JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -2 EXAMINATION- 2024

M.Tech-I Semester

COURSE CODE (CREDITS): 18M11CI114 (3)

MAX. MARKS: 25

COURSE NAME: Cryptography and Information System Security

COURSE INSTRUCTORS: Er. NITIKA MAX. TIME: 1 Hour 30 Minutes

***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	In an RSA cryptosystem, a participant uses two prime numbers p = 3 and q = 11 to generate his public and private keys. If the private key is 7, then how will the text COMPUTER be encrypted using the public key?	[5]
Q2	Discuss the Output Feedback (OFB) mode of block cipher operation. How does it differ from the Cipher Feedback (CFB) mode? Explain with proper diagrams.	[5]
Q3	Explain the working and format of X.509 authentication service and its role in secure communications.	[5]
Q4	Describe the two main modes of IPsec: Transport mode and Tunnel mode. How do they differ in terms of functionality and use cases?	[5]
Q5	What is the purpose of the Multipurpose Internet Mail Extensions protocol, and how does it enhance email communication?	[5]