Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VI • EXAMINATION – WINTER 2013

Subject Code: 160702 Date: 29-11-2013

Subject Name: Information Security

Time: 02:30 pm to 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)**	(i) Define the terms threat and attack. List and briefly define categories of security attacks.	**04**
		(ii) List and briefly define the security services.	**03**
	(b)	(i) Explain Blowfish encryption algorithm.	**04**
		(ii) Construct a playfair matrix with the key "occurrence". Generate the cipher text for the plaintext "Tall trees"	**03**
Q.2	**(a)**	Define the terms diffusion and confusion. What is the purpose of S-box in DES? Explain the avalanche effect in DES.	**07**
	(b)	Explain monoalphabetic cipher and polyalphabetic cipher by giving an example.	**07**
		OR	
	(b)	What is cryptography? Briefly explain the model of Asymmetric Cryptosystem.	**07**
Q.3	**(a)**	(i) Explain RSA algorithm and list the possible approaches to attacking it.	**04**
		(ii) Perform encryption and decryption using the RSA algorithm for p=3,q=11, e=7, M=5.	**03**
	(b)	Why mode of operation is defined? Explain the block cipher modes of operation?	**07**
		OR	
Q.3	**(a)**	(i) Compare conventional encryption with public key encryption.	**04**
		(ii) What is a trap-door one-way function? What is its importance in public key cryptography?	**03**
	(b)	Explain the general format of PGP(Pretty Good Privacy) message	**07**
Q.4	**(a)**	Briefly explain Diffie-Hellman key exchange. Is it vulnerable to man in the middle attack? Justify.	**07**
	(b)	(i) What characteristics are needed in a secure hash function?	**04**
		(ii) What is the difference between weak and strong collision resistance?	**03**
		OR	
Q.4	**(a)**	Discus the ways in which public keys can be distributed to two communication parties.	**07**
	(b)	(i) Write the key features of secure electronic transaction.	**04**
		(ii) What is the difference between transport mode and tunnel mode?	**03**
Q.5	**(a)**	List the security services provided by digital signature. Write and explain the Digital Signature Algorithm.	**07**
	(b)	What is MAC? Why it is required? Explain HMAC algorithm.	**07**

OR

Q.5 **(a)** What problem was Kerberos designed to address? Briefly explain how session key is distributed in Kerberos. **07**

(b) List and define the parameters that define secure socket layer connection state. **07**

****