Seat No.: ________ Enrolment No.___________

GUJARAT TECHNOLOGICAL UNIVERSITY

ME – SEMESTER I (NEW) – • EXAMINATION – SUMMER 2016

Subject Code: 2710211 **Date:19/05/2016**
Subject Name: INFORMATION SECURITY
Time:02:30 pm to 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 the working of Feistel Cipher in detail. **07**
(b) Explain Data Encryption Standard algorithm in detail. **07**

Q.2 **(a)** What are the Block Cipher Design Principles, list and explain. **07**
(b) Explain AES Encryption Process. **07**

OR

(b) Explain Block Cipher Modes of Operations. **07**

Q.3 **(a)** What are the requirements for Public-Key Cryptography? Explain in detail. **07**
(b) Explain RSA Algorithm. **07**

OR

Q.3 **(a)** Explain SHA-512 Round Function. **07**
(b) Explain Digital Signature Algorithm in detail. **07**

Q.4 **(a)** Explain Symmetric key distribution using Symmetric encryption. **07**
(b) Explain X.509 Certificate format in detail. **07**

OR

Q.4 **(a)** Explain Symmetric key distribution using Asymmetric encryption. **07**
(b) Explain Public-key infrastructure. **07**

Q.5 **(a)** Explain Kerberos Version 4. **07**
(b) Explain Buffer overflow, Incomplete Mediation and Race Conditions with respect to software flows. **07**

OR

Q.5 **(a)** Explain Salami attack, linearization and time bomb in detail. **07**
(b) What is the role of disassembler and debugger in software reverse engineering? Explain Code Obfuscation in detail. **07**

****