163

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATIONS- 2026

B.Tech-VI Semester (CSE/IT)

COURSE CODE (CREDITS): 25B1WCI644 (3) MAX MARKS: 35

COURSE NAME: Network Security and Cryptography

COURSE INSTRUCTOR: 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

(c) Use of calculator is allowed

Q.No	Question	CO	Marks
Q1	A defense agency sends encrypted instructions to a surveillance drone using the Vigenère Cipher. Plaintext: ATTACKATDAWN Keyword: EAGLE Tasks: a) Construct the Vigenère table mapping for encryption. b) Encrypt the plaintext using the keyword. c) Assume the ciphertext is intercepted. Decrypt it using the same keyword. d) Calculate how many shifts occur for each alphabet during encryption. e) Explain why repeating keywords may weaken security in long military communications.	3	5
Q2	Define Zero-Knowledge Proofs. Explain how: a) Graph Isomorphism protocols b) Sigma Protocols c) Zero Knowledge and NP contribute toward secure authentication without revealing secret information. Include practical applications in modern privacy-preserving systems such as cryptocurrency authentication.	4	5
Q3	Explain the concept of Oblivious Transfer. How does it preserve privacy between sender and receiver? Discuss its applications in secure multiparty computation.	3	5
Q4	Two banking servers establish a secure communication channel using Diffie–Hellman Key Exchange. Given: Prime number p=23, Primitive root g=5 Private keys: Bank Server A chooses a=6, Bank Server B chooses b=15 Perform the following: a) Compute the public keys exchanged between the servers.	2	5

	b) Determine the shared secret key generated by both servers. c) Verify mathematically that both parties obtain the same key. d) If an attacker intercepts only the public keys, explain why computing the shared secret is difficult. e) Discuss one real-life application of Diffie–Hellman in online banking systems.		
Q5	What are Hybrid Ciphers? Explain how symmetric and asymmetric encryption techniques are combined in hybrid cryptographic systems. Illustrate the working using SSL/TLS communication.	3	5
Q6	Discuss the security requirements of Digital Signature Algorithms. Compare authenticity, integrity, and non-repudiation with suitable real-world examples such as e-governance or digital banking systems.	1	5
Q7	A university digitally signs student degree certificates using RSA. Given: p=13, q=19, e=5 Message digest M=9 Tasks: a) Compute: n, $\phi(n)$ b) Find the private signing key d. c) Generate the digital signature using: S=Mdmodn d) Verify the signature using the public key. e) Explain how digital signatures help prevent fake certificates.	4	5