Seat No.: _____ **Enrolment No._____**

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VI- EXAMINATION – SUMMER 2016

Subject Code:160702 **Date:21/05/2016**

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 data confidentiality,data authentication and data integrity. [7]

(b) With example explain function of s-box in DES. [7]

Q.2 (a) Explain generation of encryption matrix in play fair cipher. [7]

(b) Explain one time pad cipher with example. [7]

OR

(b) Explain Diffie - Hellman key exchange algorithm. [7]

Q.3 (a) Explain rail fence Cipher technique. [7]

(b) Explain various steps of AES in short. [7]

OR

Q.3 (a) What is MAC? Explain HMAC. [7]

(b) Explain RSA algorithm with example. **[7]**

Q.4 (a) Explain authentication mechanism of Kerberos. [7]

(b) Explain use and concept of dual signature in SET. [7]

OR

Q.4 (a) Write a short note on SSL. [7]

(b) Write a short note on 3-D secure protocol. [7]

Q.5 (a) Explain Token authentication. [7]

(b) Write a short note on Pretty Good Privacy (PGP). [7]

OR

Q.5 (a) Explain key distribution using KDC. [7]

(a) Write a short note on IP security. [7]

----------*----------*----------