Enrolment No./Seat No_____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE- SEMESTER– VII EXAMINATION – SUMMER 2026

Subject Code:3170720 Date:08-06-2026

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)**	List and explain any three active attack?.	**03**
	(b)	Discuss security of Hill cipher.	**04**
	(c)	Compare Counter and Cipher Block Chaining mode of operation used for encryption and decryption.	**07**
Q.2	**(a)**	Define Confusion and Diffusion	**03**
	(b)	Draw the operation performed in one round of DES encryption.	**04**
	(c)	With the help of diagram explain decryption of DES.	**07**
		OR	
	(c)	Compare DES, Double DES and Triple DES.	**07**
Q.3	**(a)**	What is symmetric cipher? List requirements for it.	**03**
	(b)	In RSA algorithm if p = 7, q = 11 and e = 13 then what will be the value of d?	**04**
	(c)	With the help of diagram explain use of RSA algorithm for confidentiality and authentication.	**07**
		OR	
Q.3	**(a)**	List applications of RSA algorithm.	**03**
	(b)	What is trap door one way function? Give example.	**04**
	(c)	Discuss the fast and efficient algorithm use for exponentiation in RSA.	**07**
Q.4	**(a)**	What is hash function? How it helps to protect integrity of a message?	**03**
	(b)	Compare strong and weak hash function.	**04**
	(c)	Draw and explain round function of SHA512 algorithm	**07**
		OR	
Q.4	**(a)**	List applications of Cryptographic Hash Function	**03**
	(b)	Discuss Birth day attack.	**04**
	(c)	Discuss the security of MAC algorithm	**07**
Q.5	**(a)**	Explain signing in DSA algorithm.	**03**
	(b)	How signature can be verified in ElGamal digital signature	**04**
	(c)	List various alternatives used for key distribution in symmetric key cryptography. Also discuss the issue with key distribution.	**07**
		OR	
Q.5	**(a)**	Discuss generation of a private/public key pair in Schnorr digital signature	**03**
	(b)	Draw the model for Digital Signature.	**04**
	(c)	With the help of diagram explain the two alternatives used for placement of encryption/decryption.	**07**

****