No. of Printed Pages : 02 **Roll No. .....**

18BB1011

M. Tech. EXAMINATION, 2020

(Second Semester)

(C Scheme) (Re-appear)

(CSE)

MTCSE548C

NETWORK SECURITY

Time : 2½ *Hours*] [*Maximum Marks :* 75

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

Note : Attempt *Four* questions in all. All questions carry equal marks.

1. (a) Explain the classical encryption techniques with Symmetric cipher and Hill cipher model.

(b) Explain the Diffie-Hellman key exchange algorithm in detail.

2. (a) With the help of suitable example explain, how substitution cipher works ?

(b) Consider a group of 30 people who wish to establish pair-wise secure communications using symmetric-key cryptography. How many keys need to be exchanged in total ? Justify your answer.

3. Design a protocol which achieves mutual authentication and key agreement between two parties using minimum number of exchanges. Assume that both parties share a secret. Also assume that both parties have the ability to compute the cryptographic

hashes but have No support for performing the symmetric key encryption/decryption. Also write the shortcomings of the protocol if any.

4. List the principal advantages of :

(i) Biometric authentication over Cryptographic authentication

(ii) Cryptographic authentication over Biometric authentication

5. List any *five* strategies followed by cyber criminals and hackers to steal your important information. Suggest at least *five* remedial steps to safeguard your crucial data against these stacks.

6. (a) Differentiate between Intrusion prevention system IPs and Intrusion detection system IDs. Explain, how do they work ?

(b) After which message and following which computation in SSL, is the client certain that he/she is talking to authentic server ?

7. Many e-commerce sites use SSL for customer to merchant transactions over the internet. Can you think of any drawbacks in use of SSL for this purpose and ways to counter these drawbacks ?

8. List and explain any *three* biometrics which can be used for identification and authentication.