B.E. Eighth Semester (Computer Technology) (C.B.S.)
Cyber & Information Security

P. Pages : 2

Time : Three Hours

|||||||||||||||||||||||
0652

Max. Marks : 80

_____

Notes : 1. All questions carry marks as indicated.
2. Solve Question 1 OR Questions No. 2.
3. Solve Question 3 OR Questions No. 4.
4. Solve Question 5 OR Questions No. 6.
5. Solve Question 7 OR Questions No. 8.
6. Solve Question 9 OR Questions No. 10.
7. Solve Question 11 OR Questions No. 12.
8. Due credit will be given to neatness and adequate dimensions.
9. Assume suitable data whenever necessary.
10. Illustrate your answers whenever necessary with the help of neat sketches.

1. a) Explain the OSI security Architecture and security attacks with example. **8**

   b) Explain the various aspects of Information security. **5**

OR

2. a) Explain cryptanalysis and its types. **5**

   b) Explain transposition Technique? How it is different form substitution ciphers? If the Cipher is keyed by a word "Computer" and plain text is "Please transfer one million dollars to my account Six Six two" Obtain Cipher text by Playfair substitution method. **8**

3. a) Write an algorithm for DES and analyze it. **7**

   b) What are the Block Cipher modes of operation of DES. **6**

OR

4. a) Differentiate public keys and convention encryption **7**

   b) What are the principle elements of public key cryptosystem. **6**

5. a) Write a short note on "Centralized key Distribution Scenario". **7**

   b) Describe Diffie - Hellman key exchange algorithm. **7**

OR

6. a) Write RSA algorithm. Explain its implementation an security. **7**

   b) Perform Encryption and decryption using the RSA algorithm, for the following P = 7, q = 11, e = 3, m = 9 **7**

7.	a)	Give properties and requirements of Digital signatures.	**6**
	b)	What is message authentication? What is requirement which three classes grouped while functioning.	**7**

OR

8.	a)	Explain the various steps of Kerberos Version?	**6**
	b)	Explain Authentication function with neat sketch diagram and example.	**7**

9.	a)	What are the approaches to intrusion detection.	**6**
	b)	Explain various firewall design principles what are the different firewall characteristics? What are the different types of firewalls.	**7**

OR

10.	a)	Explain in detail the operation of secure socket Layer.	**7**
	b)	Explain the following terms.	**6**
		i) Trap doors and cross-site scripting (XSS).	
		ii) Worm signature Extraction.	

11.	a)	Explain in detail transaction Attacks.	**7**
	b)	What is S/MIME? What are function it provides.	**7**

OR

12.		Write a short note on **any three.**	**14**
	a)	Types of virus.	
	b)	Phishing.	
	c)	PGP.	
	d)	SQL injection.	
	e)	Firewall	

****