Enrollment No: ______________________ **Exam Seat No:**______________________

C.U.SHAH UNIVERSITY

Summer Examination-2019

Subject Name: Cryptography and Network Security

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

Semester: 6 **Date: 30/04/2019** **Time: 10:30 To 01:30** **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) Define Diffusion.
b) List out the requirements of Authentication.
c) Full form of VIRUS.
d) List out Active Attack.
e) Draw a Network Security Model.
f) If Sender send plaintext as “Computer” using Rail Fence Find Out Cipher Text.
g) What is the use of Euclidean Algorithm?
h) Why One time Pad technique is Unbreakable?
i) What is Anomaly Based Intrusion detection?
j) Define Firewall.
k) What are the advantages of IPSec?
l) Difference between Block Cipher and Stream Cipher.
m) What is Steganography?
n) What is the use of X.509?

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

Q-2 **Attempt all questions** **(14)**

a) Describe the term: Authentication, Authorization, Integrity and Non – repudiation and Access Control. **(07)**
b) Discuss Data Encryption Standard with neat sketches. **(07)**

Q-3 Attempt all questions **(14)**

a) Explain Playfair and Encrypt the Message “Surgical Strike” with key “GUJAR” using PLAYFAIR technique. **(07)**
b) Write a Short Note on “International Data Encryption Algorithm”. **(07)**

Q-4 **Attempt all questions** **(14)**

a) P and Q are two prime numbers. P=7, and Q=17. Take public key E=5. If plain text value is 6, then what will be cipher text value according to **(07)**

RSA algorithm? Explain in detail.

b) Explain Blowfish encryption algorithm. **(07)**

Q-5 **Attempt all questions** **(14)**

a) Encrypt the message "meet me Party " using the Hill cipher with the key {9 4} and {5 7} **(07)**

b) Explain Diffie Hellman key exchange algorithm. **(07)**

Q-6 **Attempt all questions** **(14)**

a) Explain Handshake protocol in SSL. **(07)**

b) What problem was Kerberos designed to address? Briefly explain how session key is distributed in Kerberos. **(07)**

Q-7 **Attempt all questions** **(14)**

a) Write a detailed note on Secure Hash Algorithm. **(07)**

b) Explain PGP with its Authentication and Confidentiality Operation. **(07)**

Q-8 **Attempt all questions** **(14)**

a) What is the limitation of Electronic Codebook Mode (ECB)? How it is overcome by Cipher Block Chaining (CBC) mode? Also explain CBC mode in detail **(07)**

b) What is a dual signature? Explain in detail the following transactions supported by SET(secure electronic transaction) **(07)**

(i) Purchase request

(ii) Payment authorization