Enrolment No./Seat No_____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE- SEMESTER–VII EXAMINATION – WINTER 2025

Subject Code:2170709 Date:26-11-2025

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

			MARKS
Q.1	**(a)**	Explain data confidentiality, data authentication and data integrity.	**03**
	(b)	Differentiate symmetric and asymmetric key cryptography. Draw the design model of symmetric key cryptography.	**04**
	(c)	Explain play fair cipher with example.	**07**
Q.2	**(a)**	Compare and contrast symmetric key cryptography and asymmetric key cryptography.	**03**
	(b)	Explain columnar transposition Cipher technique.	**04**
	(c)	Describe various steps of AES	**07**
		OR	
	(c)	Write a short note on DES	**07**
Q.3	**(a)**	How meet in the middle attack is performed on double DES?	**03**
	(b)	Explain public key cryptosystem with neat diagram	**04**
	(c)	Explain authentication mechanism of Kerberos	**07**
		OR	
Q.3	**(a)**	What is the difference between weak and strong collision resistance? Consider the hash functions based on cipher block chaining, What kind of attack can occur on this?	**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 encryption and decryption using RSA with example.	**07**
Q.4	**(a)**	Explain digital public key certificate format.	**03**
	(b)	Write a short note on Man-in-the-middle attack	**04**
	(c)	Explain the logic of SHA(Secure Hash Algorithm).	**07**
		OR	
Q.4	**(a)**	Why HASH function is required in cryptography?	**03**
	(b)	Explain various public key distribution techniques	**04**
	(c)	Briefly explain Diffie-Hellman key exchange with example.	**07**
Q.5	**(a)**	Define the parameters that define SSL session state and session connection.	**03**
	(b)	What is defined by X.509 certificate? Write the process of authentication in X.509.	**04**
	(c)	Explain SSL architecture	**07**
		OR	
Q.5	**(a)**	Explain MAC code generation using block cipher	**03**
	(b)	What problem was Kerberos designed to address? What are the three threats associated with user authentication over a network or Internet?	**04**
	(c)	Explain digital signature schemes Elgamal and Schnorr	**07**

****