ASSIGNMENT-1

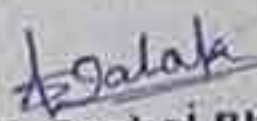| Subject	:	Cryptography & Network Security (BTCT701T)	Semester	:	VII – A and B
Subject Teacher	:	Prof. P. U. Tembhare	Prof. Snehal Bhujade	Assignment No.	:	1
Unit	:	I, II and III	Date of Display	:	21-08-2023

Course Outcomes:

After completing the course, students will be able to :

CO1 : To develop the student's ability to understand the concept of security goals in various applications and learn classical encryption techniques.

CO2 : To apply fundamental knowledge on cryptographic mathematics used in various symmetric and asymmetric key cryptography.

CO3 : To develop the student's ability to analyze the cryptographic algorithms.

Sr. No.	Que. No.		Questions	Mapping with CO	BT Level
1	1.		Apply Extended Euclid algorithm to compute GCD (99,78). Show all the computations.	CO1	III
2	2.	a)	What is Vigenere Cipher? Explain it's working using suitable example.	CO1	II
	2.	b)	Demonstrate the working of encryption and decryption procedure in Hill Cipher with respect to following parameters: Plain Text : ACOLLEGE Key : $\begin{bmatrix} 7 & 8 \\ 19 & 3 \end{bmatrix}$	CO1	III
3	3.		Explain Key Calculation Procedure in Simplified DES algorithm.	CO2	III
4	4.		Explain in detail about encryption procedure in IDEA algorithm.	CO2	II
5	5.		Demonstrate the working of RSA decryption algorithm with following parameters: Cipher Text C = 10 Public Key (e,n) = (5,35)	CO3	III
6	6.		Apply the Chinese Remainder Theorem to solve following congruent equations. $X \equiv 2 \pmod 3$ $X \equiv 3 \pmod 5$ $X \equiv 2 \pmod 7$	CO3	II

Prof. P. U. Tembhare |
Subject Teachers

Prof. Snehal Bhujade

Dr.(Mrs.) N. M. Thakare
HOD, CT

Head of Department,
Dept. of Computer Technology
Priyadarshini College of Engineering
Hingna Road, Nagpur-10