Seat No.: _____ Enrolment No._____

# GUJARAT TECHNOLOGICAL UNIVERSITY
## MCA– SEMESTER –V EXAMINATION –SUMMER-2019

**Subject Code: 2650002** **Date: 04-05-2019**

**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)** Answers the following: **07**

1. Give one major difference between a passive and an active attack.
2. What is a clear signed message in SMIME?
3. What do you mean by Certificate Revocation?
4. Differentiate Transport and Tunnel Mode in IPSec.
5. Explain Access control?
6. Write name of any two Symmetric Cipher algorithms.
7. Explain Data Authentication.

**(b)** Fill in the blanks **07**

1. The two types of operation used for transforming plain text to cipher text are _____ and _____.
2. Hash function produces a _____ output for _____ input.
3. Kerberos server consists of two server _____ and _____.
4. Size of fragment in SSL record protocol is _____.
5. The PGP message encryption algorithms are _____ and _____.
6. Full form of ESP is _____.
7. In Anti-Replay service TCP sequence numbers are between ___ to ____.

**Q.2** **(a)** Write any one type/example of following: **07**

1. Active attack
2. Digital Signature generation algorithm
3. Alert message in SSL
4. Public key encryption algorithm
5. Cryptanalysis attack
6. Key exchange
7. Subject name in X.509 certificate

**(b)**

1. Mention and very briefly explain any five fields/elements of the format of X.509 Public Key Certificate. **05**
2. Compare DES, 3DES and AES. **02**

**OR**

**(b)** **Attempt any two** **07**

1. Explain three different ways to secure the web traffic using different layers.
2. Explain: Rule and statistical anomaly based Intrusion Detection.
3. Write at least four important differences between a block and a stream cipher

| | | | |
|---|---|---|---|
| **Q.3** | **(a)** | 1. Explain PGP Services Authentication and confidentiality with suitable diagram. | **05** |
| | | 2. Write any two advantages of counter mode. | **02** |
| | **(b)** | 1. Write any four important differences between Kerberos version 4 and 5. | **04** |
| | | 2. What is the need for using both, symmetric and asymmetric keys in construction of Enveloped Data? | **03** |

**OR**

| | | | |
|---|---|---|---|
| **Q.3** | **(a)** | Briefly explain the structure/format indicating the different fields of Public Key Ring in PGP. | **07** |
| | **(b)** | Attempt any two<br>1. Explain SSL record Protocol in Detail.<br>2. Explain IP spoofing and tiny fragment attack with respect to packet filter firewall.<br>3. Why compression is applied before encryption and after authentication in PGP? | **07** |
| **Q.4** | **(a)** | 1. Draw ESP format for IPsec and show the need of fields SPI, sequence number, payload data, padding, pad length. | **04** |
| | | 2. Write any three differences between SSL and TLS. | **03** |
| | **(b)** | 1. How Man-in-Middle attack performed in Diffie Hellman key exchange. | **04** |
| | | 2. What is the role of function P_hash() in TLS? | **03** |

**OR**

| | | | |
|---|---|---|---|
| **Q.4** | **(a)** | What is IPSec? What are the applications of IPSec? Explain the modes of IPSec operations. | **07** |
| | **(b)** | **Attempt any two**<br>1. Why web security is more important issue today? List at least four reasons for the same.<br>2. Write any three differences between WAP and HTML.<br>3. Differentiate between forward and backward certificates. And explain the role of CA in PKIX. | **07** |
| **Q.5** | **(a)** | 1. Explain the five ingredients of symmetric encryption. | **05** |
| | | 2. Write the name of two cipher based MAC. | **02** |
| | **(b)** | 1. Explain: HMAC with suitable Diagram. | **04** |
| | | 2. Write the phases of Handshake Protocol. | **03** |

**OR**

| | | | |
|---|---|---|---|
| **Q.5** | **(a)** | 1. Explain MIME content type Multipart along with its subtype. | **04** |
| | | 2. Write any three routing applications of IPSec. | **03** |
| | **(b)** | **Attempt any two**<br>1. Write the steps used in AES algorithm.<br>2. Explain the stages of Virus.<br>3. Write how outbound traffic is processed with the first packet on a new secure connection in IPsec. | **07** |

**********