B.Tech. (CSE) Professional Elective-V, 7th Semester
(G-Scheme) Examination, December-2022
NETWORK SECURITY AND CRYPTOGRAPHY
Paper-PEC-CSE-411-G

Time allowed : 3 hours] *[Maximum marks : 75*

Note: *Attempt **five** questions in all, selecting at least one question from each section. **Question no. 1 is compulsory.** All question carry equal marks.*

1. Explain the following : 6×2.5=15

(a) Product cipher
(b) Homophonic Substitution Cipher
(c) Cipher Block Chaining
(d) DES Design Principles
(e) Email Security
(f) Kerberos

Section-A

2. (a) What are the elements of cryptographic operation? Explain in detail with the help of a diagram. 10

(b) Explain Polyalphabetic Substitutioin Cipher. Explain using suitable examples. 5

3. (a) Explain Transposition techniques in details with suitable examples. 8

(b) What is the problem of key distribution in symmetric key cryptography? 7

Section-B

4. (a) Explain overview of the DES Encryption Algorithm with the help of a diagram.

   (b) What are Limitations of various DES Modes

   2×7.5=15

5. Explain the subkey generation in the Blowfish algorithm. 15

Section-C

6. (a) Why is the SSL Layer positioned between the application layer and transport layer?

   (b) What is the purpose of the SSL alert protocol?

   2×7.5=15

7. (a) What is the significance of the time stamping protocol? 8

   (b) How does SET protect payment information from the merchant? 7

Section-D

8. Explain the following:

   (a) Certificate base authentication 8

   (b) Biometric base authentication 7

9. What is single sign on (SSO) approach? Explain in detail. 15