Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

M. E. - SEMESTER – II • EXAMINATION – SUMMER • 2014

Subject code: 2725104 Date: 12-06-2014

Subject Name: PKI and Biometrics

Time: 02:30 pm - 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)**	Explain Public key encryption and how is it different from digital signature?	**07**
	(b)	What is the difference between passive and active security threats?	**07**
Q.2	**(a)**	Explain Elliptic Curve Arithmetic	**07**
	(b)	What is the source of presence of the Weak-keys, Semi-Weak-keys and Possibly-Weak-keys in the DES?	**07**
		OR	
	(b)	Explain the SSL architecture and Protocol. How SSH works on TLS.	**07**
Q.3	**(a)**	Compare RC-5 and AES in terms of cryptographic design.	**07**
	(b)	Explain the working of Kerberos with Remote User Authentication.	**07**
		OR	
Q.3	**(a)**	What is the need of Hash? Explain SHA (Secure Hash Algorithm).	**07**
	(b)	Explain CIA triad for the security. What is the difference between authentication and authorization?	**07**
Q.4	**(a)**	Explain Diffie Hellman Key Exchange Algorithm.	**07**
	(b)	What are the requirements a public key cryptosystems must fulfill to be a secure algorithm?	**07**
		OR	
Q.4	**(a)**	Explain RSA Algorithm.	**07**
	(b)	In a public-key system using RSA, you intercept the ciphertext C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M?	**07**
Q.5	**(a)**	Show that the transposition cipher is vulnerable to a known plaintext attack.	**07**
	(b)	List important design considerations for a stream cipher.	**07**
		OR	
Q.5	**(a)**	What is the main drawback of the onetime pad cryptosystem?	**07**
	(b)	For plaintext and key pair given, encrypt using simple-DES. P= 00000000 and Key = 00000000.	**07**

****