Code No: 814AT **R13**

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

Time: 3 Hours **Max. Marks: 60**

Note: This question paper contains two parts A and B.
Part A is compulsory which carries 20 marks. Answer all questions in Part A. Part B consists of 5 Units. Answer any one full question from each unit. Each question carries 8 marks and may have a, b, c as sub questions.

PART - A

5 × 4 Marks = 20

1.a) Explain different kinds of security approaches. [4]
b) Describes the Diffie- Hellman key exchange technique. [4]
c) Discuss the techniques of public key certificates for distribution of public keys. [4]
d) Compare and contrast the key management in PGP and S/MIME. [4]
e) Explain the operation of secure socket layer in detail. [4]

PART - B

5 × 8 Marks = 40

2.a) Consider the following:
Plaintext: "KEY"
Secret key: "CRYPTOGRAPHY"
Compute the cipher text from given plain text and key using hill cipher method.
b) Give an overview of various security services. [4+4]

OR

3. Explain symmetric and asymmetric key cryptography. [8]

4. Apply the mathematical foundations of RSA algorithm. Perform encryption decryption for the following data, p=17, q=7, e=5, n=119, message = "6". Use extended Euclid`s algorithm to find the private key. [8]

OR

5.a) With a neat diagram, explain about the multiple encryptions (Triple DES with two and three keys).
b) Briefly explain RC4 algorithm. [4+4]

6. Describe digital signature algorithm and show how signing and verification is done using DSS. [8]

OR

7.a) X.509 includes three alternative authentication procedures, what are these three procedures? Explain them in brief.
b) Explain in detail about MAC algorithms and its requirements. [4+4]

8.a) What do you mean by Security Association? Specify the parameters that identify the Security Association.

b) Summarize about the authentication header of IP and discuss about encapsulating security payload of IP. [4+4]

OR

9.a) Explain the general format of Pretty Good Privacy Message.

b) Discuss the architecture of IP security. [4+4]

10. Explain the different types of firewalls with neat diagrams. [8]

OR

11.a) List and explain the major classes of intruders.

b) Describe Secure Electronic Transaction for E- Commerce transaction with neat diagram. [4+4]

---ooOoo---