Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA– SEMESTER –IV EXAMINATION –SUMMER-2019

Subject Code:3640004 **Date: 21-05-2019**

Subject Name: Network Security

Time:10.30 am to 1.00 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)** Answer the following **(Any Seven)** **07**

Give Abbriviation for following Terms

1. SSH
2. PKI
3. DMZ
4. OSI
5. AES
6. PRF
7. Define : Threat
8. Define : Attack
9. A masquerade takes place when one entity pretends to be a different entity True/False

(b) Define Following Terms with one/two line(s) definition **07**

1. Block cipher
2. Security Service
3. Public Key
4. Steam cipher
5. Encryption
6. Security Mechanism
7. Hyper Text Browser

Q.2 **(a)** Write symmetric encryption scheme five ingredients and draw figure. **07**

(b) Discuss categories of passive and active security attacks. **07**

OR

Q.2 **(b)** What is OSI Security Architecture? Discuss OSI-SA with reference of security attack, mechanism and services. **07**

Q.3 **(a)** List type of Attack on Encrypted Messages **07**

(b) What are three different independent dimensions of Cryptography **07**

OR

Q.3 **(b)** Short note on Feistel Cipher Structure **07**

Q.4 **(a)** Discuss HASH Functions requirements **07**

(b) Short note on Public Key Encryption Structure **07**

OR

Q.4 **(b)** Why do some block cipher modes of operation only use encryption while others use both encryption and decryption? Differentiate between a block cipher and a stream cipher. **07**

Q.5 **(a)** What is FIREWALL? Describe the various types of Firewall and why is neede in Security network? **07**

(b) Discuss the Comparusib if Threats on the web **07**

OR

Q.5 **(a)** Describe three alternative approaches to providing WAP end-to-end security. **07**

(b) Discuss the SSL Architecture **07**

****