Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. Sem. – IInd - Examination – June/July- 2011

Subject code:1720205

Subject Name: Cryptography and Network Security

Date:29/06/2011 **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)**	Distinguish between a monoalphabetic and polyalphabetic cipher. List and explain two monoalphabetic and polyalphabetic technique.	**07**
	(b)	Explain the playfair cipher with example. Also explain the various Block cipher modes of operation.	**07**
Q.2	**(a)**	What is the block size in DES? What is the cipher key size in DES? What is the round key size in DES? What is the number of rounds in DES? Why does the DES function need an expansion permutation? What is triple DES ? Explain.	**07**
	(b)	List the criteria define by NIST for AES. Explain all steps of AES in brief.	**07**
		OR	
	(b)	Distinguish between symmetric-key and asymmetric-key cryptosystem. Distinguish public and private keys in an asymmetric-key cryptosystem. Explain RSA public key cryptosystem.	**07**
Q.3	**(a)**	1) What is key distribution center? What is the difference between session key and master key? 2) What is nonce? What is the difference between statistical randomness and unpredictability?	**07**
	(b)	Explain MD5 and Secure Hash algorithm login.	**07**
		OR	
Q.3	**(a)**	What are the properties a digital signature should have? What requirement should a digital signature scheme satisfy?	**07**
	(b)	Define PGP and S/MIMIE. Explain the characteristics of PGP and what are the principal services provided by PGP.	**07**
Q.4	**(a)**	What is the requirement of authentication? List the various authentication functions. Explain Hash function in detail.	**07**
	(b)	Briefly explain Diffie – Hellman key exchange.	**07**
		OR	
Q.4	**(a)**	Give the overview of Kerberos. And what is the major difference between Kerberos version 4 and 5 ?	**07**
	(b)	Explain : (a) security issues in RFIDs. (b) Biomatric Authenticaion (c) Smart Cards and Security.	**07**

Q.5	**(a)**	Give the overview of IPsec. Also list the application of IPsec. Explain IPsec architecture in brief.	**07**
	(b)	Explain the various cryptanalysis attacks	**07**

OR

Q.5	**(a)**	What are the web security considerations? Explain its threats and its countermeasures.	**07**
	(b)	Explain the Secure Electronic Transaction. List the SET participants and explain its role in detail.	**07**

****