KADI SARVA VISHWAVIDYALAYA

B.E. Semester VI (NEW) EXAMINATION (APRIL – 2025)

Subject Code: CE603-N **Subject Name: Cryptography And Network Security**
Date: 07/04/2025 **Time: 12:30 p.m. to 03:30 p.m.** **Total Marks: 70 Marks**

Instructions:
1. **All questions are compulsory.**
2. **Figures to the right indicate full marks.**
3. **Use of scientific calculator is permitted.**
4. **Indicate clearly, the options you attempt along with its respective question number.**
5. **Use the last page of main supplementary for rough work.**

Section-I

Q:1 **(A)** Explain Steganography in detail with example. **[5]**

(B) Explain Playfair cipher with its rule to encrypt the message and also encrypt the **Message: Indian Cricket Team** with **Keyword: Champions Trophy** **[5]**

(C) Explain single round function of DES algorithm in detail with suitable diagram. **[5]**

OR

(C) List all the block cipher modes of operation and explain CBC (Cipher Block Chaining) and OFB (Output Feedback) modes of operation with proper diagram. **[5]**

Q:2 **(A)** Explain AES structure in detail. **[5]**

(B) Find the multiplicative inverse of 50 in Z_{71} using Extended Euclidean Algorithm. **[5]**

OR

Q:2 **(A)** Differentiate Conventional Encryption and Public Key Encryption. **[5]**

(B) Prove Euler's theorem holds true for a = 11 & n = 33 and a = 2 & n = 5? **[5]**

Q:3 **(A)** Perform encryption and decryption using RSA algorithm: **[5]**

a. P=7, Q=11, e=17 and M=8 **b.** P=3, Q=11, e=7 and M=14

(B) Find GCD of following using Euclid's algorithm. **[5]**

a. (16762, 24140) **b.** (2947, 3997)

OR

Q:3 **(A)** Explain Elliptic Curve Cryptography (ECC) with diagram. **[5]**

(B) Find Euler's Totient for following. **[5]**

a. $\Phi(5)$ **b.** $\Phi(35)$ **c.** $\Phi(11)$ **d.** $\Phi(28)$ **e.** $\Phi(43)$

Section II

Q:4 (A) What are the requirements of Digital Signature? Discuss Digital Signature Standard in detail. [5]

(B) Differentiate Message Authentication Code and Hash function. [5]

(C) Explain side channel attack in detail. [5]

OR

(C) Explain MD5 algorithm in brief. [5]

Q:5 (A) Explain Time-Memory Trade-off Attack in detail. [5]

(B) Enlist and explain roles of various servers are used in Kerberos. Explain through diagram, how Kerberos can communication with other administrative domains for providing trusted services to the clients. [5]

OR

Q:5 (A) Write a note on X.509 certificate format. [5]

(B) Describe the functions provided by S/MIME. [5]

Q:6 (A) Discuss SSL architecture with neat diagram in brief. [5]

(B) Differentiate Identity based Encryption and Attribute based Encryption. [5]

OR

Q:6 (A) Explain PGP protocol in detail. [5]

(B) Discuss the following terms in detail. [5]

a. Quantum cryptography **b.** Bitcoin and Cryptocurrency