Dr. Ureqa

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT
TEST -1 EXAMINATION- Sep 2018
B.Tech(ECE/CSE/IT/BI/BT) VII Semester

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. [5 Marks. Each part is one mark]

a) Define the avalaunche effect?
b) List design principles of block symmetric ciphers?
c) List modes of operation of block symmetric ciphers and explain the limitations of ECB?
d) Describe the cryptanalysis of monoalphbatic cipher.
e) Compare the brute force attack complexity of 2-DES and 3-DES.

Q.2. [2.5 marks] Describe the security services as given in ITU-T-X800.

Q.3. [2.5 marks] Describe the cryptanalytic attacks based on the amount of information collected by the attacker.

Q.4. [2.5 marks] Discuss the algorithm for round operation in AES.

Q.5. [2.5 marks] Explain the key scheduling algorithm used in DES.