Enrolment No./Seat No_______________

GUJARAT TECHNOLOGICAL UNIVERSITY

BE- SEMESTER–VI (NEW) EXAMINATION – WINTER 2024

Subject Code:3161606 **Date:25-11-2024**

Subject Name:Cryptography and Network security

Time:02:30 PM TO 05:00 PM **Total Marks:70**

Instructions:

1. **Attempt all questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**
4. **Simple and non-programmable scientific calculators are allowed.**

Q.1 **(a)** Summarize the difference between Substitution and Transposition techniques. **03**

(b) Differentiate the cipher properties of confusion and diffusion. **04**

(c) Perform encryption using Hill Cipher for the following. Message: PEN and Key: ACTIVATED **07**

Q.2 **(a)** Compare all the features of stream and block ciphers. **03**

(b) What are the merits of Output-Feedback (OFB) as compared to Cipher Feedback (CFB)? **04**

(c) Describe Triple DES and its applications. **07**

OR

(c) Describe in detail the key generation in AES algorithm and its expansion format. **07**

Q.3 **(a)** Compare public key and private key. **03**

(b) Using CRT(Chinese Remainder Theorem), solve for x for the following: **04**
$x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 5$; $x \equiv 2 \pmod 7$

(c) Users Alice and Bob use the Diffie-Hellman key exchange technique with a common prime $q = 83$ and a primitive root $\alpha = 5$. If Alice has a private key $X_A = 6$, what is Alice's public key Y_A? **07**

OR

Q.3 **(a)** Define Euler's totient function. **03**

(b) Find 11^{13} mod 53 using modular exponentiation. **04**

(c) Perform encryption and decryption using RSA algorithm for the following: p=7 q=11, e=7, M=9. **07**

Q.4 **(a)** Explain the significance of signature function in DigitalSignature Standard (DSS) approach. **03**

(b) Identify 4 requirements defined by Kerberos. **04**

(c) Illustrate the security of hash functions and MACs. **07**

OR

Q.4 **(a)** Define: message digest. **03**

(b) What is Message Authentication code? Explain its functions and basic uses. **04**

(c) Explain the format of the X.509 certificate. **07**

Q.5 **(a)** Demonstrate the working SSL Record Protocol. **03**

(b) Explain Schnorr Digital Signature Scheme **04**

(c) Explain key distribution process using Key Distribution Center (KDC). **07**

OR

Q.5 **(a)** What is HTTPS? How it works? **03**

(b) Describe Elgamal Digital Signature Scheme. **04**

(c) Explain Importance of SSL Handshake Protocol with detailed explanation. **07**

****