

GUJARAT TECHNOLOGICAL UNIVERSITY**BE - SEMESTER-VI (NEW) EXAMINATION – SUMMER 2024****Subject Code:3164204****Date:22-05-2024****Subject Name:Data 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) List and explain any three security mechanisms.	03
	(b) Differentiate known plaintext and chosen plaintext attack. Consider following scenario: Bob secretly gets access to Alice's computer and using her cipher encrypts plain text "security compromised". Bob gets "SRCRSEIOOECTMMDUYPI" as cipher text. What type of attack Bob is launching? If rail fence cipher is used for encryption, what is the depth of rail fence used by Alice?	04
	(c) Explain playfair cipher. Encrypt the plaintext message "communication" with the key "chandrayaan" using playfair cipher. Discuss how playfair cipher provides security against frequency analysis.	07
Q.2	(a) Differentiate diffusion and confusion.	03
	(b) Explain following modes of operation (i) Cipher Block Chaining Mode (ii) Electronic Codebook Mode	04
	(c) Explain single round of DES encryption.	07
	OR	
	(c) Explain different stages of AES structure.	07
Q.3	(a) Explain any three possible security attacks on RSA algorithm.	03
	(b) Decrypt the cipher text "VZLQJWDFRCDHJ" applying the Vigenère cipher, using the key "GOLD".	04
	(c) P and Q are two prime numbers. P=5, and Q=11. Take public key E=7. If plain text value is 2, then what will be the private key and cipher text value according to RSA algorithm? Explain in detail.	07
	OR	
Q.3	(a) Describe applications of public key cryptosystems.	03
	(b) Encrypt the message "full" using the Hill Cipher with key $\begin{bmatrix} 3 & 1 \\ 6 & 5 \end{bmatrix}$	04
	(c) Explain in detail man-in-the-middle attack on Diffie-Hellman Key Exchange.	07
Q.4	(a) Explain any one simple hash function.	03
	(b) What is MAC? How it is useful in cryptosystem? Is it same as encryption? Justify.	04
	(c) What is message digest? Briefly explain how it is generated in SHA-512.	07
	OR	
Q.4	(a) Explain strong collision resistant property of hash function.	03
	(b) Explain MAC based on cipher block chaining.	04

- (c) Discuss the ways in which hash code can be used to provide message authentication. **07**
- Q.5** (a) What is a nonce? Differentiate session key and master key. **03**
(b) List the requirements for a digital signature. **04**
(c) Write short note on X509 certificate. **07**
- OR**
- Q.5** (a) Explain use of Ticket Granting Server (TGS) in Kerberos. **03**
(b) Explain symmetric key distribution with confidentiality and authentication. **04**
(c) Describe Schnorr digital signature scheme. **07**
