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

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VI (OLD) - EXAMINATION – SUMMER 2018

Subject Code:160702 **Date:08/05/2018**

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)**	What is cipher? Explain any two mono alphabetic cipher.	**07**
	(b)	Apply Caesar cipher to encrypt and decrypt the message "ashish". Use key value 12.	**07**
Q.2	**(a)**	Draw and explain simplified model of DES.	**07**
	(b)	What are the various mode of operation of DES?	**07**
		OR	
	(b)	What is S Box? How it works?	**07**
Q.3	**(a)**	Compare public key cryptography with private key cryptography.	**07**
	(b)	Write and explain Euclidean algorithm.	**07**
		OR	
Q.3	**(a)**	Define GCD. Find GCD of 2740 and 1760 using Euclidean algorithm.	**07**
	(b)	Explain encryption and decryption process in asymmetric cryptography.	**07**
Q.4	**(a)**	Explain SSL Session and Connections.	**07**
	(b)	List advantages and disadvantages of firewall.	**07**
		OR	
Q.4	**(a)**	What are the various types of attacks? Explain them in detail.	**07**
	(b)	What is authentication? How it can be done using cryptography?	**07**
Q.5		Write a note on following (any 4)	**14**

1) Hash algorithm
2) Message authentication code
3) Digital signature
4) Man in the middle attack
5) Intrusion detection system

****