JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATION- 2023

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

COURSE CODE (CREDITS): 18B1WCI734(2) MAX. MARKS: 35

COURSE NAME: Cryptography and Network Security

COURSE INSTRUCTORS: Dr. Pankaj Dhiman & Mr. Prateek Thakral

MAX. TIME: 2 Hours

***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. Explain the process of obtaining a user's certificate in X.509. Also explain the process of forward certificates and reverse certificates. **[CO-6][5 Marks]**

Q2. Apply Chinese Remainder Theorem to find x such that: x ≡ 1 (mod 5), x ≡ 2 (mod 7), x ≡ 3 (mod 9) & x ≡ 4 (mod 11). **[CO-2][4 Marks]**

Q3.Using Fermat's Little Theorem, find the modular inverse of 17 modulo 23. **[CO-2][4 Marks]**

Q4. Encrypt the text "FOUR" using Hill Cipher with the key $\begin{bmatrix} 5 & 8 \\ 7 & 9 \end{bmatrix}$? **[CO-1][4 Marks]**

Q5. Describe the steps in finding the message digest using SHA-512 algorithm. What is the order of finding two messages having the same message digest? **[CO-4][5 Marks]**

Q6. Find the secret key shared between user *A* and user *B* using Diffie-Hellman algorithm for the variables Q=353, α (primitive root) = 3, X_A=45, X_B =50. **[CO-3][5 Marks]**

Q7. List and explain the sequence of steps followed in Message Digest (MD5) algorithm

[CO-4][3 Marks]

Q8. Explain the concept of a digital signature and how it enhances the security of authentication messages in systems using asymmetric encryption. **[CO-5][5 Marks]**