**Code No: 117DY** **R13**

**JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY HYDERABAD**
**B. Tech IV Year I Semester Examinations, April/May - 2018**
**INFORMATION SECURITY**
**(Information Technology)**

**Time: 3 Hours** **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**

**(25 Marks)**

| | | |
|---|---|---|
| 1.a) | What is the need of network security? | [2] |
| b) | Differentiate between active attacks and passive attacks. | [3] |
| c) | Define avalanche effect. | [2] |
| d) | What is the purpose of diffie hellman key exchange? | [3] |
| e) | List any three hash functions. | [2] |
| f) | List out the requirements of hash functions. | [3] |
| g) | Illustrate the services provided by IPSec. | [2] |
| h) | Describe tunnel mode in IP security. | [3] |
| i) | Define transport layer security. | [2] |
| j) | List out various types of firewalls. | [3] |

**PART-B**

**(50 Marks)**

2.a) With a neat diagram explain the model of network security.
b) Demonstrate with an example transposition technique. [5+5]

**OR**

3.a) Apply Caesar cipher where k=5 and decrypt the given Cipher text "YMJTYMJWXNIJTKXNQJSHJ".
b) Give an overview of various security services. [5+5]

4. Draw the general structure of DES and describe how encryption and decryption are carried out and identify the strengths of DES algorithm. [10]

**OR**

5. 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. [10]

6. Where are hash functions used? What characteristics are needed in secure hash functions? Write about the security of hash functions and MACs. [10]

**OR**

7. Describe digital signature algorithm and show how signing and verification is done using DSS. [10]

8. How does PGP provide authentication and confidentiality for email services and for file transfer applications? Draw the block diagram and explain the components. [10]

**OR**

9. Summarize about the authentication header of IP and discuss about encapsulating security payload of IP? [10]

10. Describe Secure Electronic Transaction for E-Commerce transaction with neat diagram. [10]

**OR**

11. Estimate what is the role of intrusion detection system? What are the three benefits that can be provided by the intrusion detection system? [10]

**--ooOoo--**