

GUJARAT TECHNOLOGICAL UNIVERSITY**BE- SEMESTER-VI (NEW) EXAMINATION – WINTER 2024****Subject Code:3164204****Date:02-12-2024****Subject Name: Data 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) Discuss about following Security Principles a) Integrity b) Non-Repudiation c) Availability	03
	(b) Differentiate Mono-Alphabetic and Poly-alphabetic Cipher.	04
	(c) Decrypt the following Encrypted message using playfair Cipher Technique. Encrypted Message: “XFOLIXMKPVLR” Keyword: “PLAYFAIR EXAMPLE”	07
Q.2	(a) Find $(939)^{-1} \bmod 26$ using Extended Euclidean algorithm.	03
	(b) Differentiate public key cryptography and private key cryptography.	04
	(c) Discuss the difference between Output Feedback mode (OFB) and Counter (CTR) mode of block ciphers with appropriate diagram.	07
	OR	
	(c) Illustrate the working of Electronic Codebook (ECB) and Cipher Block Chaining mode of block ciphers with diagram.	07
Q.3	(a) Given a block cipher with a specific block size, explain how this block size affects the encryption process.	03
	(b) Name and briefly describe two fundamental design principles of block ciphers.	04
	(c) Draw the diagram of broad level steps of DES algorithm and explain S-box substitution with example.	07
	OR	
Q.3	(a) Define a public key cryptosystem and mention one of its applications.	03
	(b) Illustrate the four main transformation functions used in AES.	04
	(c) Given a scenario where an attacker intercepts communication between two users, explain how a Man-in-the-Middle attack could be carried out.	07
Q.4	(a) Define confusion and diffusion with respect to data security.	03
	(b) Discuss the attacks on the RSA algorithm, including blinding attacks and chosen ciphertext attacks.	04
	(c) Generate the common key using Diffie-Hellman key exchange algorithm. Show the complete process of key generation by taking suitable example.	07
	OR	
Q.4	(a) Define a hash function and list two examples of simple hash functions.	03
	(b) Given a message, explain how a cryptographic hash function could be used to verify the integrity of that message.	04
	(c) Show the encryption of message 47 and 98 using RSA algorithm. Decide the suitable public key and private key of RSA algorithm.	07

- Q.5** (a) Explain how a MAC provides both message integrity and authenticity. **03**
(b) List the steps involved in distributing a symmetric key using asymmetric encryption. **04**
(c) Discuss how Public Key Infrastructure (PKI) ensures the secure distribution and verification of public keys. What are the key components of a PKI? **07**

OR

- Q.5** (a) Identify one advantage of using the Schnorr signature scheme over the ElGamal signature scheme. **03**
(b) Explain how an HMAC differs from a simple hash function in ensuring message integrity. **04**
(c) Outline the structure of an X.509 certificate and its role in ensuring the authenticity of public keys. **07**
