Prof S P Ghrera.

JAYPEE UNIVERSITY OF INFORMATRION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATION- Dec 2017

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

COURSE CODE: 10B1WCI735 MAX. MARKS: 35

COURSE NAME: Network Security and Cryptography Techniques

COURSE CREDITS: 3 MAX. TIME: 120min

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 half mark]

a) Describe a state in AES.

b) Distinguish between cryptology and cryptanalysis.

c) Define a INTEGRAL DOMAIN in a finite field.

d) How secure is 3-DES?

e) Describe a KDC.

f) What is an arbitrated digital signature?

g) List Block cipher design parameters.

h) List importance of modes of operation for symmetric ciphers.

i) What are the key sizes in AES?

j) What is a CIPHERTEXT only attack?

Q.2. [5 marks] What is the need for a firewall. Describe the configurations of a basic firewall system.

Q.3. [5 marks] What are characteristics of malicious softwares? How can you build a digital immune system?

Q.4. [5 marks] How is intrusion detected? Explain the operation of a Distributed Intrusion Detection System.

Q.5. [5 marks] It is proposed to secure the electronic transactions. Describe the standard security implementations for secure electronic transaction.

Q.6. [5 marks] What is authentication? Describe mechanisms used for authentication.

Q.7. [5 marks] Explain the operation of AES cryptosystem.