Enrolment No./Seat No_____

GUJARAT TECHNOLOGICAL UNIVERSITY

BE - SEMESTER–VII (NEW) EXAMINATION – SUMMER 2024

Subject Code:3170720 Date:01-06-2024

Subject Name:Information 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)**	List and explain different types of attacks.	**03**
	(b)	Explain Caesar cipher algorithm with the help of example.	**04**
	(c)	List and explain different mode of operation used for encryption and decryption.	**07**
Q.2	**(a)**	List use of public key cryptography	**03**
	(b)	Write steps for sub key generation in DES	**04**
	(c)	Explain DES encryption.	**07**
		OR	
	(c)	List and explain possible attacks on DES.	**07**
Q.3	**(a)**	List requirements of public key cryptography.	**03**
	(b)	How same key can be calculated in diffi hellman key exchange algorithm.	**04**
	(c)	Explain key generation of RSA algorithm	**07**
		OR	
Q.3	**(a)**	Write Euclid algorithm.	**03**
	(b)	Discuss security of diffi hellman key exchange algorithm.	**04**
	(c)	Write down the algorithm used for calculation exponentiation efficiently. Also give example.	**07**
Q.4	**(a)**	What is authentication? How can we implement message authentication?	**03**
	(b)	List and explain requirements of secure hash function	**04**
	(c)	List basic uses of Hash function.	**07**
		OR	
Q.4	**(a)**	Define weak collision resistance and strong collision resistance.	**03**
	(b)	Draw message digest generation using SHA 512 algorithm.	**04**
	(c)	Explain message authentication based on DES.	**07**
Q.5	**(a)**	Define Mutual authentication with example.	**03**
	(b)	How public key cryptography can be used for Digital signature? Explain.	**04**
	(c)	Draw and explain DSS approach for digital signature.	**07**
		OR	
Q.5	**(a)**	List and explain various key distribution approach of symmetric key cryptography.	**03**
	(b)	Discuss the security of digital signature.	**04**
	(c)	What is replay attack? How can we avoid this attack using digital signature?	**07**

****