JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -2 EXAMINATION- 2025

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

COURSE CODE (CREDITS): 18B1WCI734 (2) MAX. MARKS: 25

COURSE NAME: Cryptography and Network Security

COURSE INSTRUCTORS: Dr. Ramesh Narwal MAX. TIME: 1 Hour 30 Min

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	Show with an example that two different plaintexts M_1 and M_2 can result in the same ciphertext if the modulus *n* or exponent *e* are chosen incorrectly. Take small values (e.g., n = 33, e = 3) and find M_1, M_2 (with $0 \leq M_1, M_2 < n$) such that $M_1^e \equiv M_2^e$ (mod n). Explain your steps.	2	5
Q2	Discuss the standards used for digital signatures such as: a) DSS (Digital Signature Standard) b) ECDSA (Elliptic Curve Digital Signature Algorithm) Explain how these differ from RSA-based signatures.	4, 6	5
Q3	Explain how AI or LLM-based systems can be used for malware identification. Also mention the challenges in detecting zero-day attacks.	1	5
Q4	Explain the RSA algorithm with below example. Given: p = 11, q = 17 Public key exponent e = 7 Find: a) Private key d. b) Encrypt message M = 19. c) Decrypt to obtain the original message.	2	5
Q5	Differentiate between authentication and authorization. Explain how X.509 Authentication Service ensures user authenticity in secure communication.	5	5