JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST-1 EXAMINATION- 2024

B. Tech-VI Semester (CSE/IT)

COURSE CODE (CREDITS): 19B1WCI632 (2) MAX. MARKS: 15

COURSE NAME: Information Security

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

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) Which aspect of the CIA Triad is violated by a successful Denial of Service (DOS) attack against a company's servers? [2+3] [CO1]

(b) What is the difference between Symmetric and Asymmetric Key Cryptography?

Q2. (a) Explain why a polyalphabetic cipher such as Vigenere is stronger against letter frequency analysis when compared to a monoalphabetic cipher like Caesar. [2+3] [CO2]

(b) What is the largest key size that RC4 can use? Describe RC4 algorithm in detail.

Q3. (a) Encrypt the message 'hey' and obtain the cipher text using a multiplicative cipher considering a key as 3. Also, decrypt the obtained cipher text showing all the involved steps. [3+2] [CO3]

(b) Consider the classic symmetric Playfair cryptographic technique and answer the following:

i. Construct a table for the Playfair Cipher with the keyword EFFECTIVENESS?

ii. Using the constructed table, encrypt the phrase "EXAMFORINFORMATIONSECURITY".