Prof S P Ghrera

JAYPEE UNIVERSITY OF INFORMATRION TECHNOLOGY, WAKNAGHAT
TEST -2 EXAMINATION- Oct 2018
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 factorization problem in RSA algorithm.
b) What is importance of random numbers in security applications?
c) What is a revocation list?
d) Explain Needham Schroeder authentication protocol.
e) List properties of hash functions.

Q.2. [4 marks] Describe the SHA-512 standard hashing algorithm.

Q.3. [4 marks] Discribe the X.509 public key certificate. How can public keys be authenticated?.

Q.4. [4 marks] Explain the standards approach to Digital Signatures and their verification.

Q.5. [4 marks] Describe how assymetric crypto systems complement the symmetric crypto systems. Describe step by step, the implementation aspects of Diffie Hellman algorithm.

Q.6. [4 marks] What is a stream cipher. Decscribe the general structure of RC-4 algorithm.