Enrolment No./Seat No_____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE- SEMESTER– VI EXAMINATION – SUMMER 2026

Subject Code:3164204 Date:29-05-2026

Subject Name:Data 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)**	Briefly explain any two active security attacks.	**03**
	(b)	Discuss the following terms in brief: - brute force attack - cryptography	**04**
	(c)	What is symmetric key cryptography? What are the challenges of symmetric key cryptography? List out various symmetric key algorithms and explain Caesar cipher in detail.	**07**
Q.2	**(a)**	Write differences between substitution techniques and transposition techniques.	**03**
	(b)	Write a Short note on Euclidean algorithm with suitable example.	**04**
	(c)	Explain single round of DES algorithm with suitable diagram.	**07**
		OR	
	(c)	Elaborate AES encryption with neat sketches.	**07**
Q.3	**(a)**	Briefly explain Hill cipher encryption with suitable example.	**03**
	(b)	Why CFB(Cipher feedback mode) encrypted messages are Less subject to tampering than OFB(Output feedback mode)?	**04**
	(c)	Explain playfair cipher substitution technique in detail. Find out cipher text for the following given key and plaintext. Key = ENGINEERING Plaintext=COMPUTER	**07**
		OR	
Q.3	**(a)**	Explain the rail fence cipher. Why a pure transposition cipher is easily recognized?	**03**
	(b)	Explain triple DES with two keys.	**04**
	(c)	Explain RSA algorithm in detail with suitable example.	**07**
Q.4	**(a)**	Give differences between hash function and message authentication codes.	**03**
	(b)	What is the purpose of X.509 standard? How is an X.509 certificate revoked?	**04**
	(c)	Discuss Diffie-Hillman key exchange algorithm in detail.	**07**
		OR	
Q.4	**(a)**	What problem was Kerberos designed to address? What are the three threats associated with user authentication over a network or Internet?	**03**
	(b)	What are the principal elements of public-key cryptosystem? Explain in brief.	**04**
	(c)	Explain any one approach to Digital Signatures.	**07**
Q.5	**(a)**	Briefly explain symmetric key distribution using symmetric and asymmetric encryptions.	**03**

	(b)	Is a message authentication code(MAC) function is similar to encryption. Does MAC provide authentication or confidentiality? Justify your answer	**04**
	(c)	Explain the logic of SHA(Secure Hash Algorithm).	**07**
		OR	
Q.5	**(a)**	Justify answer: Why Onetime Pad is More Secure.	**03**
	(b)	Write a short note “Public key infrastructure”.	**04**
	(c)	Explain implementation of Data Security techniques.	**07**