R13

Code No: 814AT

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD

MCA IV Semester Examinations, April/May - 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) What are the security services? [4]
b) Discuss the terms: Block ciphers and stream ciphers. [4]
c) What are the design objectives for HMAC? Compare HMAC and CMAC. [4]
d) Explain transport mode and tunnel mode in IPSec. [4]
e) Compare SSL and TLS. [4]

PART - B

5 × 8 Marks = 40

2. Discuss about active attacks and passive attacks. [8]

OR

3. Explain the following:
a) Steganography b) Polyalphabetic cipher [4+4]

4. Explain RSA algorithm in detail with relevant diagrams. [8]

OR

5. Explain AES algorithm in detail. [8]

6. Describe HMAC algorithm. [8]

OR

7. Explain Kerberos version 4 message exchanges for providing authentication. [8]

8. Explain the following related to S/MIME messages
a) EnvelopedData.
b) SignedData
c) ClearSigning
d) RegistrationRequest
e) Certificate-only Messages. [8]

OR

9.a) Give a brief note on Encapsulating security payload.
b) Discuss about different combinations of security associations. [4+4]

10. Discuss in detail the messages exchanged between client and server during the phase of SSL handshake protocol. [8]

OR

11. Discuss about virtual elections. [8]

---ooOoo---