Seat. No. _____

KADI SARVA VISHWAVIDYALAYA

BE SEMESTER-VI (Information Technology) Examination April- 2025

Subject Name: Information Security
Subject Code: IT-602-N

Date: 7/4/2025 **Time: 12:30 PM to 3:30 PM** **Total Marks: 70**

Instructions:
1. Answer each section in separate answer sheet.
2. All questions are Compulsory.
3. Indicate clearly, the option you attempt along with its respective question number.
4. Use the last page of main supplementary of rough work.

Section-I

Q-1 **(A)** Define Security attack, Security Mechanism, Security Services. [5]

(B) Encrypt the plaintext "attack", using Hill cipher for the given key $\begin{bmatrix} 2 & 3 \\ 3 & 6 \end{bmatrix}$ [5]

(C) What is Steganography? Explain its features. [5]

OR

(C) Convert the following plain text message **PT= hide money** into cipher text with key **key=tutorials** by using play fair cipher technique? [5]

Q-2 **(A)** Write note on Intrusion Detection System (IDS). [5]

(B) Explain different types of Network layer attacks. [5]

OR

Q-2 **(A)** Write a note on IP spoofing and intruders. [5]

(B) Write a short note on firewall design principles and types of firewalls. [5]

Q-3 **(A)** Explain Diffie –hellman key exchange algorithm. [5]

(B) Explain Basic security protocol. Explain any two. [5]

OR

Q-3 **(A)** Explain Blind Signatures in detail. [5]

(B) What is Zero-Knowledge Proofs? Explain working methodology of it. [5]

Section-II

Q-4 **(A)** Find GCD (1970, 1066) using Euclid's algorithm. [5]

(B) Explain overall structure of AES Encryption in brief. [5]

(C) For each of the following equations, find an integer x that satisfies the equation. [5]

(1) $5x \equiv 4 (\text{mod } 3)$.

(2) $7x \equiv 6 (\text{mod } 5)$.

OR

(C) Define Euler's theorem and its application. [5]

Q-5 **(A)** Perform encryption and decryption using the RSA algorithm for p=5; q=11; e=3; M=9 [5]

(B) Explain DES algorithm with proper Diagram. [5]

OR

Q-5 **(A)** Differentiate between Symmetric and Asymmetric Key Encryption. [5]

(B) Explain Fermat Theorem with example. [5]

Q-6 **(A)** Describe three Authentication Functions in detail. [5]

(B) Give various Hash Functions. Discuss secure hash algorithm with suitable examples [5]

OR

Q-6 **(A)** Explain MD5-Message Digest Algorithm in detail. [5]

(B) What is Digital Signature? Explain with example. [5]