Dr. S.P. Ghrera

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT
TEST -1 EXAMINATION- Sep 2016
B.Tech(ECE/CSE/IT/BI) VII Semester

COURSE CODE: 10B1WCI735 MAX. MARKS: 15
COURSE NAME: Network Security and Cryptography Techniques
COURSE CREDITS: 3 MAX. TIME: 1 HR

Note: All questions are compulsory. Carrying of mobile phone during examinations will be treated as case of unfair means.

Q.1. [3 Marks. Each part is half mark]

a) List properties of oneway functions?
b) Define confidentiality as a security service.
c) Differentiate between mono- alphabetic and poly- alphabetic ciphers.
d) What is a random number sequence? List its properties.
e) In a symmetric encryption system with n users, how many secret keys are required ?
f) Discuss the location of confidentiality services in a network.

Q.2. [2 marks] How can keys be securely distributed using a KDC?

Q.3. [2 marks] Describe the security mechanisms as given in ITU-T-X800.

Q.4. [2 marks] Discuss the operations in a round of DES.

Q.5. [2 marks] Differentiate between AES and DES.

Q.6. [2 marks] Explain the general structure of RC-4 stream cipher.

Q.7. [2 marks] Describe the CBC and OFB modes of operation of block symmetric ciphers.