Enrollment No: ______________________ Exam Seat No:______________________

C.U.SHAH UNIVERSITY

Summer Examination-2022

Subject Name: Cryptography and Network Security

Subject Code: 4TE06CNS1 **Branch: B.Tech (CE)**

Semester: 6 **Date: 05/05/2022** **Time: 02:30 To 05:30** **Marks: 70**

Instructions:

(1) Use of Programmable calculator & any other electronic instrument is prohibited.
(2) Instructions written on main answer book are strictly to be obeyed.
(3) Draw neat diagrams and figures (if necessary) at right places.
(4) Assume suitable data if needed.

Q-1 Attempt the following questions : **(14)**

a) What is threat?
b) List out names of substitution technique.
c) How many rounds are used in des?
d) Define digital certificate.
e) Full form of worm.
f) Difference between symmetric and asymmetric key.
g) Difference between authentication and authorization.
h) Define avalance effect.
i) If sender send plaintext as “security” and key = 4. Find out cipher text.
j) Define one time pad.
k) Define transport mode.
l) List out of real time application of steganography.
m) Define non repudiation.
n) What is the principle of security?

Attempt any four questions from Q-2 to Q-8

Q-2 Attempt all questions

a) Explain Security Attack and Security Services with suitable diagram. **07**
b) Explain Hill Cipher with suitable examples. **07**

Q-3 Attempt all questions

a) Explain Block Cipher Principles with suitable diagram. **07**
b) Explain Single Round of DES Algorithm with suitable diagram **07**

Q-4 Attempt all questions

a) What is dual signature and explain construction of dual signature. **07**

b) Explain different modes of Block cipher. **07**

Q-5 Attempt all questions

a) Briefly explain Diffie-Hellman key exchange. Is it vulnerable to man in the middle attack? Justify. **07**

b) Explain MD5 algorithm. **07**

Q-6 Attempt all questions

a) Why mode of operation is defined? Explain the block cipher modes of operation? **07**

b) P and Q are two prime numbers. P=7, and Q=17. Take public key E=5. If plaintext value is 6, then what will be cipher text value according to RSA algorithm? Explain in detail. **07**

Q-7 Attempt all questions

a) What is SSL? Which security services does it offers? How does it works? **07**

b) What is SSH? How does SSH works? **07**

Q-8 Attempt all questions

a) Differentiate between hashing and encryption. What are the practical applications of hashing? **07**

b) Write a short note on IP security. **07**