(Autonomous College Affiliated to University of Mumbai)

End Semester Exam

Nov – Dec 2021

Program: B.Tech

Examination: TY Semester: V

Course Code: 1UTTC502 and Course Name: Computer Network Security

Duration: 03 Hours   Max. Marks: 60

Instructions:
(1) All questions are compulsory.
(2) Draw neat diagrams wherever applicable.
(3) Assume suitable data, if necessary.

		Max. Marks	CO	BT level
Q 1	Solve any six questions out of eight	12		
i)	Distinguish between passive attack from active attack with example	2	CO1	U
ii)	Explain two basic functions used in encryption algorithms.	2	CO1	U
iii)	Describe an avalanche effect.	2	CO2	U
iv)	Explain a Substitute byte transformation in AES.	2	CO2	U
v)	Describe Trojan horse attack.	2	CO3	U
vi)	Explain the steps involved in SSL required protocol.	2	CO4	U
vii)	List the design goals of firewalls.	2	CO6	U
viii)	Define the principal elements of NAC.	2	CO5	U
Q.2	Solve any four questions out of six.	16		
i)	Describe digital signature.	4	CO2	U
ii)	Describe the benefits and services provided by IPSec.	4	CO4	U

iii)	Explain various types of viruses.	4	CO3	U
iv)	Illustrate OSI Security architecture model with neat diagram	4	CO1	A
v)	Explain implementation of NAC solution.	4	CO5	U
vi)	Explain the types of Intrusion Prevention System.	4	CO6	U
Q.3	**Solve any two questions out of three.**	16		
i)	Explain IP Security architecture. Show how ESP works in transport and tunnel mode.	8	CO4	U

ii)	Perform encryption and decryption on below:
	   1. Affine cipher:
	       Message: PASCAL Key: (9,2)
	
	Perform encryption on below:
	   2. Keyed Transposition cipher:
	       Message: Live life cleaner by making Earth greener
	       Key: (3,1,6,4,5,7,2)
		5
		
		3
			CO1	A

iii)	Explain configuration management and SNMPv3.	8	CO5	U
Q.4	**Solve any two questions out of three.**	16		
i)	Illustrate the generation of public and private keys and hence generation of cipher text through RSA with the help of example	8	CO2	A
ii)	Explain in detail phishing, backdoors, rootkits and zombie.	8	CO3	U
iii)	An organization named "ABC" wants to implement IDS for security reasons, compare different configuration of IDS and suggest suitable for organization.	8	CO6	An