Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

ME - SEMESTER–I(New course)• EXAMINATION – WINTER- 2015

Subject Code: 2715601 **Date: 05/01/2016**

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 Playfair cipher with an example.	**07**
	(b)	(i) Explain Active and Passive attacks. (ii)Explain the following terms: (1) Access Control (2) Data Integrity (3) Data Confidentiality	**07**
Q.2	**(a)**	Explain single round of DES algorithm.	**07**
	(b)	Explain key expansion in AES.	**07**
		OR	
	(b)	Explain Linear and Differential Cryptanalysis in detail.	**07**
Q.3	**(a)**	Explain RSA algorithm with an example.	**07**
	(b)	Explain encryption and decryption in Cipher Block Chaining Mode.	**07**
		OR	
Q.3	**(a)**	Explain Diffie-Hellman key exchange algorithm with an example.	**07**
	(b)	Explain MAC (Message Authentication Code) along with its applications.	**07**
Q.4	**(a)**	Write down the requirements and properties of Digital Signature with its types.	**07**
	(b)	Explain MD5 hash algorithm.	**07**
		OR	
Q.4	**(a)**	Explain Secure Electronic Transaction.	**07**
	(b)	Explain X.509 authentication Service.	**07**
Q.5	**(a)**	Explain PGP services in detail.	**07**
	(b)	Explain the following terms: (1) Intruders (2) Viruses	**07**
		OR	
Q.5	**(a)**	Explain IP Security scenario along with its applications.	**07**
	(b)	Explain the following terms: (i) Biometric Authentication (ii) Security and Privacy Issues in RFIDs	**07**

****