R19

Code No: 863AE

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
MCA III Semester Examinations, July/August - 2021
INFORMATION SECURITY

Time: 3 Hours   Max.Marks:75

Answer any five questions
All questions carry equal marks
- - -

1.a) Describe the model for Network Security with a neat diagram.
  b) Explain about Block Cipher design principles.   [8+7]

2. What are the basic requirements of Authentication? How the message is authenticated using secure hash algorithm (SHA-512)?   [15]

3. Describe the Kerberos security mechanism and explain why Kerberos is important for providing security in real time?   [15]

4. What are the applications of IPSec? Explain about IPSec architecture with a neat sketch.   [15]

5.a) What are the limitations of firewalls? Explain about Firewall design principles.
  b) Explain various file access activities used for intrusion detection.   [8+7]

6.a) Discuss about various kinds of security mechanisms in detail.
  b) Differentiate between Symmetric and Asymmetric key cryptography.   [7+8]

7. Explain RSA algorithm for encryption and decryption. Find n, d where p=11, q = 3 , and e = 3. Encrypt the message "MEET ME AFTER" using RSA.   [15]

8. Explain the following
   a) S/MIME Functionalities
   b) Viruses and Worms.   [7+8]

---ooOoo---