Seat No.: ________ Enrolment No.___________

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VI(OLD) – EXAMINATION – SUMMER 2019

Subject Code:160702 Date:21/05/2019

Subject Name: Information 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 types of Security Attacks. **07**

(b) Explain Diffie - Hellman key exchange algorithm. Also explain Man-in-Middle attack with example. **07**

Q.2 **(a)** Explain conventional security model used for information security. **07**

(b) Encrypt Message "Secure" using Hill Cipher with key $\begin{bmatrix} 17 & 10 \\ 23 & 19 \end{bmatrix}$ **07**

OR

(b) Encrypt the given message using playfair cipher. **07**
Message : GOOD MORNING
Key : GTU EXAMS

Q.3 **(a)** Compare Symmetric Key Algorithm with Asymmetric Key Algorithm. **07**

(b) Explain Data Encryption Standards Algorithm with diagram. **07**

OR

Q.3 **(a)** Explain Modes of Algorithm. **07**

(b) Explain SHA-512 Algorithm. **07**

Q.4 **(a)** List & Explain various key management techniques. **07**

(b) Explain concept of Dual Signature in SET. **07**

OR

Q.4 **(a)** What is SSL? Explain SSL Handshake & Record Protocol. **07**

(b) Explain Authentication mechanism of Kerberos. **07**

Q.5 **(a)** What are the five services principal services provided by PGP? Explain in detail. **07**

(b) Explain Digital Signature. Also explain its use with the help of example. **07**

OR

Q.5 **(a)** Explain IP Sec with its benefits. **07**

(b) What are the characteristics of hash function? Also explain basic techniques of hash algorithm. **07**

****