Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA Integrated- SEMESTER– VIII EXAMINATION – WINTER 2019

Subject Code: 4480603 Date:20/11/2019

Subject Name: Network Security

Time: 02:30 PM TO 05:00 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)** Write any one major difference between the following: **07**

1. DES and AES
2. SSL and TLS
3. Symmetric and Asymmetric Encryption
4. Public and Private key
5. Virus and Worm
6. Enveloped and clear signed data
7. Attack and threat

(b) Explain fiestal structure. What is the role of fiestal structure in implementation of DES algorithm? Explain in detail. **07**

Q.2 **(a)** Write any one difference between block and stream cipher. Explain CBC and counter cipher block modes of operations with advantages and Limitations. **07**

(b)
1. Explain the working of MAC with suitable diagram. **03**
2. Explain the role of public and private key in RSA algorithm to achieve confidentially and authentication using suitable diagram. **04**

OR

(b)
1. Write any four differences between Kerberos V4 and V5. **04**
2. Explain any three important fields of X.509 V3 certificate. **03**

Q.3 **(a)** Explain the need and working of SSL Handshake protocol in detail with suitable diagram. **07**

(b) Briefly explain the structure/format indicating the different fields of Public Key Ring in PGP. **07**

OR

Q.3 **(a)** Explain SSL record protocol and SSL alert protocol with suitable diagram. **07**

(b) Explain PGP services Authentication, Confidentiality, Authentication & Confidentiality using suitable diagram. **07**

Q.4 **(a)**
1. Write the two differences between transport and tunnel mode. **02**
2. Write any four applications of IPSec. **04**
3. Write full form of ESP **01**

(b)
1. Explain classes of Intruders. **03**
2. Define the terms false positive and False Negative. **02**
3. Write the importance of Honey pots in Intrusion Detection. **02**

OR

Q.4 **(a)** Explain Profile and Rule based Intrusion detection system in detail. **07**

(b)
1. Why web security is more important issue today? List at least four reasons for the same. **04**
2. Explain any three fields related with SAD in IPSec. **03**

Q.5	**(a)**	What is proactive password checking? Explain with example. Explain how it is different and better than reactive checking.	**07**
	(b)	1. Write any three advantages of Firewall.	**03**
		2. Explain the attacks performed on firewalls.	**04**

OR

Q.5	**(a)**	Explain the need of Firewall. Explain different types of Firewalls in detail.	**07**
	(b)	1. What is an Audit record in IDS.	**03**
		2. Explain the types of active attacks using suitable diagram.	**04**

****