JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -2 EXAMINATION- 2023

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

COURSE CODE (CREDITS): 18B1WCI734(2) MAX. MARKS: 25

COURSE NAME: Cryptography and Network Security

COURSE INSTRUCTORS: Dr. Pankaj Dhiman & Dr. Prateek Thakral MAX. TIME: 1 Hour 30 Min

---

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. Discuss the strengths and weaknesses of the Data Encryption Standard (DES) with reference to a specific example. [CO-2] [4 Marks]

Q2. Differentiate between security services and security mechanisms. Provide examples of security services and mechanisms and explain how they contribute to overall computer security. [CO-1] [4 Marks]

Q3. Describe the principles of pseudorandom number generation and discuss the importance of using high-quality pseudorandom number generators in cryptographic applications.

[CO-3] [4 Marks]

Q4. Describe the complete structure of Advance Encryption Standard (AES) in detail.

[CO-3] [4 Marks]

Q5. Find out whether the number is prime or composite number using Fermat Theorem $2^{11} - 1 = 2047$. [CO-3] [4 Marks]

Q6. Consider the following pairs of integers:

a) m=48 and n=18 b) m=105 and n=84 c) m=72 and n=60

Apply the Euclidean Algorithm to find the greatest common divisor (GCD) of each pair. Show the steps of the algorithm and determine the GCD. [CO-3] [5 Marks]