(187)

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -2 EXAMINATIONS- 2026

B.Tech-VI Semester (CSE/IT)

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

COURSE NAME: Network Security and Cryptography

COURSE INSTRUCTOR: 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

(c) Use of calculator is allowed

Q.No	Question	CO	Marks
Q1	Two employees working remotely want to establish a secure communication channel over an insecure network (internet). (a) Explain how Diffie–Hellman Key Exchange helps them generate a shared secret. (b) Illustrate the key exchange process with a diagram. (c) Why is the shared key secure even if values are transmitted publicly?	3	5
Q2	Explain: (a) What is Wiener's attack on RSA? Explain with conditions. (b) Describe lattice-based attacks on RSA.	4	5
Q3	A company wants to send confidential contracts via email where the receiver must verify the sender's identity. (a) Explain how Digital Signature ensures authenticity and integrity in this scenario. (b) Draw a neat diagram showing signing and verification process.	4	5
Q4	Decrypt the ciphertext "KHOORZRUOGVHFXULWB" which was generated by first applying a 4-rail Rail Fence Cipher and then a Caesar Cipher with shift k=3. Show all steps clearly.	3	5
Q5	(a) Using RSA, given p=13, q=19, e=5, find d. (b) Encrypt message M=9 and compute ciphertext.	3	5