JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

Make-up Examination-Nov-2025

COURSE CODE (CREDITS): 18B1WCI734 (2)

COURSE NAME: Cryptography and Network Security MAX. MARKS: 25

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

Note: 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	A message "SECURITY" is encrypted first using a Caesar cipher (shift = 5) and then subjected to a columnar transposition cipher with key "SAFE". a) Derive the final ciphertext. b) Demonstrate decryption by reversing the operations.	1	5
Q2	Explain the process of key management in large organizations implementing PKI (Public Key Infrastructure). Discuss the roles of Registration Authority (RA) and Certificate Authority (CA) in certificate lifecycle management.	3	5
Q3	Given two prime numbers p = 11 and q = 13. a) Compute n and φ(n). Choose e = 7. b) Find the private key d. c) Encrypt the plaintext M = 9 and show the ciphertext C. Note: Use RSA Algorithm to solve this question.	2	5
Q4	Write short notes on: a) Secure Socket Layer (SSL) b) Transport Layer Security (TLS) c) Secure Electronic Transaction (SET) protocol	3	5
Q5	Explain how poor random prime selection during RSA key generation can lead to vulnerabilities. Provide a numerical example showing how two users sharing a common prime can be exploited using the GCD method to recover private keys.	2	5

(90)