JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -1 EXAMINATION- 2024

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

COURSE CODE(CREDITS): 18B1WCI734 (2) MAX. MARKS: 15

COURSE NAME Cryptography and Network Security

COURSE INSTRUCTORS: Dr. Pankaj Dhiman 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. If the plain text is "**Relational Algebra Expression**" with keyword as "**Component**", find out the cipher text using Play-fair Cipher Algorithm. **[CO-1] [3 Marks]**

Q2. Describe the security service of non-repudiation and its importance. **[CO-1] [2 Marks]**

Q3. Given that DES operates with a 56-bit key and considering the potential for a successful meet-in-the-middle attack on a 2-key variant of DES, explains the theoretical approach to such an attack and estimate the time complexity if each DES operation takes 10 microseconds.

[CO-2] [5 Marks]

Q4. Describe how the Vigenère Cipher improves upon the security of a simple substitution cipher. Provide an example of encrypting the plaintext "**Monoalphabetic Substitution**" using the keyword "**KEY**".

[CO-2] [5 Marks]