JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -2 EXAMINATION- 2024

B. Tech-VI Semester (CSE/IT)

COURSE CODE (CREDITS): 19B1WCI632 (2) MAX. MARKS: 25

COURSE NAME: INFORMATION SECURITY

COURSE INSTRUCTORS: Dr. Nancy Singla MAX. TIME: 1 Hour 30 Minutes

---

Note: *(a) All questions are compulsory.*
(b)Marks are indicated against each question in square brackets.
(c) The candidate is allowed to make Suitable numeric assumptions wherever required for solving problems

---

Q1. (a) Show that the output of each round during decryption is the input to the corresponding round during encryption except for the left-right switch between the two halves for every choice of the Feistel function F. [3+2] [CO3]

(b) Explain the operation in key Expansion process in AES.

Q2. (a) Explain the use of nonces in the following protocol.
Assume that Alice and Bob know a previously agreed secret key K, N_A is the nonce generated by Alice, N_B is the nonce generated by Bob. E(M,K) represents the encryption of M with K. [2+3] [CO2]

(b) Which mode of operation does not involve feedback and is suitable for high-speed network encryption? Describe its encryption and decryption process.

Q3. (a) Describe the steps of Diffie-Hellman key exchange. [2+3] [CO4]

(b) Alice and Bob both use public numbers P = 23, G = 9. Alice selected private key a = 4, and Bob selected b = 3 as the private key. Find the secret key using Diffie-Hellman key exchange algorithm.

Q4. (a) How symmetric key distribution using asymmetric encryption provides confidentiality and authentication? [5+5] [CO3]

(b) What is the role of Public key Certificates in key distribution?