SECTION – A

2. (a) Explain substitution techniques in details with suitable examples. 10

   (b) What are the two primary ways in which a plain text message be codified to obtain cipher text ? 5

3. (a) Define encryption and decryption. Explain using suitable examples. 8

   (b) Explain Diffie-Hellman Key-Exchange / Agreement Algorithm. 7

SECTION – B

4. (a) How does the one-time initialization step work in AES ? Explain the steps in the various rounds in AES. 7.5

   (b) Give advantages and disadvantages of different DES Modes. 7.5

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

SECTION – C

6. (a) Explain the SSL handshake protocol. 7.5

   (b) How is SHTTP different from SSL ? 7.5

7. (a) Outline the broad level steps in SET. 8

   (b) How is 3-D Secure different from SET ? 7

SECTION – D

8. (a) What are the problems and their solutions Related to Smart Card Technology. 8

   (b) What is Kerberos ? The Internet is an insecure place, Justify. 7

9. Explain the following : $7.5 \times 2 = 15$

   (a) Key Distribution Center(KDC)

   (b) Security handshake pitfalls

Roll No. .....

3538

B. Tech. 7th Semester (CSE) Professional Elective-V Examination – May, 2023

NETWORK SECURITY AND CRYPTOGRAPHY

Paper : PEC-CSE-411-G

Time : Three hours] *[Maximum Marks : 75*

Before answering the questions, candidates should ensure that they have been supplied the correct and complete question paper. No complaint in this regard, will be entertained after examination.

Note : Attempt ***five*** questions in all, selecting ***one*** question from each Section. Question No. 1 is ***compulsory***.

1. Explain the following : 2.5 × 6 = 15

(a) Cryptanalyst

(b) Rail-Fence Technique

(c) Electronic Codebook Book

(d) DES Weak Keys

(e) Electronic Money

(f) Biometric authentication