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

Information & Cyber Security

P. Pages : 2

Time : Three Hours

* 0 6 2 0 *

NJR/KS/18/4747

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) Define cryptography in network security. What do you understand by service, mechanism and attacks related to the cryptography with an example. **8**

b) Describe conventional encryption model. What are the requirements for secure use of conventional encryption? **6**

OR

2. a) Write a short note on polyalphabetic ciphers with an example. **6**

b) Encrypt the message "Money helps to build infrastructure" using Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$ Show your calculations and result. **8**

3. a) Write a short note on-strength of DES. **6**

b) Explain centralized and decentralized key distribution in brief. **7**

OR

4. a) Briefly Explain cipher block chaining mode of operation. **7**

b) Describe key generation of AES algorithm. **6**

5. a) How does asymmetric key encryption ensure "Non-repudiation"? Explain with an example. **7**

b) What is the role of key distribution center? What are it's drawbacks. **6**

OR

6. a) Explain RSA algorithm in details. Perform encryption and decryption p = 17; q = 11; e = 7; M = 88. **8**

b) Explain about man in middle Attack. **5**

7. a) Describe Diffie-Hellman key exchange Algorithm with suitable example. What are the weakness of the Algorithm explain. **7**

b) Write a short note on Hash function? Give the basic uses of hash function. **6**

OR

8. a) Explain public key infrastructure architecture and its function. **6**

b) Explain the digital signature requirements and direct digital signature in detail. **7**

9. a) Explain the SSL protocol stack in detail. **6**

b) Explain the transport layer security in detail. **7**

OR

10. a) What do you mean by "Trusted Systems", "Intrusion Detection system" & "Intrusion Prevention system". **8**

b) Explain Applications and advantages of IP Sec. **5**

11. a) How Chipcard transaction is perform? Explain in detail. **8**

b) Describe SQL Injection in detail. **6**

OR

12. a) Write a short note on **any two.** **14**

a) S|MIME

b) E-transaction attack.

c) Buffer Overflow

*****