Seat No.: ________ Enrolment No.______________

GUJARAT TECHNOLOGICAL UNIVERSIT

MCA INTEGRATED– SEMESTER VIII- EXAMINATION –SUMMER-2022

Subject Code: 4480603 **Date: 04/06/2022**

Subject Name: Network Security

Time: 10:30 AM to 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)** Explain the Following terms: **07**

i) Message Confidentiality
ii) ii) Message Integrity
iii) Message Authentication
iv) iv) Non Repudiation
v) v) Denial of Service
vi) vi) Symmetric Encryption
vii) vii) Cryptanalysis

(b) 1. Explain working of CBC and CFM cipher block modes of operations with diagram. **04**
2. Explain the Fiestel Cipher Structure with suitable diagram. **03**

Q.2 **(a)** 1. Explain Diffie-Hellman key exchange with highlighting the need of it. **04**
2. Explain the HMAC algorithm with diagram. **03**

(b) 1. Explain any four differences between Kerberos version 4 and Kerberos version 5. **04**
2. Explain X.509 Authentication Procedures in brief. **03**

OR

(b) 1. Explain the Public Key Infrastructure X.509 architecture model. **04**
2. Explain Nonce; Ticket; Authenticator with respect to Kerberos. **03**

Q.3 **(a)** Draw the SSL Protocol Stack. Explain the SSL handshake protocol. **07**

(b) 1. What is a Security Association? What are the three parameters that uniquely identify it? **04**
2. Differentiate between transport and tunnel modes of IPSec **03**

OR

Q.3 **(a)** What is SSH? Explain in brief the three protocols of SSH. **07**

(b) 1. Explain the Anti-Replay Service ESP? **04**
2. Why is R-64 conversion is useful for an email application? **02**
3. What does the ChangeCipherSpec protocol do? **01**

Q.4 **(a)** 1. What are the basic building blocks of an 802.11 WLAN? **04**
2. What security areas are addressed by IEEE 802.11i? **03**

(b) Explain the four services provided by PGP along with suitable diagram. **07**

OR

Q.4 **(a)** What is IPSec? What are the applications of IPSec? Explain the modes of IPSec operations. **07**

(b) 1. What is the difference in message authentication code calculation process in SSL and TLS? **04**
2. What is the role of function P_hash() in TLS? **03**

Q.5 **(a)**

1. Write any two methods of learning passwords. **02**
2. What are honey pots? How they help learning about attacker activities? **02**
3. What is proactive password checking? Why it is better than other password checking techniques? **03**

(b) Briefly explain the following terms:

1. Key rings in PGP **04**
2. Password selection strategies (any one) **03**

OR

Q.5 **(a)**

1. Which are the benefits of IDS? Write the principle on which the Intrusion detection is based. **03**
2. What is an Audit record in IDS. **02**
3. What is Salt in password management **02**

(b) Explain how attacks like IP address spoofing, source routing and tiny fragments can be carried out on packet filtering routers? What are the counter measures? **07**

****