Enrollment No._____

NAVRACHANA UNIVERSITY
a UGC recognized University

School: School of Engineering and Technology
Program/s: Computer Science & Engineering
Year: 3rd **Semester:** 6th
Examination: End Semester Examination
Examination year: May - 2023

Course Code: CS321 **Course Name:** Information Security
Date: 18/05/2023
Time: 2:00 pm to 4:00 pm

Total Marks: 40
Total Pages: 2

Instructions:

- *Write each answer on a new page.*
- *Use of a calculator is permitted.*

Q. No.	Details	Marks	COs*	BTL#
Q.1	**Very Short Answer Type Questions - All are compulsory. (2 Marks for each)**	10		
	1. What is the difference between substitution cipher and transposition cipher?		CO1	BT1
	2. Define the terms threat and attack with an example.		CO3	BT1, BT2
	3. Describe the term: Authentication, Authorization, Integrity and Non – repudiation		CO2	BT1
	4. What is the difference between weak and strong collision resistance?		CO1	BT1, BT2
	5. Difference between block cipher and stream cipher.		CO1	BT1
Q.2	**Short Answer Type Questions - Attempt any 5 questions. (3 Marks for each)**	15		
	1. Differentiate symmetric and asymmetric key cryptography with an example.		CO1, CO4	BT1, BT4
	2. Briefly explain Diffie-Hellman Key Exchange. Is it vulnerable to man in middle attack? Justify.		CO1, CO3	BT1, BT4
	3. Is a message Authentication code (MAC) function is similar to encryption? Does MAC provide authentication or confidentiality? Justify your answer.		CO2	BT2, BT3, BT4
	4. How the Kerberos will provide the central authentication between server and user? Explain with diagram.		CO2, CO4	BT1, BT6
	5. Briefly explain authentication factors and authentication methods.		CO2	BT1
	6. Encrypt the plaintext "attack", using Hill cipher for the given key= [2 3] [3 6]		CO1	BT5, BT6
	7. Explain Multiple level Security Models and also differentiate the difference between the two models.		CO4	BT1, BT4
Q.3	**Long Answer Type Questions - Attempt any 3 questions. (5 Marks for each)**	15		
	1. Explain how DES (Data Encryption Standard) algorithm observes Fiestel structure. Explain key generation and use of S-box in DES algorithm.		CO1	BT1
	2. Differentiate between hashing and encryption. What are the practical applications of hashing? Compare MD5 and SHA-1 hashing algorithms.		CO1, CO2	BT1, BT2

	3. List the security services provided by digital signature. Write and explain the Digital Signature Standard (DSS) and also explain the signing and verifying function.		CO1	BT1
	4. Write a note on following: a) Single Sign-On b) X.509 Certificate		CO2	BT1, BT4
	5. a) Please consider prime numbers 7 and 11 to generate the public and private keys and encrypt plaintext 9 using the RSA public-key encryption algorithm. b) For Diffie-Hellman algorithm, two publically known numbers are prime number 23 and primitive root (g) of it is 9. A selects the random integer 4 and B selects 3. Compute the public key of A and B. Also compute common secret key.		CO1, CO4	BT4, BT5, BT6

**********End of Question Paper**********