Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE – SEMESTER – VI (OLD).EXAMINATION – WINTER 2016

Subject Code: 160702 Date: 26/10/2016

Subject Name: Information Security

Time: 02:30 AM 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)**	1. What is the difference between a block cipher and a stream cipher?	**02**
		2. What is the purpose of the S-boxes in DES?	**05**
	(b)	1. What is the difference between an unconditionally secure cipher and a computationally secure cipher?	**02**
		2. What are the essential ingredients of a symmetric cipher?	**05**
Q.2	**(a)**	What is the limitation of Electronic Codebook Mode (ECB)? How it is overcome by Cipher Block Chaining (CBC) mode? Also explain CBC mode in detail.	**07**
	(b)	1. What is the difference between differential and linear cryptanalysis?	**02**
		2. Why is it important to study the Feistel cipher?	**05**
		OR	
	(b)	1. What are the problems with one-time pad?	**02**
		2. Encrypt the following message using playfair cipher. Message: COMSEC means communications security Keyword: Galois	**05**
Q.3	**(a)**	1. How many keys are used in triple encryption?	**02**
		2. What are differences between RC5 and blowfish?	**05**
	(b)	Discuss different techniques for public-key distribution.	**07**
		OR	
Q.3	**(a)**	1. Define session key and master key.	**02**
		2. Discuss decentralized key distribution approach.	**05**
	(b)	Explain public-key cryptosystem in detail.	**07**
Q.4	**(a)**	What is message authentication code? What are the requirements for MACs? Briefly discuss MAC based on DES.	**07**
	(b)	Discuss the possible approaches to attack the RSA algorithm. Also discuss various mathematical and timing attacks for RSA algorithm.	**07**
		OR	
Q.4	**(a)**	What characteristics are needed in secure hash function? Explain the concept of simple hash function.	**07**
	(b)	What are the five principal services provided by PGP? Why does PGP generate signature before applying comparison?	**07**
Q.5	**(a)**	What are the requirements of digital signature? Explain the concept of arbitrated digital signature.	**07**
	(b)	What are the benefits from IPSec? Mention the most important documents of IPSec along with their significance.	**07**
		OR	
Q.5	**(a)**	What are the limitations of Diffie-Hellman algorithm? Which are the features of Oakley algorithm?	**07**
	(b)	Explain SSL architecture.	**07**

****