Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA - SEMESTER–V • EXAMINATION – WINTER - 2016

Subject Code:650002 Date:19/11/ 2016

Subject Name: Network Security

Time:10.30 am to 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)**	Briefly explain the following terms. 1. Data Confidentiality 2. Data Integrity 3. Non-repudiation 4. Traffic Padding 5. Trusted Functionality 6. Security Service 7. Security Mechanism	**07**
	(b)	Differentiate between following 1. passive and active 2. block cipher and stream cipher 3. SSL and TLS 4. kerberos v4 and v5 5. statistical and rule based IDS 6. proactive and reactive password checking 7. application level gateway and circuit level gateway	**07**
Q.2	**(a)**	Explain feistel cipher structure with parameters and design features.	**07**
	(b)	Explain RC4 algorithm.	**07**
		OR	
	(b)	Explain any two cipher block modes.	**07**
Q.3	**(a)**	Explain different approaches to provide authentication using one way hash function.	**07**
	(b)	Explain KERBEROS version 4.	**07**
		OR	
Q.3	**(a)**	Explain diffie hellman algorithm.	**07**
	(b)	Explain KERBEROS version 5.	**07**
Q.4	**(a)**	Explain services provided by PGP	**07**
	(b)	Explain ISAKMP Payload Types.	**07**
		OR	
Q.4	**(a)**	Describe message format of PGP.	**07**
	(b)	Define SET. Explain SET participants.	**07**
Q.5	**(a)**	Write short note on combining security association.	**07**
	(b)	Explain DIDS in detail.	**07**
		OR	
Q.5	**(a)**	Explain packet filter firewall.	**07**
	(b)	Explain markov model.	**07**

****