

GUJARAT TECHNOLOGICAL UNIVERSITY
MCA - SEMESTER– V EXAMINATION – WINTER - 2018

Subject Code: 650002**Date:17/11/2018****Subject Name: Network Security****Time:10.30 am to 01.00pm****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) Define following in Brief** **07**
1. Data Integrity 2. Security Association. 3. Digital Signature.
4. Honey pot 5. Message Confidentiality 6. Stream Cipher 7. Active Attack
- (b) Explain key features of SET.** **07**
- Q.2 (a) Difference between Active & Passive Attack** **07**
(b) Difference between Block & Stream Cipher **07**
- OR**
- (b) Difference between SSL & TLS** **07**
- Q.3 (a) Explain RC4 algorithm in detail.** **07**
(b) Discuss IP Security and its architecture. **07**
- OR**
- Q.3 (a) Discuss the concept of ESP** **07**
(b) Compare DES, 3DEC & AES. **07**
- Q.4 (a) Define Deffie-Hellman key exchange algorithm with example.** **07**
(b) Explain Kerberos Version 4. **07**
- OR**
- Q.4 (a) Explain ISAKMP payload type.** **07**
(b) Explain X.599 Certificate. **07**
- Q.5 (a) Briefly explain properties of Hash function.** **07**
(b) Explain PGP and its services. **07**
- OR**
- Q.5 (a) Discuss Firewall and its types.** **07**
(b) What is Intrusion explain its detection techniques. **07**
