B.E.(Computer Science & Engineering) Eighth Semester (C.B.S.)

Information & Cyber Security

P. Pages : 2 **NRT/KS/19/3691**

Time : Three Hours * 0 6 9 5 * 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.
11. Use of non programmable calculator is permitted.

1. a) What are the different issues in information security. Explain in brief. **7**

b) Explain columnar cipher techniques with example. **6**

OR

2. a) Distinguish between monoalphabetic and polyalphabetic cipher with example of each. **7**

b) Draw and explain internetwork security model. **6**

3. a) What is session key? Explain centralized and decentralized key distribution in brief. **8**

b) Explain IDEA in brief. **6**

OR

4. a) Explain data encryption standard in detail. **8**

b) Explain any three block cipher modes of operation. **6**

5. a) Differentiate between conventional encryption and public key encryption. **7**

b) Explain "Man in the middle attack" in detail. **6**

OR

6. a) In a public key cryptosystem using RSA. Ciphertext C = 10 sent to user whose public key is e=5, n = 35 what is the plaintext?
Also write steps of RSA. **7**

b) Explain Diffie Hellman key exchange algorithm. Clearly mention the weaknesses of this algorithm. **6**

7.	a)	Explain Kerberos version 4 in detail.	**7**
	b)	Draw and explain PKI Architecture.	**7**

OR

8.	a)	Explain X-509 digital certificate (directory) format.	**7**
	b)	Explain "MD5" in detail.	**7**
9.	a)	Explain transport and tunnel mode of security in brief.	**7**
	b)	Draw and explain SSL stack format in brief.	**6**

OR

10.	a)	What do you mean by "Intrusion detection system" and "intrusion prevention system".	**6**
	b)	Explain different firewall design principles.	**7**
11.	a)	Explain pretty good privacy in detail.	**8**
	b)	Explain secure electronic transaction.	**5**

OR

12.	a)	Write a note on :-	
		i) Cross site scripting.	**4**
		ii) SQL injection.	**4**
		iii) E-transaction Attack.	**5**

****