H Roll No. ....

TCS–619

B. TECH. (CSE) (SIXTH SEMESTER) MID SEMESTER EXAMINATION, April/May, 2022

NETWORK AND SYSTEM SECURITY

Time : $1\frac{1}{2}$ 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) Explain two general approaches to attacking a conventional encryption scheme. 10 Marks (CO1)

OR

(b) What do you mean by attacks ? Differentiate between active and passive attack. 10 Marks (CO1)

P. T. O.

2. (a) What is the difference between a block cipher and a stream cipher ?

10 Marks (CO2)

OR

(b) Explain DES encryption algorithm with the help of example. 10 Marks (CO2)

3. (a) What is the difference between substitution cipher and transposition cipher ? 10 Marks (CO1)

OR

(b) Explain the OSI security architecture in details. 10 Marks (CO1)

4. (a) Alice and Bob want to establish a secret key using the Diffie-Hellman key exchange protocol. Assuming the value as $n = 11$, $g = 5$, $x = 2$ and $y = 3$, find out the values of A, B and secret key (K1, K2).

10 Marks (CO2)

OR

(b) Distinguish between symmetric and asymmetric key encryption key cryptography. 10 Marks (CO2)

5. (a) Which parameters and design choices determine the actual algorithm of a Feistel cipher ? 10 Marks (CO1, CO2)

OR

(b) State an example of public key cryptography. For the given values trace the sequence of calculation in RSA. P = 7, Q = 13, e = 5, M = 10.

10 Marks (CO1, CO2)

570