JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATION- 2023

B.Tech-IV/VI/VIII Semester (CSE/IT/ECE/CE)

COURSE CODE (CREDITS): 19B1WCI632 (2) MAX. MARKS: 35

COURSE NAME: Information Security

COURSE INSTRUCTORS: Dr Pankaj Dhiman MAX. TIME: 2 Hours

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

Q1. What will be the ciphered text if the string "Mathematical Technique" is given as input to the code of Vigenere Cipher with keyword as "ABOVE". [CO-1][Marks-3]

Q2. What are the advantages of steganography comparing with cryptography [CO-6][Marks-3]

Q3. Suppose S_1 is the Shift Cipher (with equi-probable keys) and S_2 is the Shift Cipher where keys are chosen with respect to some probability distribution PK (which not is equi-probable). Prove that $S_1 \times S_2 = S_1$. [CO-2][Marks-5]

Q4. Explain the approaches for Digital Signatures based on Public Key Encryption.

[CO-6][Marks-2]

Q5. Consider the following: Plaintext: "Message Authentication Codes", Secret key: "NETWORK", what is the corresponding cipher text using Play fair cipher method

[CO-1][Marks-4]

Q6. What is the property in the DES construction which helps to increase the key length by performing such composition? [CO-4][Marks-5]

Q7. In Elgamal cryptosystem, given the prime $p=31$. Encrypt the message "HELLO"; use *00* to *25* for encoding. The value of C_2 for character '*L*' is [CO-5][Marks-5]

Q8. Using Chinese Reminder Theorem $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, find the value X.

[CO-5][Marks-5]

Q9. In an RSA system, the public key of a given user is $e=31$, $n=3599$. What is the private key of this user. [CO-4][Marks-3]