Dr S.P. Ghrera

JAYPEE UNIVERSITY OF INFORMATRION TECHNOLOGY, WAKNAGHAT
TEST -2 EXAMINATION- Oct 2017
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 half mark]

a) List the security services required in a e-mail application.
b) List the information contained in X-509 Certificate.
c) Explain threeway authentication scheme.
d) List and explain the functions of PKI.
e) Explain properties of MAC functions.
f) What is the ideal location for placement of the encryption function?
g) What is traffic analysis?
h) if n users need to communicate securely, how many secret keys will be required?
i) Explain meet in the middle attack.
j) Explain DES-CBC mode of operation.

Q.2. [4 marks] Describe the operation of PGP security and draw the output message format.

Q.3. [4 marks] Discuss the general structure of authentication by KERBEROS system.

Q.4. [4 marks] Explain need for digital signatures. Describe the digital signature standard and explain the digital signature algorithm for generation and verification of digital signatures.

Q.5. [4 marks] Explain two major functions of Public key cryptography. Describe step by step, the implementation aspects of RSA algorithm.

Q.6. [4 marks] What is a HASH function? Describe the WHIRLPOOL algorithm to generate the hash of a given message.