R15

Code No: 824AE

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
MCA IV Semester Examinations, April/May - 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) Differentiate symmetric and asymmetric encryption. [5]
b) Justify how DES algorithm uses feistel cipher structure. [5]
c) Describe the Kerberos security mechanism and explain why it is important in real time for providing security? [5]
d) Describe how encapsulating security payload is defined. [5]
e) Enumerate counter measure for viruses and worms. [5]

PART - B

5 × 10 Marks = 50

2.a) Explain the principles of security.
b) Demonstrate model for internetwork security with neat diagram? [5+5]

OR

3. Describe the following
a) Security attacks b) Security services c) Security mechanisms [10]

4.a) Enumerate the principles of conventional encryption algorithms.
b) Formulate AES encryption and decryption process with neat sketch. [5+5]

OR

5.a) Explain linear and differential cryptanalysis in a detail manner.
b) Explain RCY Algorithm. [5+5]

6.a) Differentiate public key and private key and explain public key infrastructure with an example.
b) Describe the differences between HMAC and CMAC. [5+5]

OR

7.a) Describe digital signatures with an example.
b) Describe the different types of the message authentication codes and explain with an example. [5+5]

8.a) Enumerate all services of Pretty Good Privacy and explain with neat sketch.
b) Justify why S/MIME is a security enhancement to MIME internet email format standard. [5+5]

OR

9.a) Discuss the importance of the authentication header and explain its structure.
b) Demonstrate MIME transfer encoding techniques and certificate processing. [5+5]

10.a) Demonstrate how does the intrusion detection system work when the contents of the network message are encrypted? At what level can this packet be read and analyzed.
b) Differentiate statistical anomaly detection and rule–based intrusion detection. [5+5]

OR

11.a) Discuss firewall design principles and also explain techniques.
b) Discuss how intrusion prevention is achieved through password management. [5+5]

---ooOoo---