Enrollment No: ______________________ Seat No:______________________

C.U.SHAH UNIVERSITY

Summer Examination-2018

Subject Name: Cryptography and Network Security

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

Semester: 6 **Date: 27/04/2018** **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) Define Cryptanalysis.
b) What is the Full Form of VIRUS?
c) List the characteristics of Cryptography.
d) Why Onetime pad technique is Secure?
e) Write differences between Symmetric key and Asymmetric Key.
f) What is One-Way function?
g) How can you prevent a brute force attack on a windows login page?
h) Which protocol does https uses at the transport layer for sending and receiving data?
i) What is Firewall?
j) If receiver receive cipher text as “debit” and k=4 Find Out Plaintext.
k) Name one secure network protocol which can be used instead of telnet to manage a router?
l) What are requirements of authentication?
m) What is the objective of IDEA?
n) What is the purpose of Euclidean Algorithm?

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

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

a) Explain OSI Security Architecture with suitable diagram. **(07)**
b) Explain playfair cipher substitution technique in detail. Find cipher text for the following given key and plaintext. **(07)**
Key = ENGINEERING Plaintext=COMPUTER

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

a) Explain transposition techniques with appropriate example. **(07)**
b) Explain SSL Architecture with suitable diagram. **(07)**

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

a) Explain Single round of DES with suitable diagram. **(07)**

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

Q-5 **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 RSA algorithm? Explain in detail. **(07)**

b) Write a note on “Digital Signature Algorithm”. **(07)**

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

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

b) List and explain various block cipher modes of operation with the help of diagram. **(07)**

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

a) How message authentication code can be used to achieve message authentication and confidentiality? **(07)**

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

Q-8 **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 central authority public key distribution scenario with neat and diagram. **(07)**