiate between homophonic substitution cipher and polygram substitution cipher.	**3**
	iii.	Encrypt the message "this is an exercise" using multiplicative cipher with key=15.	**5**
OR	iv	Use a hill cipher to encipher the message "we live in an insecure world".	**5**
Q.4	i.	Round key generator need a parity drop permutation	**3**
	ii.	Draw block diagram of DES 3 marks Feistel round structure 4 marks	**7**
OR	iii.	Draw block diagram of AES-128 3 marks All transformation of AES-128 4 marks	**7**
Q.5	i.	Differentiate Symmetric and Asymmetric Cryptography.	**2**
	ii.	Draw block diagram of Asymmetric Cryptography 2 marks Explain of Asymmetric Cryptography. 1 mark	**3**
	iii.	RSA Cryptosystem. 1 mark Bob Chooses 7 and 11 as p and q. Show how alice send a plaintext "5". 4 marks	**5**
OR	iv	RSA Digital signature scheme 3 marks Compare it to the RSA cryptosystem. 2 marks	**5**
Q.6		Write short note on any two:	
	i.	Firewalls	**5**
	ii.	Virtual Private Networks (VPN)	**5**
	iii.	Secure Socket Layer (SSL)	**5**

******