Seat No.: ________ **Enrolment No.___________**

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII (NEW) - EXAMINATION – SUMMER 2018

Subject Code:2170709 **Date:01/05/2018**

Subject Name:Information and Network 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.**

			MARKS
Q.1	**(a)**	Explain data confidentiality, data authentication and data integrity.	**03**
	(b)	Describe mono alphabetic cipher.	**04**
	(c)	Explain playfair cipher with example.	**07**
Q.2	**(a)**	Explain one time pad cipher with example.	**03**
	(b)	Explain columnar transposition Cipher technique.	**04**
	(c)	Write a short note on DES.	**07**
		OR	
	(c)	Describe various steps of AES.	**07**
Q.3	**(a)**	Explain key pair generation using RSA algorithm.	**03**
	(b)	Explain encryption and decryption using RSA.	**04**
	(c)	What is digital signature? Explain hash code base digital signature.	**07**
		OR	
Q.3	**(a)**	Explain Diffie Hellman key exchange algorithm.	**03**
	(b)	Explain man in middle attack in Diffie Hellman key exchange	**04**
	(c)	Explain HMAC algorithm.	**07**
Q.4	**(a)**	Explain digital public key certificate format.	**03**
	(b)	Explain double and triple DES.	**04**
	(c)	Explain authentication mechanism of Kerberos.	**07**
		OR	
Q.4	**(a)**	Explain DSA (Digital Signature Algorithm).	**03**
	(b)	Explain various public key distribution techniques.	**04**
	(c)	Write a short note on SSL.	**07**
Q.5	**(a)**	Explain basic Hash code generation.	**03**
	(b)	Explain cipher feedback mode of DES operation.	**04**
	(c)	Write a short note on public key infrastructure.	**07**
		OR	
Q.5	**(a)**	Explain MAC code generation using block cipher.	**03**
	(b)	Explain counter mode of DES operation.	**04**
	(c)	Explain HTTPS and SSH.	**07**

****