JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATION- 2025

B.Tech-I Semester (CSE/IT/ECE/CE/BT/BI)

COURSE CODE (CREDITS): 18B1WCI734 (2) MAX. MARKS: 35

COURSE NAME: Cryptography and Network Security

COURSE INSTRUCTORS: Dr. Ramesh Narwal MAX. TIME: 2 Hours

Note: *(a) All questions are compulsory.*

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

Q.No	Question	CO	Marks
Q1	Decrypt the ciphertext "SIRUHWDO FRPPXQLFDWLRQ" which was encrypted using: a) Caesar Cipher shift +3 b) Followed by Rail Fence Cipher depth 2 c) Reverse the process and find the original plaintext.	2	7
Q2	Compare Message Authentication Codes (MAC) and Digital Signatures in terms of security guarantees, implementation complexity, and suitability for distributed cloud environments. Provide conclusion and recommendation.	4	7
Q3	Explain the RSA algorithm with the example below. Given: p = 13, q = 19 Public key exponent e = 5 Find: a) Private key d. b) Encrypt message M = 21. c) Decrypt to obtain the original message.	3	7
Q4	Compare and contrast Substitution, Transposition, and Steganography techniques. Discuss their strengths, weaknesses, and applicability in modern cryptographic systems.	2	7
Q5	A company experiences a data breach where customer financial records are leaked. As a cybersecurity analyst: a) Identify three possible causes using system security concepts (firewalls, IDS, trusted computing). b) Describe actions required under the IT Act 2000/IT Amendment Act 2008. c) Recommend at least three preventive security controls.	1	7