

Date 12/5/26

12.00 P.M.

(40)

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATIONS- 2026

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

COURSE CODE (CREDITS): 19B1WCI632 (2)

MAX MARKS: 35

COURSE NAME: Information Security

COURSE INSTRUCTOR: Dr Pankaj Dhiman

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 multinational bank uses RSA encryption to secure online financial transactions between customers and cloud servers. The bank selects two prime numbers $p=61$ and $q=53$, and chooses public exponent $e=17$.	3	5
Q2	A cyber forensic laboratory uses SHA-512 hashes to verify digital evidence collected during investigations. Explain how SHA-512 ensures data integrity. Compare SHA-256 and SHA-512 in terms of: Security strength, Computational complexity, Collision resistance.	5	5
Q3	A smart home system uses 6-digit password authentication for IoT devices. An attacker can attempt 500 passwords per second. Compute the worst-case brute-force attack time. Compute the average expected attack time. Discuss weaknesses of password-only authentication in IoT systems.	6	5
Q4	A blockchain platform must verify whether a large integer is prime before generating cryptographic keys, $n=561$. Apply Fermat's Little Theorem to test primality.	2	5
Q5	Euler's Totient Function and Euler's Theorem are central to RSA cryptography. Explain these concepts and discuss how they contribute to secure encryption and decryption processes.	4	5
Q6	Solve the following system of congruences using the Chinese Remainder Theorem: $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 2 \pmod{7}$. Further, verify the obtained solution.	6	5
Q7	Data breaches involving personal and sensitive information have become increasingly common. Discuss the causes of large-scale data breaches and critically evaluate strategies organizations can adopt to minimize breach impact.	1	5