R13

Code No: 814AT

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
MCA IV Semester Examinations, June/July - 2018
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 is the need for information security? [4]
 b) Differentiate between block and stream ciphering scheme. [4]
 c) Explain about hash functions. [4]
 d) Define the services provided by PGP. [4]
 e) State and explain about Intruders. [4]

PART - B
5 × 8 Marks = 40

2. List and explain in detail about various types of security services. [8]
OR
3. With an example explain in detail about mono-alphabetic substitution technique. [8]

4. Draw a neat diagram, explain the DES algorithm for 64 bit data and 64 bit key size.[8]
OR
5. Explain the encryption and decryption are performed using RSA algorithm. Using RSA algorithm generate the cipher text with given data: p=11, q=5,e=3, PT=9. [8]

6. Describe in detail about secure hash algorithm (SHA) in detail. [8]
OR
7. Illustrate in detail about X.509 authentication service with a neat diagram. [8]

8. With a neat diagram explain the architecture of IP Security. [8]
OR
9. Describe in detail about various techniques used for key management. [8]

10. Explain the different types of firewall and its configurations in detail. [8]
OR
11. Explain in detail about Secure Inter-branch Payment Transactions. [8]

---oo0oo---