Seat No.: _____ **Enrolment No._____**

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VI (OLD) - EXAMINATION – SUMMER 2017

Subject Code: 160702 **Date: 08/05/2017**

Subject Name: Information 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.**

Q.1	**(a)**	Differentiate public key cryptography and symmetric key cryptography. Explain any one substitution method for symmetric key cryptography.	**07**
	(b)	Differentiate mono alphabetic and poly alphabetic substitution method. Vigenere cipher with example.	**07**
Q.2	**(a)**	Write Short Note on Types of Attacks.	**07**
	(b)	Explain Columnar Transposition cipher with example.	**07**
		OR	
	(b)	Explain rail fence transposition technique with example.	**07**
Q.3	**(a)**	Explain Feistel Cipher Structure with respect to its design features.	**07**
	(b)	Explain block cipher mode of operation.	**07**
		OR	
Q.3	**(a)**	Explain block cipher design principles.	**07**
	(b)	Explain simplified DES method with example.	**07**
Q.4	**(a)**	Write Short Note: PGP	**07**
	(b)	Explain SHA-512 algorithm.	**07**
		OR	
Q.4	**(a)**	Write Short Note: S/MIME	**07**
	(b)	Explain four stages of a single round in AES.	**07**
Q.5	**(a)**	Explain RSA Algorithm.	**07**
	(b)	Explain central authority public key distribution scenario with neat and diagram.	**07**
		OR	
Q.5	**(a)**	Explain Diffie Hellman key exchange algorithm.	**07**
	(b)	Explain Exchange of public key certificate scenario with neat diagram.	**07**

****