Seat No.: ________ Enrolment No.___________

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER– VIII EXAMINATION – SUMMER 2020

Subject Code: 2170709 Date:27/10/2020

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)**	Define the terms: Confidentiality, Data integrity, Non-repudiation	**03**
	(b)	Construct a Playfair matrix with the key "engineering". And encrypt the message "impossible".	**04**
	(c)	Define Cryptography and Cryptanalysis. Draw and explain conventional cryptosystem.	**07**
Q.2	**(a)**	Write the differences between conventional encryption and public key encryption.	**03**
	(b)	Write a note on Hill Cipher.	**04**
	(c)	Explain the key generation in DES algorithm.	**07**
		OR	
	(c)	Explain the key generation in AES algorithm.	**07**
Q.3	**(a)**	What is the purpose of the S-boxes in DES? Explain the avalanche effect.	**03**
	(b)	Explain Cipher Block Chaining (CBC) and Electronic Code Book (ECB) block cipher modes of operation with the help of diagram.	**04**
	(c)	Explain X.509 authentication service.	**07**
		OR	
Q.3	**(a)**	What is the difference between a session key and a master key?	**03**
	(b)	Explain Cipher Feedback (CFB) and Output Feedback mode (OFB) block cipher modes of operation with the help of diagram.	**04**
	(c)	Explain authentication mechanism of Kerberos.	**07**
Q.4	**(a)**	What characteristics are needed in a secure hash function?	**03**
	(b)	In a public key system using RSA, the cipher text intercepted is C=10 which is sent to the user whose public key is e=5, n=35. What is the plaintext M?	**04**
	(c)	What do you mean by key distribution? Give at least one method for key distribution with proper illustration.	**07**
		OR	
Q.4	**(a)**	What is the purpose of the State array? How many bytes in State are affected by ShiftRows?	**03**
	(b)	Is message authentication code same as encryption? How message authentication can be done by message authentication code?	**04**
	(c)	Briefly explain Diffie-Hellman key exchange. Is it vulnerable to man in the middle attack? Justify.	**07**
Q.5	**(a)**	Using the Vigenère cipher, encrypt the word "ATTACKATDAWN" using the key "LEMON".	**03**
	(b)	Write a note on HTTPS.	**04**
	(c)	Write a short note on "Digital Signature Algorithm".	**07**
		OR	
Q.5	**(a)**	Explain basic Hash code generation.	**03**
	(b)	How public keys can be distributed.	**04**
	(c)	Explain SSL architecture.	**07**

****