Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

ME – SEMESTER-1 (NEW) EXAMINATION – WINTER 2016

Subject Code: 2715601 **Date:07/01/2017**

Subject Name: Cryptography and Network Security

Time: 2:30 pm to 5:00 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 Hill cipher with an example.	**07**
	(b)	Explain in detail: (1) X.800 security services (2) Differential cryptanalysis	**07**
Q.2	**(a)**	Describe encryption and decryption in Cipher Block Chaining mode.	**07**
	(b)	Describe encryption operation of AES algorithm.	**07**
		OR	
	(b)	Describe encryption operation of DES algorithm.	**07**
Q.3	**(a)**	Explain man-in-the-middle attack against Diffie-Hellman algorithm.	**07**
	(b)	Describe the ticket granting server (TGS) scheme for Kerberos.	**07**
		OR	
Q.3	**(a)**	Describe RSA algorithm with an example.	**07**
	(b)	Explain IPSec in detail.	**07**
Q.4	**(a)**	Explain Secure Hash Algorithm (SHA) in detail.	**07**
	(b)	Describe Message Authentication Code (MAC) in detail.	**07**
		OR	
Q.4	**(a)**	Describe MD5 hash algorithm.	**07**
	(b)	Explain in detail: (1) Digital Signature (2) SSL Protocol	**07**
Q.5	**(a)**	Elaborate two types of malicious programs with examples.	**07**
	(b)	Explain in detail: (1) PGP (2) Intrusion Detection System	**07**
		OR	
Q.5	**(a)**	Explain in detail: (1) Zero knowledge protocol (2) Biometric authentication	**07**
	(b)	Explain in detail: (1) Firewall (2) Secure Electronic Transaction	**07**

****