Enrollment No: _______________________ Exam Seat No:_______________________

C. U. SHAH UNIVERSITY

Winter Examination-2019

Subject Name: Cryptography and Network Security

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

Semester: 6 Date : 16/09/2019 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 Cryptography.
b) What is the difference between an unconditionally secure cipher and a computationally secure cipher?
c) List out the Substution techniques.
d) How many keys are used in triple encryption?
e) Define Diffusion.
f) Write down a full form of HTTP.
g) Define Authentication.
h) Why onetime pad is more secure?
i) What is the use of SET?
j) Define Message Digest.
k) List out Passive Attack.
l) What is the use of Kerberos?
m) Define Integrity.
n) List Out the Application of Security.

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

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

a) Explain OSI Security Architecture. **(07)**
b) Explain columnar transposition Cipher technique. **(07)**

Q-3 **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) Distinguish between Symmetric encryption and Asymmetric encryption using suitable example. **(07)**

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

a) Encrypt the following message using playfair cipher. Message: COMSEC means communications security Keyword: Galois **(07)**

b) Explain single round of DES. **(07)**

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

a) Discuss the possible approaches to attack the RSA algorithm. Also discuss various mathematical and timing attacks for RSA algorithm. **(07)**

b) Explain HMAC algorithm. **(07)**

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

a) Explain SSL architecture. **(07)**

b) What is digital signature? Explain hash code base digital signature. **(07)**

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

a) What are the five principal services provided by PGP? Why does PGP generate signature before applying comparison? **(07)**

b) Explain process of MD5 algorithm. **(07)**

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

a) What are the benefits from IPSec? Mention the most important documents of IPSec along with their significance. **(07)**

b) Briefly explain Diffie Hellman Key exchange with an example **(07)**