VIT Vidyalankar Institute of Technology Accredited A+ by NAAC (Autonomous College Affiliated to University of Mumbai)	*Weekly Test-1 (R-2022 Scheme) -(2023-24)*

Date:	Time: 1 Hr.	Branch: CMPN
Semester: 6	Subject: CSS Test 1	Marks: 30

Q. 1)	Attempt any Five (2 Marks Each)	CO	BL
a)	What to do in Playfair Cipher when If both the letters are neither in the same column nor in same row?	CO1	L2
b)	What is the difference between Authentication and Authorization?	CO4	L1
c)	Why end to end encryption is two ways?	CO1	L2
d)	Which are the threats that causes loss of all three goals of security, show with example.	CO1	L1
e)	Which key is used to verify the digital signature by CA?	CO4	L2
f)	What is 3D's of security?	CO1	L1
g)	A hacker locks out users and encrypts their personal computer files and data, holding it hostage until they agree to pay to the attacker. What is this practice called?	CO1	L3
h)	Encrypt the plain text "VIDYLANKAR" using Caesar Cipher. (n=3)	CO1	L3
Q. 2)	Attempt anyone (10 Marks Each)		
a)	Apply keyless transposition using key=3 for the plaintext "TECOMPUTERENGG"	CO1	L2
b)	What is Euclid's algorithm is used for? Write the algorithm and apply the same on (80,105)	CO1	L3
Q 3)	Attempt anyone (10 Marks Each)		
a)	Server A needs to prove its identity to client, how the digital certificate is created by the server and authorized by Certification Authority? Show the detailed steps between server and CA.	CO4	L3
b)	Discuss the RSA algorithm is used to create digital signature.	CO4	L2

CO1	Understand system security goals and concepts, classical encryption techniques and acquire fundamental knowledge on the concepts of modular arithmetic and number theory.
CO4	Apply different digital signature algorithms to achieve authentication and design secure applications.