Seat No. □□□□□□□□

KADI SARVA VISHWAVIDYALAYA

B.E. Semester-VI Examination (April-2022)

SUBJECT CODE: CE603-N **SUBJECT NAME: Cryptography and Network Security**
DATE: 12/04/2022 **TIME: 12.30 P.M. to 3:30 P.M.** **TOTAL MARKS: 70**

Instructions:
1. Answer each section in separate Answer Sheet.
2. All questions are compulsory.
3. Indicate clearly, the options you attempted along with its respective question number.
4. Use the last page of main supplementary for rough work.

SECTION – 1

Q-1. **A)** Explain Security Services in detail. **[5]**

B) Explain Euler's Theorem in detail. **[5]**

C) Explain Feistel Cipher Structure. **[5]**

OR

C) Explain Steganography in detail. **[5]**

Q-2. **A)** Describe SubBytes, ShiftRows, MixColumns and AddRoundKey in AES (Advanced Encryption standard). **[5]**

B) Explain Electronic code Book block cipher mode of operation in detail with figure. **[5]**

OR

Q-2. **A)** Explain single round function of DES with suitable diagram. **[5]**

B) Explain Cipher feedback mode of operation in detail with figure. **[5]**

Q-3. **A)** Find the multiplicative inverse of following using extended Euclidean algorithm. **[5]**
(1) 50 mod 71
(2) 43 mod 64

B) Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root α = 7. **[5]**
a.) If user A has private key XA = 5,
what is A's public key YA?
b.) If user B has private key XB = 12, what is B's
public key YB?
c.) What is the shared secret key?

OR

Q-3. **A)** Encrypt the following message using playfair cipher. **[5]**

P.T.O

Message: INSTRUMENTS Keyword: MONARCHY

B) Perform encryption and decryption using the RSA algorithm for p=3; q=11; e=7; M=5 [5]

SECTION – 2

Q-4. A) Differentiate Conventional Encryption vs. Public-Key Encryption. [5]

B) Explain X.509 Certificate Format. [5]

C) Explain Triple DES with two keys. [5]

OR

C) Explain SHA- Secure Hash Algorithm. [5]

Q-5. A) Write a short note on Kerberos. [5]

B) Explain Message Authentication Code in detail. [5]

OR

Q-5. A) Explain Digital Signature Standard. [5]

B) Describe the desired properties of a Hash function. [5]

Q-6. A) What is Blockchain? Explain advantages and Disadvantages of Blockchain. [5]

B) Explain IP Security Architecture. [5]

OR

Q-6. A) What is Transport Layer Security? Explain in detail. [5]

B) Explain Attribute-based encryption. [5]

********BEST OF LUCK********