Enrolment No./Seat No_____

GUJARAT TECHNOLOGICAL UNIVERSITY

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

Subject Code: 3161606 Date:17-05-2024

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)**	Define the following aspects of security. (i)Security Attack (ii) Security Mechanism (iii) Security Service	**03**
	(b)	Differentiate passive attack from active attack with example.	**04**
	(c)	Encrypt the text "SWARAJ IS MY BIRTH RIGHT" using play fair cipher using the keyword MONARCHY.	**07**
Q.2	**(a)**	Find gcd(1970, 1066) using Euclidean algorithm	**03**
	(b)	Discuss the properties that are satisfied by Groups, Rings and Fields.	**04**
	(c)	Explain Confidentiality, Integrity and Availability as basic security principles with example.	**07**
		OR	
	(c)	Demonstrate encryption using Hill Cipher with suitable example.	**07**
Q.3	**(a)**	What are the differences between diffusion and confusion?	**03**
	(b)	Convert the Given Text "CRYPTOGRAPHY" into cipher text using Rail fence cipher.	**04**
	(c)	What are the different modes of operation in Block Cipher? Explain any three of them with diagram.	**07**
		OR	
Q.3	**(a)**	Identify the any three possible threats for RSA algorithm and list their counter measures.	**03**
	(b)	Explain the Key Generation process of DES algorithm using example.	**04**
	(c)	Elaborate double DES process. What are disadvantages of double DES	**07**
Q.4	**(a)**	Why is asymmetric cryptography bad for huge data? Specify the reasons.	**03**
	(b)	Explain the key management of public key encryption in detail?	**04**
	(c)	Perform encryption and decryption using RSA Algorithm for the following. P=17; q=11; e=7; M=88.	**07**
		OR	
Q.4	**(a)**	What is the difference between public key and private key cryptosystem?	**03**
	(b)	Explain Digital signature with example.	**04**

	(c)	Demonstrate the Substitute byte transformation in AES with example.	**07**
Q.5	**(a)**	Describe importance of the SSL Architecture.	**03**
	(b)	Define Kerberos. Derive the Kerberos procedure, If the client C wants to communicate server S.	**04**
	(c)	Analyze and explain Diffie Hellman key exchange algorithm with its merits and demerits.	**07**

OR

Q.5	**(a)**	List any two applications of X.509 Certificate.	**03**
	(b)	Explain about MD5 algorithm in detail.	**04**
	(c)	Compare and Draw diagram of RSA Approach and DSS Approach Digital Signature.	**07**

****