Seat No.: ________ Enrolment No.______________

GUJARAT TECHNOLOGICAL UNIVERSITY

MCA INTEGRATED– SEMESTER - VIII EXAMINATION- SUMMER-2023

Subject Code: 4480603 **Date: 20/06/2023**

Subject Name: 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. Use of simple calculators and non-programmable scientific calculators are permitted

Q.1	**(a)**	Answers the following: 1. Give one use case of passive and an active attack. 2. What is a clear signed message in SMIME? 3. What do you mean by Asymmetric encryption? 4. Differentiate Transport and Tunnel Mode in Ipsec. 5. What is a honey pot? 6. Write name of any two block Cipher algorithms. 7. Explain the term “Salt”.	**07**
	(b)	Mention and very briefly explain design features/parameters considered while designing the symmetric block cipher.	**07**
Q.2	**(a)**	1. Compare DES, 3DES and AES. (3) 2. List different fields of Authentication Header.(4)	**07**
	(b)	Why is the mode of operation defined? Explain any two cipher block modes of operations.	**07**
		OR	
	(b)	1. Write two important advantages of public key cryptography over shared secret key based cryptography. (3) 2. How MAC is calculated using a one-way hash function? (4)	**07**
Q.3	**(a)**	Briefly explain the structure/format indicating the different fields of Public Key Ring in PGP.	**07**
	(b)	What is the need of a Hash function? Explain SHA512 algorithm with a suitable diagram.	**07**
		OR	
Q.3	**(a)**	Explain RSA public key encryption algorithm using suitable examples.	**07**
	(b)	Explain pseudo random function and cryptographic computation of TLS with suitable diagrams.	**07**
Q.4	**(a)**	Explain the public key ring and its structure with a suitable diagram.	**07**
	(b)	What is IPSec? What are the applications of IPSec? Explain the modes of IPSec operations.	**07**
		OR	
Q.4	**(a)**	Explain ESP packet format in detail with suitable examples.	**07**
	(b)	Why is web security a more important issue today? List at least four reasons for the same.	**07**

Q.5 **(a)** Explain types of firewalls in detail using suitable diagrams. **07**

(b) 1. Explain how one can use Markov model for proactive password checking. (3) **07**

2. What do you mean by false positive and false negative in an Intrusion Detection System? (4)

OR

Q.5 **(a)** Explain how attacks like IP address spoofing, source routing and tiny fragments can be carried out on packet filtering routers? What are the countermeasures? **07**

(b) Explain the three parts and four phases of computer viruses. **07**

****