VIT

Vellore Institute of Technology

(Deemed to be University under section 3 of UGC Act, 1956)

Continuous Assessment Test-2(CAT-2) – March 2023

Programme	:	M. Tech Int. CSE(Business Analytics)	Semester	:		Win 2022-23
Course Title	:	Network Security and Cryptography Fundamentals	Code	:		CSE1029
			Slot	:		D1
Faculty	:	Dr. R. Sendhil , Dr. C. Balaji	Class Nbr	:		CH2022235001919 CH2022235001916
Duration	:	1 hour 30 mins	Max. Marks	:		50

Answer all the Questions

Ques. No.	Sub sec	Question Description	Marks
1.		Privacy and security issues such as Confidentiality, Integrity, and Availability (CIA) are associated with the electronic medical record storage and transmission of medical data. Describe at least two kinds of people and situation that could threaten CIA possession.	[10]
2.	a.	Consider a system that allows weak passwords to enter the secure database where all the confidential information of the company is stored. Identify the possible threats, Vulnerabilities and Risks present in this system and explain it with example. (5 marks)	[10]
	b.	A spy needs to send a secret message to their handler using a row-column based transposition technique. The message is "MEET ME TONIGHT AT THE PARK" and the key is "3,1,4,2". Find the Ciphertext for the above Plaintext. (5 marks)	
3.	a.	Is PLAYFAIR CIPHER a stream or block cipher? Perform decryption for Ciphertext "TUOBDPBMOMPDAW" using the key "ORANGE". (5 marks)	[10]
	b.	Using CAESAR CIPHER, Encrypt the following Plaintext with key=6, Plaintext: "Continuous Assessment Test". (5marks)	
4.	a.	Use the matrix form of key= $\begin{pmatrix} 17 & 5 & 17 \\ 21 & 21 & 18 \\ 19 & 2 & 2 \end{pmatrix}$ (mod26) to encrypt the message "NUMBER" based on hill cipher. (5 marks)	[10]
	b.	Find the inverse of the key. (5 marks)	
5.		What is the output of the first round of the DES algorithm when the plaintext and the key are both all zeros?	[10]

****