

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -1 EXAMINATION- 2026

B.Tech-VI Semester (CSE)

COURSE CODE (CREDITS): 25B1WCI644 (3)

MAX. MARKS: 15

COURSE NAME: Network Security and Cryptography

COURSE INSTRUCTOR: Dr. Ramesh Narwal

MAX. TIME: 1 Hour

Note: (a) All questions are compulsory.

(b) The candidate is allowed to make Suitable numeric assumptions wherever required for solving problems

(c) Use of calculators is not allowed

Q.No	Question	CO	Marks
Q1	Encrypt CONFIDENTIALDATA using Rail Fence Cipher with 3 rails and explain : a) How ciphertext changes if rails become 4? b) Compare security of Rail Fence vs Caesar Cipher.	2	4
Q2	Discuss Key Management issues in symmetric cryptography. Explain: a) Secret key distribution methods b) How asymmetric cryptography solves the issues arising in symmetric cryptography. c) Man-in-the-middle attacks	1	4
Q3	Encrypt the plaintext INFORMATIONSECURITY using Caesar Cipher with shift value $k = 7$. a) Show alphabet mapping clearly. b) Perform character-wise encryption. c) Write the final ciphertext.	2	4
Q4	Define hash functions. Explain the properties of a secure hash function. Discuss the steps involved in designing cryptographic hash functions.	1	3