OR

(b) Encrypt the message "KILL AT TWO" using Playfair cipher using the key "SECURITY". Show the necessary steps for converting plain text to cipher text.

10 Marks (CO1)

740

H Roll No. .....

TCS–491

B. TECH. (CSE)

(FOURTH SEMESTER)

MID SEMESTER EXAMINATION,

April/May, 2022

INTRO TO CRYPTOGRAPHY

Time : 1½ Hours

Maximum Marks : 50

Note : (i) Answer all the questions by choosing any ***one*** of the sub-questions.

(ii) Each question carries 10 marks.

1. (a) What is the difference between Passive and Active security attack ? Explain each type by giving *two* examples of each type.

10 Marks (CO1)

P. T. O.

OR

(b) What are the *two* types of classical cipher ? Explain with *one* example of each. 10 Marks (CO1)

2. (a) What do you mean by Steganography ? Write about any *two* techniques of steganography. 10 Marks (CO1)

OR

(b) What do you mean by OSI security Architecture ? Write about five security services and 8 security mechanism. 10 Marks (CO1)

3. (a) With the help of a diagram briefly discuss the functions performed in S-DES. Explain the key generation and Encryption process with the help of necessary block diagram. 10 Marks (CO2)

OR

(b) Explain with the help of suitable diagram the key generation process of S-DES cipher. 10 Marks (CO2)

4. (a) Calculate the round keys (sub keys) K1, K2 from the key K = 1010101011 using S-DES algorithm. Give the values of P10 = {3, 5, 2, 7, 4, 10, 1, 9, 8, 6} and P8 = {6, 3, 7, 4, 8, 5, 10, 9}. 10 Marks (CO2)

OR

(b) Explain about double DES and Triple DES with suitable block diagram and the keys used. 10 Marks (CO2)

5. (a) Show the Encryption and Decryption calculation of plain text "attack at two am" use the value of key = 7 using CAESAR CIPHER. Show the necessary steps for converting Plain text to cipher text. Write the relevant formulae. 10 Marks (CO1)