

Seat No.: _____

Enrolment No. _____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE – SEMESTER- VII EXAMINATION-SUMMER 2023

Subject Code: 2170709

Date: 28/06/2023

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 various cryptanalytic attacks on encrypted message.	03
	(b) Explain mono alphabetic cipher with example.	04
	(c) Discuss in detail encryption and decryption process of DES.	07
Q.2	(a) Differentiate between block cipher and stream cipher.	03
	(b) Justify “CFB(Cipher feedback mode) encrypted messages are less subject to tampering than OFB(Output feedback mode)”.	04
	(c) Explain how DES(Data Encryption standard) algorithm observes Fiestel structure. Explain key generation and use of S-box in DES algorithm.	07
	OR	
	(c) Draw neat diagram of AES key generation. Explain encryption process of AES.	07
Q.3	(a) Define MAC. Explain how it useful in cryptosystem.	03
	(b) Explain man in the middle attack.	04
	(c) Explain diffie-hellman key exchange mechanism with suitable example	07
	OR	
Q.3	(a) Define trap-door one way function. Describe its use in cryptography.	03
	(b) Perform encryption and decryption using RSA algorithm for following: $p=3; q=11, e=7; M=2$	04
	(c) Write design objectives of HMAC and explain HMAC in detail.	07
Q.4	(a) Discuss various public key distribution techniques.	03
	(b) Define Digital Signature. Mention the requirements of Digital Signature.	04
	(c) Explain the logic of SHA (Secure Hash Algorithm).	07
	OR	
Q.4	(a) Define TGT. Explain its use in Kerberos.	03
	(b) Explain Hash function based on Cipher Block Chaining.	04
	(c) Write a brief note on X509 certificate.	07
Q.5	(a) Explain Hand Shake protocol in SSL.	03
	(b) Write a short note on HTTPS.	04
	(c) Describe Elgamal Digital Signature.	07
	OR	
Q.5	(a) Describe types of security threats that are faced by user while using the web.	03
	(b) Draw Generic Model of Digital Signature Process.	04
	(c) Write a short note on public key infrastructure	07
