Seat No.: ________ Enrolment No.___________

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VI (NEW) EXAMINATION – SUMMER 2023

Subject Code:3161606 Date:06-07-2023

Subject Name:Cryptography and Network security

Time:10:30 AM TO 01:00 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)**	List and define the three security goals.	**03**
	(b)	Distinguish between passive and active security attacks.	**04**
	(c)	Define Cryptography and Cryptanalysis. Draw and explain conventional cryptosystem.	**07**
Q.2	**(a)**	Define (i) group (ii) Ring (iii) Field	**03**
	(b)	Distinguish between (i) substitution cipher and transposition cipher (ii) monoalphabetic cipher and polyalphabetic cipher	**04**
	(c)	Discuss ECB & CBC block cipher modes of operation with the help of diagram.	**07**
		OR	
	(c)	Discuss Cipher Feedback & Output Feedback block cipher modes of operation with the help of diagram.	**07**
Q.3	**(a)**	Encrypt the Message “BALLOON” with key $\begin{bmatrix}3 & 2\\5 & 7\end{bmatrix}$ using Hill Cipher.	**03**
	(b)	Find GCD of 1970 and 1066 using Euclid algorithm.	**04**
	(c)	Explain single round function of DES with suitable diagram.	**07**
		OR	
Q.3	**(a)**	Consider a mono-alphabetic cipher with the following key value: (A B C D I J K L E F G H M N O P U V W X Q R S T Y Z) What will be the encrypted form of the message “W I N D O W”?	**03**
	(b)	Using Extended Euclidean algorithm find multiplicative inverse of 49 in Z_{37}.	**04**
	(c)	Explain Kerberos in detail.	**07**
Q.4	**(a)**	What is the purpose of S-boxes in DES? Explain the avalanche effect.	**03**
	(b)	What is cryptographic checksum or message authentication code? Describe the three situations in which message authentication code is Used.	**04**
	(c)	Discuss RSA algorithm. Also Find d and cipher text C using P=3 q=11 e=7 and m=10.	**07**
		OR	
Q.4	**(a)**	Construct a playfair key matrix with the key “injection”.	**03**
	(b)	What characteristics are needed in secure hash function? Explain the concept of Simple hash function.	**04**
	(c)	Discuss Diffie-Hellman key exchange algorithm with example.	**07**

Q.5 **(a)** Explain Direct Digital signature. **03**

(b) Discuss four general categories of schemes for the distribution of public keys. **04**

(c) Discuss X.509 Certificates. **07**

OR

Q.5 **(a)** Explain Arbitrated Digital signature. **03**

(b) Write the key distribution scenario in which each user shares a unique master key with key distribution center. **04**

(c) Write a note on Secure Socket Layer. **07**

****