JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATION- 2024

B.Tech-7th Semester (CSE/IT)

COURSE CODE (CREDITS): 18B1WCI734 (2) MAX. MARKS: 35

COURSE NAME: Cryptography and Network Security

COURSE INSTRUCTORS: 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

Q.No	Question	CO	Marks
Q1	What are the potential future developments or improvements in cryptographic Hash Function Algorithms?	2	5
Q2	A message of 800 bits is processed using SHA-512. How many 1024-bit blocks are needed to hash this message?	2	5
Q3	If a message is signed using Elgamal with a 2048-bit modulus and the signature is composed of two 1024-bit values, what is the total signature size in bytes?	3	5
Q4	In the Kerberos authentication protocol, if the Ticket-Granting Ticket (TGT) is 512 bits long and the session ticket is 256 bits long, what is the total length of the tickets in bits?	4	5
Q5	How does TLS handle the verification of server identity to protect against impersonation attacks?	4	5
Q6	In SSL, if a message is 1,024 bits long and the encryption key is 256 bits, what is the minimum cipher-text size generated during encryption?	4	5
Q7	What are the various categories of security mechanisms, and how do they help in securing information systems?	1	5