Seat No.: _____   Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY
BE - SEMESTER– VII (New) EXAMINATION – WINTER 2019

Subject Code: 2170709   **Date: 26/11/2019**

Subject Name: Information and Network 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)**	Define following principles of security: 1) Confidentiality 2) Integrity 3) Availability	03
	(b)	Describe Rail-fence cipher algorithm with example.	04
	(c)	Explain cryptanalytic attacks with example of any encryption algorithm.	07
Q.2	**(a)**	Explain one time pad algorithm with example and mention its strength and weakness.	03
	(b)	What is the difference between a mono alphabetic cipher and a polyalphabetic cipher?	04
	(c)	Encrypt the message "GTU Examination" using the Hill cipher algorithm with the key matrix $\begin{pmatrix} 5 & 17 \\ 4 & 15 \end{pmatrix}$. Show your calculations and the result.	07

OR

	(c)	Perform encryption in Playfair Cipher algorithm with plain text as "INFORMATION AND NETWORK SECURITY", Keyword is "MONARCHY" (Note: 1.Put j and i both combine as a single field in 5*5 matrix).	07
Q.3	**(a)**	Explain CFB algorithm mode with diagram.	03
	(b)	Describe the Diffie Hellman key exchange Algorithm with example.	04
	(c)	Draw block diagram to show Broad level steps in DES and also give steps of one round in DES with another diagram.	07

OR

Q.3	**(a)**	Explain Counter (CTR) algorithm mode with diagram.	03
	(b)	Differentiate block cipher and stream cipher algorithm with example	04
	(c)	Explain process of encryption in RSA Algorithm with suitable example. (Prime Number P,Q and Encryption Key E is given for reference) P=7, Q=17, E=7	07
Q.4	**(a)**	What are the principal elements of a public-key cryptosystem?	03
	(b)	What is a meet-in-the-middle attack in double DES?	04
	(c)	Briefly describe Mix Columns and Add Round Key in AES algorithm.	07

OR

Q.4	**(a)**	What is the role of a compression function in a hash function?	03
	(b)	What is the main difference between HTTP and HTTPS protocol. When HTTPS is used, which elements of the communication are Encrypted?	04

1

	(c)	Explain working of Secure Hash Algorithm, with basic arithmetical and logical functions used in SHA.	07
Q.5	(a)	Draw Generic Model of Digital Signature Process.	03
	(b)	Explain Elgamal Digital Signature Scheme.	04
	(c)	Describe MAC with its security implications.	07

OR

Q.5	(a)	What problem was Kerberos designed to address?	03
	(b)	Explain Schnorr Digital Signature Scheme.	04
	(c)	Explain use of Public-Key Certificate with diagram and draw X.509 certificate format.	07

****