R17

Code No: 844AE

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
MCA IV Semester Examinations, October/ November - 2020
INFORMATION SECURITY

Time: 2 Hours **Max.Marks:75**

Answer any five questions
All questions carry equal marks

1.a) List and explain the security services.
b) Explain how Cipher Feedback mode can convert a block cipher to stream cipher. [7+8]

2. Explain how a plain text block is encrypted using Blowfish algorithm. [15]

3.a) Perform encryption and decryption using RSA algorithm of the following. p=17; q=11; e=7; M=88.
b) With a neat diagram explain how to transfer a message confidentially and at the same time ensure integrity and authenticity. [7+8]

4.a) Explain KerberosV4 authentication dialogue in detail.
b) What is the purpose of Digital certificates? Explain. [7+8]

5.a) Explain the fields of PGP User Public key Ring?
b) Write down the applications of Authentication protocols. [7+8]

6.a) List and describe the security services offered by S/MIME.
b) What are the requirements of web security? [7+8]

7.a) Describe how e-transactions are secured.
b) What is the purpose of SSL Change Cipher Specification protocol? [7+8]

8.a) List and explain different types of intruders.
b) Explain any two approaches of intrusion detection. [7+8]

---oo0oo---