

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -1 EXAMINATION- 2026

B.Tech-V Semester (CSE/IT)

COURSE CODE (CREDITS): 25B1WCI533 (2)

MAX. MARKS: 15

COURSE NAME: Fundamentals of Computer and Cyber Security

COURSE INSTRUCTOR: NTS*, PDN.

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 calculator is not allowed

Q.No	Question	CO	Marks
Q1	Using the Caesar cipher with a shift of 3, encrypt the plaintext "CYBERSECURITY". Show the substitution for each letter and give the final ciphertext.	CO-2	3
Q2	A message "INFORMATIONSECURITY" is to be encrypted using a 3-rail Rail Fence cipher. Construct the rail pattern and write the resulting ciphertext.	CO-2	3
Q3	A university needs to securely store students' examination records and also establish a secure shared key for communication between two departments. As the security administrator, provide a comparative analysis of AES, DES, and Diffie-Hellman for these two requirements. Justify each choice and mention one limitation of DES.	CO-2	4
Q4	Explain the CIA triad and give one suitable example of a security control for each component.	CO-1	3
Q5	Differentiate between a threat, vulnerability and exploit. Explain how these three concepts can be related in a real-world cyberattack.	CO-1	2