H Roll No. .....

TCS–392

B. TECH. (CSE) (THIRD SEMESTER)
MID SEMESTER
EXAMINATION, Oct., 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) Implement Playfair Cipher technique and find out the value of cipher text, where plaintext is "graphicerahilluniversity" and Key is "algorithms" ? (CO1)

OR

(b) What is the OSI security Architecture and how does it provide security for networks ? (CO1)

P. T. O.

2. (a) Encrypt the message "meet me at the usual place at ten rather than eight oclock" using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$. Show the calculation for the corresponding decryption of the cipher text to recover the original plaintext. (CO1)

OR

(b) Using the Vigenere cipher, Decrypt the word "ZICVTWQNGRZGVTWAVZHCQYGL MGJ" using the key : "deceptive". (CO1)

3. (a) Calculate the round keys K1, K2 from the key K= 10001101 Using S-DES algorithm. (CO2)

OR

(b) What is the RC4 algorithm and how does it work in cryptography ? (CO2)

Given S=[0 1 2 3 4 5 6 7],

K= [1 2 3 6] and

Plain text P = [1 2 2 2] and find out the cipher text using RC4 algorithm.

4. (a) What is Triple DES (DES3), and how does it enhance the security of the original DES algorithm ? What is the block size used in DES, DES2, and DES3 ? (CO2)

OR

(b) What is the fundamental difference between truly random numbers and pseudorandom numbers in the context of cryptography ? (CO2)

5. (a) Explain the concept of the steganography and types also discuss the various other techniques have been used historically, Also discuss the Shannon's theory. (CO1)

OR

(b) Explain the DES algorithm and its use in symmetric encryption methods. Mention the strengths and weakness of DES algorithm and discuss Avalanche effect. (CO2)