Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VI (OLD) EXAMINATION WINTER 2017

Subject code: 160702 Date: 20-11-2017

Subject Name: Information 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.**

Q.1 (a) Explain data confidentiality ,data authentication and non-repudiation [7]
(b) Describe mono alphabetic cipher. [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 columnar transposition Cipher technique. [7]

Q.3 (a) Explain working of two wheel rotor machine. [7]
(b) Explain single round of DES. [7]

OR

Q.3 (a) Explain process of MD5 algorithm. [7]
(b) Explain key generation using RSA algorithm. **[7]**

Q.4 (a) Explain inter realm authentication of Kerberos. [7]
(b) Which are various SET participants. [7]

OR

Q.4 (a) Explain HMAC algorithm. [7]
(b) Explain Diffie Hellman key exchange algorithm. [7]

Q.5 (a) Write a short note on S/MIME. [7]
(b) Explain X.509 Directory Authentication Service. [7]

OR

Q.5 (a) Explain transaction on E-commerce. [7]
(a) Write a short note on Pretty Good Privacy. [7]

****