JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATION- 2024

M.Tech-I Semester (IS)

COURSE CODE (CREDITS): 18M11CI114 (3) MAX. MARKS: 35

COURSE NAME: Cryptography and Information System Security

COURSE INSTRUCTORS: Er. NITIKA 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

Q.No	Question	Marks
Q1	Explain the penalties prescribed under the Information Technology (IT) Act, 2000, for various cybercrimes, focusing on their scope, effectiveness, and alignment with the evolving landscape of digital threats.	[6]
Q2	Examine the role of firewalls in enforcing network security policies, and compare the advantages of hardware versus software-based firewalls in enterprise environments.	[6]
Q3	Explain the working of RSA encryption and decryption processes and solve the numerical problem: Encryption and Decryption: 1) Given n=55, e=3, and a cipher text C=10, find the original message M. 2) Use the private key d=27 to decrypt the message.	[6]
Q4	In a Diffie-Hellman Key Exchange, A and B have chosen prime value q = 17 and primitive root = 5. If A's secret key is 4 and B's secret key is 6, what is the secret key they exchanged?	[6]
Q5	Describe the typical steps involved in establishing a secure session using TLS for web communications.	[6]
Q6	Differentiate between Network-Based Intrusion Detection Systems (NIDS) and Host-Based Intrusion Detection Systems (HIDS).	[5]