S.P. Ghrera

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT
TEST -1 EXAMINATION- Sep 2017
B.Tech(ECE/CSE/IT/BI) VII Semester/Ph. D.

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. [2.5 Marks. Each part is half mark]

a) How will you test the efficacy of a block symmetric cipher?
b) What is cryptanalytic attack?
c) Define authentication as a security service.
d) List required properties of stream ciphers.
e) Differentiate between confusion and diffusion properties of block symmetric ciphers.

Q.2. [2.5 marks] Discuss in detail the design principles of block symmetric ciphers.

Q.3. [2.5 marks] Describe the security framework as given in ITU-T-X800.

Q.4. [2.5 marks] Discuss the Encryption algorithm of Data Encryption Standard.

Q.5. [2.5 marks] Explain the key expansion algorithm used in Advanced Encryption Standard.

Q.6. [2.5 marks] Explain the general structure of a stream cipher. How is it realized in RC-4?

CI-14, BT PhD