

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -1 EXAMINATION- FEB-2023

COURSE CODE (CREDITS): 19B1WCI632 (2)

MAX. MARKS: 15

COURSE NAME: Information Security

COURSE INSTRUCTORS: Dr Pankaj Dhiman

MAX. TIME: 1 Hour

Note: All questions are compulsory. Marks are indicated against each question in square brackets.

Q1. What will be the ciphered text if the string "JAYPEE UNIVERISTY SOLAN" is given as input to the code of Vigenere Cipher with keyword as "LOCK? [CO-1][Marks-2]

Q2. List and briefly define three uses of a Public and Private Key Cryptosystem. [CO-2][Marks-3]

Q3. Using Caesar Cipher to encrypt/decrypt the message "CZECHOSLOVAKIA," and the key (shift) value of this message is 8. [CO-1][Marks-4]

Q4. Consider the Following properties. [CO-2] [Marks-4]

R-i) Closure under multiplication

R-ii) Associativity of multiplication

R-iii) Distributive Law

R-iv) Commutativity of multiplication

R-v) Multiplicative Identity

R-vi) No zero divisors

R-vii) Multiplicative Inverse.

- Abelian group satisfies which of the properties from above options?
- Ring satisfies which of the properties from above options?
- $a.(b.c) = (a.b).c$, Find out the representation from above options?
- Ring is said to be commutative if it also satisfies which of the above property.

Q5. What types of resources are targeted by such DoS attacks? [CO-1] [Marks-2]