Enrolment No./Seat No_____

# GUJARAT TECHNOLOGICAL UNIVERSITY

**BE - SEMESTER–VII EXAMINATION – SUMMER 2025**

**Subject Code:2170709 Date:21-05-2025**

**Subject Name:Information and 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.**
4. **Simple and non-programmable scientific calculators are allowed**

| | | | **Marks** |
|---|---|---|---|
| **Q.1** | **(a)** | Define: Confidentiality, Integrity and Availability. | **03** |
| | **(b)** | Discuss Confusion and Diffusion in cryptography with appropriate example. State its purposes. | **04** |
| | **(c)** | Explain Playfair cipher technique in detail. Find cipher text for plain text ‘MYSECRETMSG’ using ‘STARS’ as key. | **07** |
| **Q.2** | **(a)** | Explain the steps of key generation in Advanced Encryption Standard. | **03** |
| | **(b)** | Compare and contrast symmetric key cryptography and asymmetric key cryptography. | **04** |
| | **(c)** | Draw a detailed block diagram of decryption process in DES. Add appropriate description. | **07** |
| | | **OR** | |
| | **(c)** | Draw a detailed block diagram of decryption process in AES. Add appropriate description. | **07** |
| **Q.3** | **(a)** | Briefly explain Electronic Code Book mode for block ciphers. | **03** |
| | **(b)** | Explain the working of public key cryptosystem with neat diagram. | **04** |
| | **(c)** | Assuming two primes p=5 and q=11, calculate all the values of RSA. Assume other values appropriately. | **07** |
| | | **OR** | |
| **Q.3** | **(a)** | State the differences between birthday attack and brute force attack. | **03** |
| | **(b)** | Write a short note on Meet-in-the-middle attack. | **04** |
| | **(c)** | Assuming other values appropriately, calculate all the values for Diffie-Hellman key exchange, consider two primes q=23 and a=11. | **07** |
| **Q.4** | **(a)** | Enlist various web security threats. Explain any one in brief. | **03** |
| | **(b)** | Explain how Man-in-the-middle attack is carried out. | **04** |
| | **(c)** | Define message authentication code and its characteristics. Discuss MAC based on any standard block cipher. | **07** |

**OR**

| | | | |
|---|---|---|---|
| **Q.4** | **(a)** | Enlist and explain any one in detail, different ways for distribution of public keys? | **03** |
| | **(b)** | Explain authentication and confidentiality services provided in Pretty Good Privacy. | **04** |
| | **(c)** | Justify the characteristics needed for a hash function. Explain Secure Hash Algorithm-1 in brief. | **07** |

| | | | |
|---|---|---|---|
| **Q.5** | **(a)** | Draw X.509 certificate format neatly. | **03** |
| | **(b)** | Explain the use of TGT in Kerberose. | **04** |
| | **(c)** | Write a detailed note on SSL architecture and protocol. | |

**OR**

| | | | |
|---|---|---|---|
| **Q.5** | **(a)** | Draw SSL Architecture neatly. | **03** |
| | **(b)** | Explain key distribution process using Key Distribution Center (KDC). | **04** |
| | **(c)** | Explain digital signature schemes Elgamal and Schnorr. | **07** |

**********