H Roll No. .....

TCS–491

B. TECH. (CSE)

(FOURTH SEMESTER)

MID SEMESTER

EXAMINATION, April, 2023

INTRODUCTION TO CRYPTOGRAPHY

Time : 1½ Hours

Maximum Marks : 50

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

(ii) Each sub-question carries 10 marks.

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

(CO1)

P. T. O.

OR

(b) What are the *two* types of Classical Cipher ? Explain the working with one example of each type. (CO1)

2. (a) What do you mean by Network Security Model ? Write about the various components of the Network Security Models. (CO1)

OR

(b) What do you mean by OSI security Architecture ? Write about 5 security services and 8 security mechanism. (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. (CO2)

OR

(b) Explain with the help of suitable diagram the 8 bit round key generation process of S-DES cipher using a 10 bit main key. (CO2)

4. (a) Calculate the round keys(sub keys) K1, K2 from the key K = 1010101010 using S-DES algorithm. Given the values of P10 = {3, 5, 2, 7, 4, 10, 1, 9, 8, 6} and P8 = {6, 3, 7, 4, 8, 5, 10, 9}. (CO2)

OR

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

5. (a) Show the Encryption and Decryption calculations of plain text "MEETING AT FIVE" use the value of Key = 5 using CAESAR CIPHER. Show the necessary steps for converting Plain text to cipher text. Write the relevant formulae. (CO1)

OR

(b) Encrypt the message "ATTACK AT TWO" using Play fair cipher using the key "GRAPH". Show the necessary steps for converting Plain text to Cipher text. (CO1)