Enrolment No./Seat No_____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII EXAMINATION – SUMMER 2025

Subject Code:3170720 Date:27-05-2025

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)**	What are the key principles of security?	**03**
	(b)	Differentiate between cryptography and steganography.	**04**
	(c)	What is cryptanalysis? Explain 5 techniques of how attackers can launch attacks.	**07**
Q.2	**(a)**	What would be the transformation of a message 'Happy Birthday to you' using Rail Fence technique level =3?	**03**
	(b)	What is the idea behind meet-in-the-middle attack?	**04**
	(c)	Explain the steps in the various rounds of DES.	**07**
		OR	
	(c)	Explain the steps in the various rounds of AES.	**07**
Q.3	**(a)**	What is an Initialization Vector(IV)? What is its significance?	**03**
	(b)	Generate a Cipher text for plain text 'ACT' with key 'GYBNQKURP' using hill cipher.	**04**
	(c)	Explain RSA algorithm and also compute public key and private key of RSA with p-53, q=59 and e = 3.	**07**
		OR	
Q.3	**(a)**	Differentiate between diffusion and confusion with example	**03**
	(b)	Generate a Cipher text for plain text 'MISSION' with key 'IMPOSSIBLE' using playfair cipher.	**04**
	(c)	Explain the Deffie Hellman key exchange algorithm in detail. In a Diffie Hellman Key Exchange, Alice and Bob have chosen prime value 11 and 7. If Alice's secret key is 3 and Bob's secret key is 6, what is the secret key they exchanged?	**07**
Q.4	**(a)**	Differentiate between Session key and Master key.	**03**
	(b)	Why is SHA more secure than MD5?	**04**
	(c)	Discuss X.509 Certificates.	**07**
		OR	
Q.4	**(a)**	What are the common causes for revoking a digital certificate?	**03**
	(b)	What is the difference between MAC and message digest?	**04**
	(c)	Discuss Secure Hash Algorithm (SHA)	**07**
Q.5	**(a)**	Explain the following properties of hash function (i) One way property (ii) Weak collision resistance	**03**
	(b)	Name the four key steps in the creation of a digital certificate.	**04**
	(c)	Discuss the working of KERBEROS authentication protocol.	**07**
		OR	
Q.5	**(a)**	What are the three aspects of a 3-factor authentication?	**03**
	(b)	What is KDC? With the help of diagram explain how KDC do key distribution.	**04**
	(c)	Discuss Digital signature algorithm.	**07**

****