

Enrollment No: \_\_\_\_\_ Exam Seat No: \_\_\_\_\_

# C.U.SHAH UNIVERSITY

## Summer Examination-2017

**Subject Name: Cryptography and Network Security**

**Subject Code: 4TE06CNS1**

**Branch: B.Tech (CE,IT)**

**Semester: 6**

**Date: 17/04/2017**

**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) Which type of substitution is called monoalphabetic substitution cipher?
  - b) Write the nominal version of RC5.
  - c) Which are parameters required for Random Number Generators?
  - d) Define Virus.
  - e) How many bits are generated in SHA?
  - f) List the function of Tunnel Mode.
  - g) List the Characteristics of Cryptography.
  - h) What is the use of Euclid's Algorithm?
  - i) Define One way Authentication.
  - j) Define Intruder.
  - k) What is the full Form of S/MIME?
  - l) Define Digital Certificate.
  - m) List the name of Block Cipher Algorithms.
  - n) Write the full form of ESP.

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

- Q-2 Attempt all questions (14)**
- a) Explain OSI Security Architecture. (07)
  - b) Explain single round function of DES with suitable diagram. (07)
- Q-3 Attempt all questions (14)**
- a) List various modes of operations of block cipher. Explain any three of them briefly. (07)
  - b) If sender send Plaintext as "Paymore" and key as "CEIT" find out Cipher text using Hill Cipher. (07)



