Seat No.: ________ Enrolment No.___________

# GUJARAT TECHNOLOGICAL UNIVERSITY

**BE - SEMESTER–VI (NEW) EXAMINATION – WINTER 2023**

**Subject Code:3161606** **Date:05-12-2023**

**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.**

**Marks**

**Q.1** **(a)** Explain the following terms in brief: **03**

i) Data Integrity

ii) Cryptanalysis

iii) Relative Prime Number

**(b)** Explain different Types of Active attacks in details. **04**

**(c)** List and briefly define categories of security mechanisms. **07**

**Q.2** **(a)** Encrypt the message "Information" using the Hill Cipher with the key- $\begin{bmatrix} 3 & 2 \\ 5 & 7 \end{bmatrix}$ **03**

**(b)** Construct a Play fair matrix with the key "Constitution". And encrypt the message "The document contains the fundamental rights of the people". **04**

**(c)** Explain the steps in the various rounds of AES. **07**

**OR**

**(c)** Explain single round of DES algorithm. **07**

**Q.3** **(a)** Explain Rail-fence technique with example. **03**

**(b)** Differentiate Following: **04**

i) Stream cipher and block cipher.

ii) Active attack and Passive attack

**(c)** List and Explain various modes of operations of block cipher in details. **07**

**OR**

**Q.3** **(a)** Ramesh meets Suresh and says "Xayyogt lomnzkx pkzy gxk ut znk gzzgiq." If he is using Caesar Cipher, what does he want to convey? **03**

**(b)** Explain the distribution process of KDC with suitable diagram. **04**

**(c)** Explain SHA-1 Algorithm. **07**

**Q.4** **(a)** Define MAC? Explain HMAC in details. **03**

**(b)** In RSA, The plain text is M=8 which is sent to the user whose public key is e=17, and the value of two random no. p=7 and q=11 then What is the cipher text C? **04**

**(c)** Briefly explain the Diffie-Hellman key exchange with example. **07**

**OR**

**Q.4** **(a)** Explain the concept of Arbitrated digital signature. **03**

**(b)** User A & B exchange the key using Diffie Hellman algorithm Assume public numbers P=23 G=9 and private values X=4 Y=3 respectively. Find the Public Value R1,R2 and key K of user A and B. **04**

| | | | |
|---|---|---|---|
| | **(c)** | Explain possible approaches to attacking the RSA algorithm. | **07** |
| **Q.5** | **(a)** | Define Man in the middle attack. | **03** |
| | **(b)** | Explain various fields in X.509 certificate format. | **04** |
| | **(c)** | Explain Kerberos Protocol with Suitable Diagram | **07** |

**OR**

| | | | |
|---|---|---|---|
| **Q.5** | **(a)** | What is the purpose of HTTPS? | **03** |
| | **(b)** | Explain Four different approaches of distribution of Public Keys. | **04** |
| | **(c)** | Explain SSL handshake protocol. | **07** |

**************