Seat No.: _____ *Enrolment No._____*

GUJARAT TECHNOLOGICAL UNIVERSITY

BE- VIth SEMESTER–EXAMINATION – MAY- 2012

Subject code: 160702 **Date: 11/05/2012**

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)**	1. Construct a Playfair matrix with the key "engineering". And encrypt the message "test this process".	**04**
		2. The exact realization of Feistel network depends on the choice of which parameters?	**03**
	(b)	What is the objective of attacking an encryption system? Write the two approaches to attack a conventional encryption scheme.	**07**
Q.2	**(a)**	Write four possible approaches to attacking the RSA algorithm.	**07**
	(b)	Explain the key distribution scenario and write how does decentralized key control work?	**07**
		OR	
	(b)	Explain Blowfish encryption algorithm.	**07**
Q.3	**(a)**	1. Explain the triple DES scheme with two keys and write about proposed attacks on 3DES.	**04**
		2. What is a dual signature in reference to secure electronic transaction?	**03**
	(b)	Write and explain the Diffie-Hellman key exchange algorithm.	**07**
		OR	
Q.3	**(a)**	1. Write the key features of secure electronic transaction.	**04**
		2. Explain the one time pad scheme.	**03**
	(b)	List and explain four general categories of schemes for the distribution of public keys.	**07**
Q.4	**(a)**	1. What is an elliptic curve? What is the zero point of an elliptic curve?	**04**
		2. Define the Caesar cipher.	**03**
	(b)	Explain the general format of PGP(Pretty Good Privacy) message. Assume that message is going from A to B.	**07**
		OR	
Q.4	**(a)**	1. Explain Euler's totient function.	**04**
		2. What is the difference between transport mode and tunnel mode?	**03**
	(b)	Illustrate the overall operation of HMAC. Define the terms.	**07**
Q.5	**(a)**	Which parameters define session state and which parameters define connection state in SSL(secure socket Layer)?	**07**
	(b)	Explain the one –way and two way authentication in X.509.	**07**
		OR	
Q.5	**(a)**	Explain the ticket granting server(TGS) scheme in Kerberos.	**07**
	(b)	Explain the DES encryption algorithm.	**07**

****