Seat No.: _____ Enrolment No.

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER– VI (Old) EXAMINATION – WINTER 2019

Subject Code: 160702 **Date: 12/12/2019**

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.**

Q.1	**(a)**	Draw the block diagram and explain Shannon's theory of communication.	**07**
	(b)	(1) Encrypt the text "trust" using Caesar Cipher with key=25	**02**
		(2) Compare the strength of mono-alphabetic ciphers to poly-alphabetic ciphers.	**05**
Q.2	**(a)**	State the principles for block cipher design and explain in detail.	**07**
	(b)	Explain S-DES with necessary block diagram.	**07**
		OR	
	(b)	Explain Blowfish with necessary block diagram.	**07**
Q.3	**(a)**	Explain Diffie-Hellman key exchange protocol with block diagram and example.	**07**
	(b)	What are "relatively prime" numbers? Explain Euler's theorem the importance of modular arithmetic in information security.	**07**
		OR	
Q.3	**(a)**	Explain RSA algorithm with appropriate block diagram and example.	**07**
	(b)	How does ECC work? What are its advantages over other encryption algorithms?	**07**
Q.4	**(a)**	What is e-commerce? Discuss requirement of security w.r.t. e-commerce transactions.	**07**
	(b)	Explain Kerberos authentication protocol with necessary diagrams.	**07**
		OR	
Q.4	**(a)**	What is SHA-256? Explain with necessary block diagram.	**07**
	(b)	Why is X.509 directory authentication service used? Explain its working.	**07**
Q.5	**(a)**	Write a short note on Secure Electronic Transactions.	**07**
	(b)	Write a short note on IP security.	**07**
		OR	
Q.5	**(a)**	What is a firewall? What are standard firewall design principles?	**07**
	(b)	Explain how PGP is important for email security.	**07**

****