JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -2 EXAMINATION- APRIL-2023

COURSE CODE (CREDITS): 19B1WCI632 (2) MAX. MARK: 25

COURSE NAME: INFORMATION SECURITY

COURSE INSTRUCTORS: Dr. Pankaj Dhiman MAX. TIME: 1 Hour 30 Minutes

---

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

Q1. Find out the Cipher-text of the given Plain-text "ALPHABET", using Hill-Cipher for the given key $=\begin{bmatrix}2 & 3\\ 3 & 6\end{bmatrix}$. **[CO-1][Marks-4]**

Q2. In a RSA Algorithm, *User A* uses two Prime Numbers $p = 17$ *and* $q = 23$ to generate Public Key and Private Key. If the public key of *User A* is 40, then the Private Key of *User A* is.

[CO-3][Marks-4]

Q3. Find out whether the number is prime or composite number using Fermat Theorem $2^{11} - 1 = 2047$. **[CO-2][Marks-2]**

Q4. Using Chinese Remainder Theorem $x \equiv 6 \pmod{11}$, $x \equiv 13 \pmod{16}$, $x \equiv 9 \pmod{21}$, $x \equiv 19 \pmod{25}$, find the value X. **[CO-2][Marks-5]**

Q5. What are the security benefits and various types of Public Key Cryptography?

[CO-3][Marks-3]

Q6. What will be the Cipher-text if the Plain-Text "OXFORDUNIVERSITY" is given as input to the code of Playfair Ciphering Technique with keyword as"LETTERSPAIRS. **[CO1][Marks-3]**

Q7. Consider a Diffie-Hellman key exchange protocol with a common prime $q=13$, and a primitive root $\alpha=4$.

a) User A has public key $Y_A=7$, find User A private key X_A.

b) User B has public key $Y_B=11$, find is shared secret key K. **[CO-3][Marks-4]**