| | t No.: | GUJARAT TECHNOLOGICAL UNIVERSITY BE - SEMESTER–VI(OLD) – EXAMINATION – SUMMER 2019 | - |
|-----------|--------------------------------------|---|----------|
| Su Tii | bject me:1 tructio 1. 2. | . Attempt all questions. | |
| Q.1 | | Explain types of Security Attacks. Explain Diffie - Hellman key exchange algorithm. Also explain Man-in-Middle attack with example. | 07 07 |
| Q.2 | (a) (b) | Explain conventional security model used for information security. Encrypt Message "Secure" using Hill Cipher with key $\begin{bmatrix} 17 & 10\\ 23 & 19 \end{bmatrix}$ | 07 07 |
| | (b) | OR Encrypt the given message using playfair cipher. Message : GOOD MORNING Key : GTU EXAMS | 07 |
| Q.3 | (a) (b) | Compare Symmetric Key Algorithm with Asymmetric Key Algorithm. Explain Data Encryption Standards Algorithm with diagram. OR | 07 07 |
| Q.3 | (a) (b) | Explain Modes of Algorithm. Explain SHA-512 Algorithm. | 07 07 |
| Q.4 | (a) (b) | List & Explain various key management techniques. Explain concept of Dual Signature in SET. | 07 07 |
| Q.4 | (a) (b) | What is SSL? Explain SSL Handshake & Record Protocol. Explain Authentication mechanism of Kerberos. | 07 07 |
| Q.5 | (a) (b) | What are the fixe services principal services provided by PGP? Explain in detail. Explain Dignal Signature. Also explain its use with the help of example. OR | 07 07 |
| Q.5 | (a) (b) | Explain Sec with its benefits. What are the characteristics of hash function? Also explain basic techniques of hash algorithm. | 07 07 |
