Seat No.: ________ Enrolment No.___________

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII (NEW) EXAMINATION – SUMMER 2022

Subject Code:3170720 Date:10/06/2022

Subject Name:Information 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)** Define the following terms: **03**
(i) Security Attack (ii) Security Services (iii) Security Mechanism

(b) Answer following questions. **04**
(i) 15 parties want to exchange messages securely using symmetric key encryption algorithm. The number of distinct key values required will be_________.
(ii) 15 parties want to exchange messages securely using asymmetric key encryption algorithm. The number of distinct key values required will be_________.
(iii) Total number of s-box used in DES is_________.
(iv) How many AES rounds are required for 128-bit key size?

(c) List and explain various types of attacks on encrypted message. **07**

Q.2 **(a)** Encrypt the message “CORONA” using Hill Cipher with key $\begin{bmatrix}9 & 4\\5 & 7\end{bmatrix}$ **03**

(b) Discuss different techniques for public-key distribution. **04**

(c) Elaborate DES encryption with neat sketches. **07**

OR

(c) Elaborate AES encryption with neat sketches. **07**

Q.3 **(a)** Discuss Meet-in-the-Middle Attack. **03**

(b) Discuss Cipher Block Chaining (CBC) modes of operation with the help of diagram. **04**

(c) What is KDC? With the help of diagram explain how KDC do key distribution. **07**

OR

Q.3 **(a)** Discuss Man-in-the-Middle Attack. **03**

(b) Discuss Cipher Feedback (CFB) block cipher modes of operation with the help of diagram. **04**

(c) Discuss briefly the working of KERBEROS authentication protocol. **07**

Q.4 **(a)** Decipher the message ”KBSTZPEGBWNDGQHWQWC” Using Vigenere cipher with key “confidential” **03**

(b) Explain the following properties of hash function **04**
(i) One way property
(ii) Weak collision resistance

(c) P and Q are two prime numbers. P=17, and Q=31. Take public key E=7. If plain text value is 2, then what will be the private key and cipher text value according to RSA algorithm? Explain in detail. **07**

OR

Q.4 **(a)** Encrypt the message “WE ARE DISCOVERED FLEE AT ONCE” using Rail fence cipher with rail = 3 **03**

(b) Explain the triple DES scheme with two keys and write about proposed attacks on 3DES **04**

(c) For Diffie-Hellman algorithm, two publically known numbers are prime number 23 and primitive root (g) of it is 9. A selects the random integer 4 and B selects 3. Compute the public key of A and B. Also compute common secret key. **07**

Q.5 **(a)** Define the following terms: **03**
(i) Cryptography (ii) Cryptanalysis (iii) Brute-force attack

(b) Discuss SSL protocol stack. **04**

(c) Discuss Secure Hash Algorithm (SHA) **07**

OR

Q.5 **(a)** Illustrate variety of ways in which MAC code can be used to provide Message authentication. **03**

(b) Consider ElGamal cryptosystem in Z_{17} with generator 6. If the message is 13 and the randomness chosen is 10, then find the ciphertext computed using the public key 7. **04**

(c) Discuss X.509 authentication service. **07**

****