Code No: 824AE

R15

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
MCA IV Semester Examinations, December - 2019
INFORMATION SECURITY

Time: 3hrs   Max.Marks:75

Note: This question paper contains two parts A and B.
Part A is compulsory which carries 25 marks. Answer all questions in Part A. Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 10 marks and may have a, b, c as sub questions.

PART - A

5 × 5 Marks = 25

1.a)   Explain the model for network security .   [5]
  b)   Discuss about Linear and differential cryptanalysis?   [5]
  c)   What is the function of TGS server in Kerberoes.   [5]
  d)   Draw and explain fields in AH header.   [5]
  e)   What are the limitations of firewalls?   [5]

PART - B

5 × 10 Marks = 50

2.   Give an example to explain the concept of transposition ciphers in detail.   [10]

OR

3.   Compare and Contrast between Symmetric and Asymmetric key cryptography.   [10]

4.   In an RSA system, the public key of a given user is e=31, n=3599. What is the private key of this user?   [10]

OR

5.   Explain DES algorithm with suitable examples.Discuss its advantages and limitations[10]

6.   Give a neat sketch to explain the concept of Secure Hash Algorithm (SHA).   [10]

OR

7.   With the help of an example explain how knapsack algorithm is used for authentication?   [10]

8.   Explain the operation PGP message generation and message reception.   [10]

OR

9.   Draw the IP security authentication header and explain the functions of each field.   [10]

10.   Explain the steps involved in performing Secure Inter-branch Payment Transactions. [10]

OR

11.   List the characteristics of a good firewall implementation? How is circuit gateway different from application gateway?   [10]

---ooOoo---