Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

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

Subject Code: 2170709 **Date: 19/11/2018**

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.**

			MARKS
Q.1	**(a)**	Differentiate block cipher and a stream cipher.	**03**
	(b)	Encrypt the Message "Surgical Strike" with key "GUJAR" using PLAYFAIR technique.	**04**
	(c)	Discuss in detail encryption and decryption process of DES.	**07**
Q.2	**(a)**	Distinguish between Symmetric encryption and Asymmetric encryption using suitable example.	**03**
	(b)	Describe the term: Authentication, Authorization, Integrity and Non – repudiation.	**04**
	(c)	Discuss in detail encryption and decryption process of AES.	**07**
		OR	
	(c)	Encrypt the message "meet me at the usual place " using the Hill cipher with the key $\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$	**07**
Q.3	**(a)**	Explain Avalanche Effect.	**03**
	(b)	Discuss Man in Middle Attack.	**04**
	(c)	Explain in detail RSA algorithm, highlighting its security aspect.	**07**
		OR	
Q.3	**(a)**	Explain the VERNAM Cypher method.	**03**
	(b)	Explain the difference between diffusion and confusion.	**04**
	(c)	Briefly explain Diffie Hellman Key exchange with an example	**07**
Q.4	**(a)**	What is MAC ? How it useful in Crypto System.	**03**
	(b)	Briefly explain Digital Signature algorithm	**04**
	(c)	Described briefly the Authentication process covered by X.509.	**07**
		OR	
Q.4	**(a)**	Discuss HASH function and its application in Crypto System.	**03**
	(b)	Explain Different type of Attacks on Crypto System.	**04**
	(c)	Explain PGP with its Authentication and Confidentiality Operation.	**07**
Q.5	**(a)**	List out the various web security threats.	**03**
	(b)	What is meant by message digest? Give an example.	**04**
	(c)	Discuss clearly Secure Hash Algorithm with its real time application.	**07**
		OR	
Q.5	**(a)**	Explain HAND SHAKE protocol in SSL.	**03**
	(b)	What is KDC? List the duties of a KDC.	**04**
	(c)	Explain digital signature schemes Elgamal and Schnorr.	**07**

****