Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA SEMESTER—IV–EXAMINATION –SUMMER-2017

Subject code: 3640004 **Date: 06/06/2017**

Subject Name: Network Security

Time: 10:30 AM – 01:00 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) Expand following abbreviations **07**

1. MIME 2. IEEE 3. WPA 4. SSH
5. PKI 6. DMZ 7. OSI

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

1. Encryption
2. Data Integrity
3. Cryptanalysis
4. Public Key
5. Password Protection
6. Network Layer
7. Hyper Text Browser

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

(b) Discuss network access security model with its diagram and services. **07**

OR

(b) List and briefly mark out categories of passive and active security attacks. **07**

Q.3 (a) 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**

(b) What is triple encryption? Why the middle portion of 3DES is a decryption rather than an encryption? **07**

OR

Q.3 (a) What properties must a hash function have to be useful for message authentication? In the context of a hash function, what is a compression function? **07**

(b) What are the principal ingredients of a public-key cryptosystem? List and briefly define three uses of a public-key cryptosystem. **07**

Q.4 (a) What is the basic building block of an 802.11 WLAN? List and briefly define IEEE 802.11 services. **07**

(b) List out the security services provided by WTLS and describe with appropriate example. **07**

OR

Q.4 (a) Draw a neat and clean diagram of Secure Socket Layer (SSL) stacks and compare the SSL 2.0 and SSL 3.0 architecture. **07**

(b) Describe three alternative approaches to providing WAP end-to-end security. **07**

Q.5 (a) What are the five principal services provided by PGP? Why does PGP generate a signature before applying compression? **07**

(b) 1. What is the difference between transport mode and tunnel mode? **04**

2. List out any 3 design requirements of HMAC **03**

OR

Q.5 (a) 1. What do you understand by FIREWALL? Describe the various types of Firewall. **04**

2. Why firewall is needed in a secure network? **03**

(b) 1. List and briefly define three classes of intruders. **04**

2. Elucidate how enveloped data is generated in SMIME. **03**

****