VIT Vidyalankar Institute of Technology
Accredited A+ by NAAC
(Autonomous College Affiliated to University of Mumbai)

Weekly Test Examination (R2022 scheme) -(2023-24)

Date: 11/3/24	Time: 1 Hr.	Branch: CMPN
Semester: 6	Subject: CSS Test 2	Marks: 30

Q. 1)	Attempt any Five (2 Marks Each)	CO	BL
a)	Define the terms in Kerberos algorithm: TGS and TGT	CO2	L1
b)	If client A generates Nonce 45 as challenge, show how this is shared with client B & what client B will give as response.	CO2	L2
c)	Given C=E(K1,D(K2,E(K3,P))) what will be the steps to calculate P?	CO2	L3
d)	How to perform triple DES operation using only 2 keys? Demonstrate using diagram.	CO2	L1
e)	How many iterations are performed by RC4 for key scheduling and key stream generation?	CO2	L1
f)	Perform encryption using RC4 for Plain text {142,90} with key {63,57}	CO2	L3
g)	AES needs how may rounds of operation for 128 bits and 192 bits of block cipher?	CO2	L1
h)	Needham-Schroeder algorithm is used for sharing which type of key & who is responsible to create & share that?	CO2	L2
Q. 2)	Attempt anyone (10 Marks Each)		
a)	Client A wants to communicate with server S, A wants KDC to authenticate it and generate the Client Server Session key for such communication. Show how Needham Schroeder algorithm will do these operations.	CO2	L2
b)	Calculate the cipher text for {10110011,11001100,10110111,11000011} using knapsack algorithm having public key E={1,4,6,9,30,50,70,90}	CO2	L3
Q 3)	Attempt anyone (10 Marks Each)		
a)	Show session key generation using Diffie Hellman for q=13 and a(alpha)=6, assume suitable Private key (XA & XB), generate public key (YA &YB) and session key (S).	CO2	L2
b)	What is DES? How it works with Abstract block diagram? Show with diagram what happens in every round i.e. how L and R sub blocks are created?	CO2	L3

CO2	Understand, compare, and apply different encryption and decryption techniques to solve problems related to confidentiality and authentication.