Seat No.: _____ Enrolment No._____

# GUJARAT TECHNOLOGICAL UNIVERSITY

**MCA INTEGRATED– SEMESTER VIII - EXAMINATION –SUMMER-2021**

**Subject Code: 4480603 Date: 05-08-2021**

**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 following terms.<br>1) Honeypot intrusion detection<br>2) RC4<br>3) Public key<br>4) Private key<br>5) Hash function<br>6) Digital signature<br>7) Cryptography | **07** |
| | **(b)** | Explain boot force password attack with proper example and write code java code to crack 8 length password having a to z and 0 to 9. | **07** |
| **Q.2** | **(a)** | What is Symmetric Block Cipher? Explain AES with suitable diagram | **07** |
| | **(b)** | Why mode of operation is defined? Explain any two cipher block modes of operations. | **07** |
| | | **OR** | |
| | **(b)** | Explain HMAC algorithm with suitable diagram. | **07** |
| **Q.3** | **(a)** | Explain SHA-256 with diagram. | **07** |
| | **(b)** | Explain PGP Services. | **07** |
| | | **OR** | |
| **Q.3** | **(a)** | Discuss SSL Alert and SSL Handshake Protocol | **07** |
| | **(b)** | Discuss the Man-In-The-Middle attack with suitable diagram. | **07** |
| **Q.4** | **(a)** | Discuss Password selection strategies in detail. | **07** |
| | **(b)** | What is random number generator? Discuss TRNG, PRNG and PRF 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)** | Explain Intrusion Detection. | **07** |
| **Q.5** | **(a)** | Write notes on X.509 certificate. | **07** |
| | **(b)** | Draw AH format for IPsec and discuss all the necessary fields. | **07** |
| | | **OR** | |
| **Q.5** | **(a)** | Write java code to encrypt “abc”(input) to 123(output). | **07** |
| | **(b)** | 1) How UNIX manages passwords to make it secure from attackers?<br>2) Explain how one can use Markov model for proactive password checking? | **07** |

**********