D. S P. Ghrera

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -2 EXAMINATION- Oct 2019

B.Tech(ECE/CSE/IT/BI) VII Semester

COURSE CODE: 10B1WCI735 MAX. MARKS: 25

COURSE NAME: Network Security and Cryptography Techniques

COURSE CREDITS: 3 MAX. TIME: 90min

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

Q.1. [5 Marks. Each part is one mark]

a) Define the discrete logarithm problem in Diffie-Hellman algorithm.

b) List advantages of eliptic curve cryptography.

c) Describe a linear congruential generator.

d) Describe advantages and limitations of CBC.

e) What is HASH MAC?

Q.2. [5 marks] Describe the role of MAC and Hash Functions in solving the authentication problem. Also state the properties of these functions.

Q.3. [5 marks] Describe the key management problem of symmetric encryption. How can key management be improved by Key Distribution Centre (KDC) scenario?.

Q.4. [5 marks] What are major functions of public key cryptography? Describe the implementation aspects of RSA algorithm.

Q.5. [5 marks] Describe the Digital Signature Standard and explain the underlying Digital Signature Algorithm.