Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY
BE SEM-VI Examination-Nov/Dec-2011

Subject code: 160702 **Date: 23/11/2011**
Subject Name: Information Security
Time: 10.30 am -1.00 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)**	Define the following terms briefly. i) Cryptography ii) Relative Prime Number iii) MAC iv) Digital Signature.	**04**
	(b)	Differentiate Symmetric and Asymmetric key cryptography.	**03**
	(c)	List various modes of operations of block cipher. Explain any three of them briefly.	**07**
Q.2	**(a)**	Explain different characteristics of hash function	**04**
	(b)	Construct 5 X 5 playfair matrix for the keyword "OCCURANCE".	**03**
	(c)	Draw and explain Feistel's structure for encryption and decryption.	**07**
		OR	
	(c)	Explain single round function of DES with suitable diagram.	**07**
Q.3	**(a)**	i) Write extended Euclidean algorithm. ii) Give the steps of RSA algorithm.	**03** **04**
	(b)	Explain different key distribution techniques.	**07**
		OR	
Q.3	**(a)**	Explain Deffie Hellman key exchange scheme in detail.	**07**
	(b)	Explain X.509 authentication service.	**07**
Q.4	**(a)**	Explain modes of operations of IPsec and applications of IPsec	**07**
	(b)	Explain Secure electronic transaction protocol.	**07**
		OR	
Q.4	**(a)**	Discuss about PGP and S/MIME	**07**
	(b)	i) Explain the general structure of secure hash functions. ii)Explain briefly basic uses of MAC	**03** **04**
Q.5	**(a)**	Explain MD5 Hash Algorithm.	**07**
	(b)	Explain Kerberos in detail.	**07**
		OR	
Q.5	**(a)**	Explain SSL protocol in detail.	**07**
	(b)	Explain digital signature algorithm in detail.	**07**

_____