6TH SEM./CS&E /IT/ 2024(S)

Th-1 Cryptography and Network Security

Full Marks: 80 **Time- 3 Hrs**

Answer any five Questions including Q No.1& 2
Figures in the right hand margin indicates marks

1. Answer **All** questions 2 x 10
   a. Distinguish between passive attack and active attack.
   b. Define Denial of service.
   c. What are the protocols used in IP security?
   d. Convert the Given Text "CRYPTOGRAPHY" into cipher text using Rail fence Technique.
   e. Name three configuration of firewall.
   f. Define active webpage.
   g. Define time stamping protocol.
   h. Define block cipher.
   i. Write the name of participants in the SET system.
   j. Define SEED.

2. Answer **Any Six** Questions 6 x 5
   a. Differentiate between symmetric key and asymmetric key cryptography.
   b. Convert the plain text "ACT" using hill cipher to cipher text using key matrix.
   6 24 1
   13 16 10
   20 17 15
   c. Write the RSA algorithm and explain it with a suitable example.
   d. Define authentication token and illustrate how Challenge/Response Tokens works.
   e. Discuss briefly about Digital Signature.
   f. Define firewall. How application Gateway and Packet filter works.
   g Why is SSL layer positioned between the application layer and transport layer? Explain the SSL handshake protocol.

3 Define digital certificate and write down the steps required to generate a digital certificate. 10

4 Briefly Discuss about key principles of network security. 10

5 Define Secure Electronic Transaction. Discuss the entire SET process briefly. 10

6 Briefly explain about the architecture of VPN. 10

7 Write short notes on any two. 10
   a) SSL
   b) Biometric Authentication
   c) IPSec
   d)Encryption and Decryption