Seat No.: _____ Enrolment No._____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE – SEMESTER- VII EXAMINATION-SUMMER 2023

Subject Code: 3170720 Date: 19/06/2023

Subject Name: Information 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 following terms: non-repudiation, integrity, masquerade	**03**
	(b)	Encrypt the message "attc" with the following key using Hill cipher. $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$	**04**
	(c)	Explain playfair cipher. Encrypt the plain-text message "helloe jassmin" using playfair cipher. Use the keyword "cipherj". (There is no 'j' in the table. Any 'j' in the plaintext is replaced by 'i'.)	**07**
Q.2	**(a)**	Discuss Electronic Code Book mode and Counter mode in detail.	**03**
	(b)	Write difference between Block vs Stream Ciphers. Explain following terms in context of cryptography: confusion and diffusion	**04**
	(c)	Explain DES round structure in detail.	**07**
		OR	
	(c)	Write a note on Advanced Encryption Standard(AES).	**07**
Q.3	**(a)**	Write difference between conventional encryption and public-key encryption	**03**
	(b)	Explain man-in-the middle attack on Diffie-Hellman key exchange.	**04**
	(c)	Explain RSA algorithm in detail. Perform encryption and decryption using RSA algorithm for prime numbers p=3 & q=11, plaintext message m is 2.	**07**
		OR	
Q.3	**(a)**	Explain following terms: Avalanche Effect, Cryptanalysis	**03**
	(b)	Discuss possible approaches to attack RSA.	**04**
	(c)	Explain the Deffie Hellman key exchange scheme in detail. In a Diffie-Hellman Key Exchange, Alice and Bob have chosen prime value q = 17 and primitive root = 5. If Alice's secret key is 4 and Bob's secret key is 6, what is the secret key they exchanged?	**07**
Q.4	**(a)**	Compare and contrast – MAC VS Encryption functions. In MAC, if 80-bit key is used and the tag is 32 bits, then after how many rounds attacker will produce a key, which must be the one used by the sender ?	**03**
	(b)	Explain working of Cipher-based Message Authentication Code and Data Authentication Algorithm.	**04**
	(c)	Explain the working of Secure Hash Algorithm-512 in detail.	**07**
		OR	
Q.4	**(a)**	Discuss three applications of hash functions.	**03**

	(b)	Discuss Hash function and its requirements.	**04**
	(c)	Write the algorithm for message authentication code based on HASH functions. Also discuss its efficient implementation approach.	**07**
Q.5	**(a)**	Draw X.509 certificate format. Enlist the reasons to revoke the certificate before expiry.	**03**
	(b)	Explain different ways to distribute symmetric key using symmetric and asymmetric encryptions.	**04**
	(c)	Enlist requirements of Kerberos. Enlist and explain roles of various servers are used in Kerberos. Explain through diagram, how Kerberos can communication with other administrative domains for providing trusted services to the clients.	**07**

OR

Q.5	**(a)**	Explain briefly: Linear and Differential Cryptanalysis	**03**
	(b)	Explain various general categories of schemes for the distribution of public keys.	**04**
	(c)	Define Digital signature. Explain digital signature algorithm.	**07**

****