Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY
BE - SEMESTER– VIII EXAMINATION – SUMMER 2015

Subject Code: 183202 **Date:15/05/2015**
Subject Name: System and Network Security
Time: 10.30am - 1.00pm **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 Cryptography and Cryptanalysis. Draw and explain conventional cryptosystem.	**07**
	(b)	(i) Explain the OSI Security architecture.	**03**
		(ii) List and briefly define Security Services.	**04**
Q.2	**(a)**	Draw and Explain the OSI reference model for network. Also give its applications and critiques.	**07**
	(b)	Draw and explain the single round of DES algorithm.	**07**
		OR	
	(b)	Draw Classical Fiestel Network and also explain its parameters and design features.	**07**
Q.3	**(a)**	(i) Construct a Playfair matrix with the key "keyword". And encrypt the message "come to the window".	**04**
		(ii) Briefly define the Caesar cipher with example.	**03**
	(b)	What is KDC? With the help of diagram explain how KDC do key distribution.	**07**
		OR	
Q.3	**(a)**	(i) Differentiate Symmetric and Asymmetric key cryptography.	**04**
		(ii) Explain the terms diffusion and confusion.	**03**
	(b)	Explain Encryption and decryption in RSA algorithm.	**07**
Q.4	**(a)**	List the security services provided by digital signature. Write and explain the Digital Signature Algorithm.	**07**
	(b)	Explain the general format of PGP (Pretty Good Privacy) message.	**07**
		OR	
Q.4	**(a)**	Explain the one –way and two way authentication in X.509.	**07**
	(b)	What does authentication header provide in case of IP security? Explain the various fields in Authentication Header.	**07**
Q.5	**(a)**	What are the two important SSL Concepts? List and explain the parameters defined by each.	**07**
	(b)	What is DDoS? Give DDoS attack Description.	**07**
		OR	
Q.5	**(a)**	Draw and Explain UNIX password scheme.	**07**
	(b)	List the design goals of firewall and also explain the techniques used by firewalls to control access and enforce a security policy.	**07**

****