Code No: 824AE **R15**

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD
MCA IV Semester Examinations, January - 2018
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 in detail various types of attacks on encrypted messages. [5]
b) Explain briefly about RSA algorithm in detail manner. [5]
c) Describe how hash algorithms will provide security. [5]
d) Explain about IP traffic processing in IP security Policy. [5]
e) Define firewall. Explain the firewall design principles in a detail manner. [5]

PART - B

5 × 10 Marks = 50

2.a) Explain about the model for internetwork security.
b) Convert the following plain text message P = "cryptography provides high security" into cipher text by using simple columnar transposition technique
i) Basic technique
ii) With multiple rounds. [5+5]

OR

3.a) With a neat diagram explain simplified model of conventional Encryption.
b) Differentiate between symmetric and asymmetric key cryptography. [6+4]

4.a) Illustrate the procedure of key distribution in conventional encryption.
b) Differentiate between AES, DES and Blow fish algorithms. [7+3]

OR

5.a) Explain round function evaluation in feistel cipher structure.
b) Write the difference between session key and master key. [7+3]

6.a) Write in detail what types of attacks are addressed by message authentication.
b) Describe what arithmetical and logical functions are used in MD5? [6+4]

OR

7.a) With a neat diagram explain Kerberos security mechanism. And also explain how Kerberos is important in real time for providing security?
b) What is the difference between a public key and private key. [7+3]

8.a) Explain on what basis Zimmerman has developed PGP for email security?
b) With a neat diagram explain function modules and standardized protocols used between them in Internet mail architecture. [5+5]

OR

9.a) Explain in detail about IP security overview?
b) Write the difference between PGP and MIME types. [7+3]

10.a) Write in a detail manner that define the parameters of an SSL session state.
b) Write differences between socket layer security and transport security. [7+3]

OR

11.a) Briefly explain What are the different types of firewalls.
b) Enumerate counter measures for viruses and worms. [6+4]

---oo0oo---