Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

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

Subject Code: 2710211 **Date:06/01/2017**

Subject Name: Information 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)	1.	What is a reply attack?	7
	2.	What substitution system results when we use 25 x 1 Playfair matrix?	
	3.	Explain the avalanche effect.	
	4.	How can we achieve authentication and confidentiality using public key cryptography?	
	5.	What is the purpose of S-Box in DES?	
	6.	Digital signature does not provide integrity. True/False, Justify	
	7.	Define Information Security?	
(b)	1.	Explain Caesar Cipher with example.	2
	2.	What problem was Kerberos designed to address?	2
	3.	List and briefly define categories of passive security attacks.	3
Q. 2. (a)	1.	Explain Stream Cipher and Block Cipher.	2
	2.	Explain SubBytes and Mix column functions in AES.	2
	3.	Explain Meet in the middle attack.	3
(b)		Explain limitation of DES in detail.	7
		Or	
		What is digital signature? Explain its use with the help of example.	
Q. 3. (a)	1.	What is Prime and Relative Prime Numbers? Give Example of each	3
	2.	Write the Euclid's algorithm and show the steps of Euclid's algorithm with example.	4
(b)	1.	Why is the middle portion of 3DES a decryption rather than an encryption?	3
	2.	Explain X.509 certificates.	4
		Or	
Q. 3. (a)	1.	What is Key Distribution centre?	3
	2.	What is a primitive root of a number?	4
(b)	1.	Explain Alert protocol in Transport Layer Security	3
	2.	What are the requirements of MAC? Explain	4
Q. 4. (a)		Explain Secure Socket Layer Protocol.	7
(b)	1.	What is dual signature and what is its purpose?	3
	2.	Explain Man in The Middle attack.	4
		Or	
Q. 4. (a)		What is message Digest? Explain the process of message digest generation used in SHA-512.	7
(b)	1.	Explain Software Reverse Engineering	3
	2.	Explain Kerberos v4 with Diagram.	4
Q. 5. (a)		Compare conventional encryption with public key encryption.	7
(b)	1.	How key expansion is done in AES.	3
	2.	Differentiate between Cyber Disease and Biological diseases	4

Or

Q. 5. (a)	1.	What is Trojan Horse Defence with example	3
	2.	What is malware? List out their types and discuss metamorphic and polymorphic malware.	4
(b)	1.	Discuss Anti-Debugging Techniques	3
	2.	Discuss various miscellaneous software based attacks.	4