JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST-1 EXAMINATION-FEBRUARY 2025

B.Tech- VI th Semester

Course Code: 19B1WCI632 Max Marks: 15

Course Name: INFORMATION SECURITY

Course Credits: 02

Course Instructor: Dr. Praveen Modi Max Time: 01:00 Hours

Note: *All questions are compulsory. Marks are indicated against each question in square brackets. Write the answer of the question belonging to the same part in the same order.*

Q1.Identify which security mechanism is required for the security attack? Mark 'Yes or No' (CO1) [2]

	Security Attacks					
Security Services	Release of message Contents	Traffic Analysis	Masquerades	Replay	Message Modification	Denial of Services
Encipherement						
Digital Signature						
Authentication Exchange						
Data Integrity						

Q2. Compute the values of N1 and N2 to find the GCD between two numbers using Euclidean algorithm? (CO1) [2]

GCD	A	B
N1	24140	16762
N2	-12575	4052

Q3. Find the plaintext letters for the cipher text [7 22] and key K = $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ using Hill Ciphering method? Consider the assignment as A = 0, B =1 …Z = 25. (CO2) [5]

Q4. If P is prime, then Ø (P^n) = P^n - P^{n-1}. Find the Euler totient function value Ø(n) for following numbers? (CO1) [2]

(i) 27 (ii) 41 (iii) 231 (iv) 440

Q5. Encrypt the message with Key = "MONARCHY" using Play fair Cipher method? Ignore any blank space in message.

Message = I AM IMPROVING (CO1) [4]

Q6. (i) Using the Fermat theorem, find the value of 7^{1013} mod 93? (CO2) [2]

(ii) Using the Euler's theorem, find the value of 9^{101} mod 10?