Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VI • EXAMINATION – SUMMER • 2014

Subject Code: 160702 Date: 21-05-2014

Subject Name: Information Security

Time: 10:30 am - 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)**	Explain various types of attack on computer system.	**07**
	(b)	What is security mechanism? List and explain various security mechanism.	**07**
Q.2	**(a)**	Explain the conventional security model used for information security.	**07**
	(b)	Explain cryptanalysis. Discuss any one technique for it	**07**
		OR	
	(b)	What attacks can be done on encrypted text? Explain them.	**07**
Q.3	**(a)**	Compare public key and private key cryptography. Also list various algorithms for each.	**07**
	(b)	With the help of example explain how can we find out GCD of two numbers using Euclid algorithm	**07**
		OR	
Q.3	**(a)**	What is digital signature? Explain its use with the help of example.	
	(b)	Explain play fair cipher with suitable example.	
Q.4	**(a)**	Explain limitation of DES in detail.	**07**
	(b)	List and Explain various key management techniques.	**07**
		OR	
Q.4	**(a)**	Explain RSA algorithm	**07**
	(b)	How can we achieve web security? Explain with example.	**07**
Q.5		Write a note on followings (Any 4)	**14**

(a) Pretty Good Privacy
(b) Kerberos
(c) Hill cipher
(d) Elliptic curve cryptography
(e) Diffi hellman key exchange.
(f) Message Authentication code

****