Enrolment No./Seat No_____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII (NEW) EXAMINATION – SUMMER 2024

Subject Code:2170709 Date:28-05-2024

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.**
4. **Simple and non-programmable scientific calculators are allowed.**

			Marks
Q.1	**(a)**	List out active attacks. Using an example, describe any one attack.	**03**
	(b)	With an example, describe the Railfence transposition technique.	**04**
	(c)	Write down the steps required to convert plaintext to ciphertext using the Playfair cypher. Use the Playfair cypher algorithm to convert the given plaintext to ciphertext. PT: COMPUTATION, KEY: WORLD	**07**
Q.2	**(a)**	Differentiate stream cipher and block cipher.	**03**
	(b)	How powerful is DES? Discuss its strength in detail.	**04**
	(c)	Discuss in detail: round function of DES.	**07**
		OR	
	(c)	Discuss in detail: round function of AES.	**07**
Q.3	**(a)**	Briefly explain Man-in-the-middle attack.	**03**
	(b)	Use the Diffie-Hellman algorithm and solve the following example. q=23, α=5, X_A=6, X_B=4, Y_A=?, Y_B=?, Secret Key K=?	**04**
	(c)	Explain encryption and decryption process of cipher feedback mode with diagram.	**07**
		OR	
Q.3	**(a)**	Discuss Double DES.	**03**
	(b)	Use the RSA algorithm and solve the following example. p=17, q=11, e=7, M=15, d=?, CT=?	**04**
	(c)	Explain encryption and decryption process of output feedback mode with diagram.	**07**
Q.4	**(a)**	What is digital signature? Discuss the attacks possible on digital signature.	**03**
	(b)	Define MAC. Explain the concept of authentication and confidentiality using MAC.	**04**
	(c)	Define simple Hash function and discuss the security requirements for Hash functions.	**07**
		OR	
Q.4	**(a)**	Why message authentication is needed in security?	**03**
	(b)	Why signing and verifying properties play important role in digital signature?	**04**

	(c)	Discuss round function of SHA-512.	**07**
Q.5	**(a)**	List out the requirements of Kerberos.	**03**
	(b)	Explain public key authority with diagram.	**04**
	(c)	What is secure shell? Explain it in detail.	**07**

OR

Q.5	**(a)**	Define the following terms: KDC, TGS and TGT.	**03**
	(b)	Explain public key certificates with diagram.	**04**
	(c)	Define SSL. Explain SSL protocol stack in detail.	**07**