Seat No.: ________ Enrolment No.______________

GUJARAT TECHNOLOGICAL UNIVERSITY

B. E. - SEMESTER – VI • EXAMINATION – WINTER 2012

Subject code: 160702 **Date: 03/01/2013**

Subject Name: Information Security

Time: 02.30 pm - 05.00 pm **Total Marks: 70**

Instructions:

1. **Attempt any five questions.**
2. **Make suitable assumptions wherever necessary.**
3. **Figures to the right indicate full marks.**

Q.1	**(a)**	Define Cryptography and Cryptanalysis. Draw and explain conventional cryptosystem.	**07**
	(b)	List and explain various types of attacks on encrypted message.	**07**
Q.2	**(a)**	Let the keyword in playfail cipher is “keyword”. Encrypt a message “come to the window” using playfair cipher.	**07**
	(b)	Draw and explain the single round of DES algorithm.	**07**
		OR	
	(b)	List and explain various block cipher modes of operation with the help of diagram.	**07**
Q.3	**(a)**	Draw and explain single blowfish round in detail.	**07**
	(b)	What is KDC? With the help of diagram explain how KDC do key distribution.	**07**
		OR	
Q.3	**(a)**	1. Find GCD of 1970 and 1066 using Euclid algorithm 2. Find all primitive roots of a number 7.	
	(b)	Define congruent modulo. Also Find integer x such that 1. 5x≡4 (mod 3) 2. 7x≡6 (mod 5)	
Q.4	**(a)**	What is public key cryptography? Compare public it with conventional cryptography.	**07**
	(b)	Explain Diffie Hellman key exchange algorithm.	**07**
		OR	
Q.4	**(a)**	What is the need for message authentication? List various techniques used for authentication. Explain any one.	**07**
	(b)	Explain Encryption and decryption in RSA algorithm. Also discuss various attacks on RSA.	**07**
Q.5		Write a note on followings (Any 4) (a) Digital Signature (b) Pretty Good Privacy (c) Secure Socket Layer (d) Active Directory Service of Windows NT (e) Firewall	**14**

****