

GUJARAT TECHNOLOGICAL UNIVERSITY**BE - SEMESTER-VI (OLD) EXAMINATION – WINTER 2018****Subject Code:160702****Date: 04/12/2018****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 **07**
(b) What is cryptography? Briefly explain the model of Asymmetric Cryptosystem **07**
- Q.2** (a) Explain monoalphabetic cipher and polyalphabetic cipher by giving an example. **07**
(b) List various modes of operations of block cipher. Explain any three of them **07**
- OR**
- (b) What is the purpose of S-box in DES? Explain the avalanche effect in DES. **07**
- Q.3** (a) What is the limitation of Electronic Codebook Mode (ECB)? explain CBC mode in detail. **07**
(b) Explain public-key cryptosystem in detail. **07**
- OR**
- Q.3** (a) Explain Rail fence Cipher technique. **07**
(b) Describe MD5 message digest algorithm. **07**
- Q.4** (a) What is message authentication code? What are the requirements for MACs? **07**
(b) Briefly explain Diffie-Hellman key exchange. Is it vulnerable to man in the middle attack? Justify. **07**
- OR**
- Q.4** (a) What characteristics are needed in secure hash function? Explain the concept of simple hash function. **07**
(b) What is authentication? How it can be done using cryptography? **07**
- Q.5** (a) Explain the general format of PGP(Pretty Good Privacy) message **07**
(b) What are the requirements of digital signature? Explain the concept of arbitrated digital signature. **07**
- OR**
- Q.5** (a) Explain SSL architecture. **07**
(b) What problem was Kerberos designed to address? Briefly explain how session key is distributed in Kerberos. **07**