JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -1 EXAMINATION- 2026

B.Tech-III Semester (CSE/IT)

COURSE CODE (CREDITS): 24B11CI312 (3) MAX. MARKS: 15

COURSE NAME: Information and Cyber Security Foundation

COURSE INSTRUCTOR: Mr. Suraj Kumar MAX. TIME: 1 Hour

Note: *(a) All questions are compulsory.*

(b) The candidate is allowed to make Suitable numeric assumptions wherever required for solving problems

(c) Use of calculator is not allowed

Q.No	Question	CO	Marks
Q1	A university's examination portal is hosted on a public-facing web server. During an examination, an attacker exploits a weakness in the server and gains unauthorized access. The attacker then: • Reads confidential student examination records. • Changes the marks of several students. • Makes the examination portal unavailable for two hours. Identify the CIA Triad component(s) affected by each action. For each case, explain your reasoning and suggest one appropriate security mechanism.	2	3
Q2	A university has the following network: • A public-facing web server and mail server • A database server containing student records • Student, Faculty, and Administrator VLANs • A firewall at the Internet gateway • An IDS monitoring the internal network The web server is currently placed in the same network as the database server. During an attack, an attacker exploits an unpatched web-server service and gains access to the server. From there, the attacker attempts to access the database and later sends malicious traffic toward the Administrator VLAN. The IDS generates an alert, but the attacker is not automatically blocked.	2	3

UNIT TEST-1 EXAMINATION-AUG-2026

163

	Analyze the incident and answer the following: (a) Identify the initial vulnerability, attack surface, and attack involved. (b) Identify the CIA Triad properties that could be affected if the attacker successfully accesses and modifies the database. (c) Propose a three-layer defense-in-depth solution using appropriate controls such as DMZ, network segmentation, firewall, IDS/IPS, or access control, and explain how each layer would limit the attack.		
Q3	Using the Hill Cipher, consider the following key matrix: Using the convention A = 0, B = 1, ..., Z = 25, encrypt the plaintext: "HELP" Show all necessary steps, including: 1. Division of the plaintext into digraphs. 2. Conversion of each digraph into numerical vectors. 3. Matrix multiplication modulo 26. 4. The final ciphertext.	4	3
Q4	Using the Playfair Cipher, construct a 5 × 5 key matrix using the keyword "MONARCHY". Use the convention I/J in the same cell. Encrypt the plaintext "INFORMATIONSECURITY". Show the complete 5 × 5 key matrix, prepare the plaintext into digraphs with appropriate insertion of **X** where required, show the encryption of each digraph using the appropriate Playfair rule, and determine the final ciphertext.	4	3
Q5	A secret agent intercepts the one-word ciphertext "KHOS", encrypted using a Caesar cipher with a forward shift of exactly 3 positions ($k = 3$). (1) State whether the ciphertext should be shifted forward or backward to decrypt it. (2) Decrypt "KHOS" by reversing the 3-position shift to obtain the original plaintext. (3) Determine what the plaintext letter "Z" becomes when encrypted using the same forward shift of 3.	4	3

FINAL EXAMINATION AUG 2026