Enrollment No: ______________________ Exam Seat No:______________________

C.U.SHAH UNIVERSITY

Summer Examination-2017

Subject Name: Advance Cryptography and Network Security

Subject Code: 5TE02ANS1 **Branch: M.Tech (CE)**

Semester: 2 **Date: 09/05/2017** **Time: 02:00 To 05:00** **Marks: 70**

Instructions:

(1) Use of Programmable calculator and 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.

SECTION – I

Q-1 **Attempt the Following questions** **(07)**

a. Define :Vulnerabilities
b. Why does a network need Security?
c. Specify the four categories of Threat.
d. Define One Way Authentication.
e. List the evaluation criteria defined by NIST for AES.
f. List various types of viruses.
g. Define Direct Digital Signature.

Q-2 **Attempt all questions**

a) Explain the DES encryption algorithm. **(07)**
b) Why mode of Operation is defined? Explain any three Modes of Block cipher. **(07)**

OR

Q-2 **Attempt all questions**

a) Write a note on “Security Attack”. **(07)**
b) In a Public key system using RSA, the cipher text intercepted is C=10 which is sent to the user whose public key is e=5, n=35. What is the plaintext M? **(07)**

Q-3 **Attempt all questions**

a) Explain the general Structure of Secure hash Function. **(07)**
b) Briefly explain the Man in middle Attack Diffie Hellman key exchange. **(07)**

OR

Q-3 **a)** What is Cryptographic checksum? Describe the three situations in which message authentication code is used. **(07)**
b) Explain different key distribution techniques. **(07)**

SECTION – II

Q-4 **Attempt the Following questions** **(07)**

a. Write differences between Symmetric and Asymmetric Cryptography.

b. Define: Tunnel Mode.

c. What are the design parameters of Feistel cipher network?

d. What is the objective of RC5?

e. How do we create Digital Certificate?

f. Define Firewall.

g. Differentiate between unconditionally secure and computationally secure.

Q-5 **Attempt all questions**

a) Explain Digital Signature Algorithm. **(07)**

b) Discuss the Ticket Granting Server Scheme in Kerberos. **(07)**

OR

Q-5 **a)** Explain the general format of PGP message. Assume that Message is going From A to B. Why is segemementation and reassembly function in PGP needed? **(07)**

b) Explain categories of Firewall with suitable diagram. **(07)**

Q-6 **Attempt all questions**

a) Illustrate the overall operation of HMAC. **(07)**

b) What is the meaning of Biometric Authentication? Discuss various type of Biometric Authentication in detail. Provide brief idea: How to achieve finger print authentication? **(07)**

OR

Q-6 **Attempt all Questions**

a) Explain SET Process. **(07)**

b) Discuss the measures to protect the computer systems and networks from the worms and viruses. **(07)**