JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -2 EXAMINATIONS- 2026

B.Tech-6th Semester (CSE/IT)

COURSE CODE (CREDITS): 19B1WCI632 (2) MAX MARKS: 25

COURSE NAME: Information Security

COURSE INSTRUCTOR: Dr. Pankaj Dhiman 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

(c) Use of calculator is allowed

Q.No	Question	CO	Marks
Q1	Encrypt the plaintext "INFORMATIONSECURITY" using a Rail Fence cipher with 4 rails. Show the zigzag pattern formation and derive the final ciphertext. Also compute the total number of characters in each rail.	2	3
Q2	Assume two large primes *p=61 and q=53* are selected. Compute *'n'* and Euler's totient function $\phi(n)$. Choose a public exponent *e=17* and determine the corresponding private key *'d'* using the modular inverse. Then encrypt the plaintext message *M=65* using the public key and compute the ciphertext. Show all intermediate modular exponentiation steps.	3	5
Q3	Compare perfectly secure systems with public-key cryptosystems. Explain why public-key systems cannot achieve perfect secrecy. Analyze this limitation using information-theoretic arguments and discuss why computational security is considered sufficient in practice.	3	4
Q4	In a Diffie–Hellman key exchange algorithm setup, *p=47 and g=3*. User *A* selects *a=20*, and *User B* selects *b=30*. Compute the public keys and the shared secret key using modular exponentiation. Show how repeated squaring reduces computational complexity.	3	5
Q5	In symmetric cryptography, secure communication requires prior key exchange. Critically analyze why the key distribution problem is considered the weakest link in secure systems.	4	5
Q6	Consider a global communication system where every user requires perfectly secure communication with every other user. Analyze the scalability challenges of key generation and storage.	4	3