Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VI • EXAMINATION – WINTER • 2014

Subject Code: 160702 Date: 28-11-2014

Subject Name: Information Security

Time: 02:30 pm - 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)**	What is security Services? Explain any three types of security services.	**07**
	(b)	Explain Vegenere Cipher.	**07**
Q.2	**(a)**	Define Block Cipher. Explain Design Principles of block cipher.	**07**
	(b)	What is primitive root? Explain Diffi-Hellmen key exchange algorithm with proper example.	**07**
		OR	
	(b)	Elaborate various kinds of attacks on RSA algorithm.	**07**
Q.3	**(a)**	Explain DES algorithm with Figure.	**07**
	(b)	Explain MD5 Algorithm.	**07**
		OR	
Q.3	**(a)**	Explain Sub key generation Process in Simplified DES algorithm with Example.	**07**
	(b)	Explain SHA512 Algorithm.	**07**
Q.4	**(a)**	Write Short note on S/MIME.	**07**
	(b)	Explain Kerberos Authentication System.	**07**
		OR	
Q.4	**(a)**	Explain Key Distribution methods.	**07**
	(b)	Explain Modes of Operations.	**07**
Q.5	**(a)**	Explain Secure Socket Layer Protocol.	**07**
	(b)	Explain Active Directory Services of Windows 2000 Server.	**07**
		OR	
Q.5	**(a)**	Explain Secure Electronic Transaction Protocol.	**07**
	(b)	Explain Security of E-Commerce.	**07**

****