Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA – SEMESTER V – EXAMINATION – SUMMER 2017

Subject Code: 650002 **Date: 01/06/2017**

Subject Name: Network Security

Time:2:30 pm – 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 any 7 terms: **07**

1. Data Integrity
2. Stream Cipher
3. CBC
4. Detached Signature
5. Forward Certificate
6. Session Key
7. Integrity Check value in IPsec
8. Subject with respect to trusted system
9. Honey pot
10. Tiny fragment attack

(b) Explain Active and Passive attack in detail. **07**

Q.2 **(a)**

1. Explain types of attack on encrypted message. **04**
2. Give example of following **03**
   a. Replay attack
   b. Encryption

(b) Explain three approaches to message authentication. **07**

OR

(b) Why modes of operation are defined? Explain any three cipher block modes of operation. **07**

Q.3 **(a)** Briefly explain Diffie-Hellman key exchange. Justify that Diffie-Hellman is vulnerable to man in the middle attack. **07**

(b) Explain X.509 authentication procedures in detail. **07**

OR

Q.3 **(a)**

1. What is HMAC? Why it is useful? **04**
2. List the steps of RSA algorithm. **03**

(b) What is Kerberos realm? Write any four differences between Kerberos version 4 and version 5. **07**

Q.4 **(a)** Explain SSL architecture and SSL record protocol. **07**

(b) What is key ring in PGP? Briefly explain the structure indicating the different fields of private Key Ring in PGP. **07**

OR

Q.4 **(a)**

1. Why web security is important issue today? List any four reasons for the same. **04**
2. What does the Alert protocol do? **03**

(b) Briefly explain PGP services. **07**

Q.5 **(a)**

1. Explain Anti-Replay service. **04**
2. Write any three differences between Transport and Tunnel mode in IPsec. **03**

	(b)	Just by drawing schematic diagram, show how new password is loaded and existing password is verified in UNIX system.	**07**

OR

Q.5	**(a)**	1. Explain two rules of multilevel security.	**02**
		2. Explain Trojan horse Defense.	**05**
	(b)	What is IPsec? What are the applications of IPsec? Explain the modes of IPsec operations.	**07**

****