MANAV RACHNA
Vidyanatariksha

MANAV RACHNA UNIVERSITY
(FORMERLY MANAV RACHNA COLLEGE OF ENGINEERING
NAAC ACCREDITED 'A' GRADE INSTITUTION)
Declared as State Private University under section 2f of the UGC act, 1956

DEPARTMENT OF COMPUTER SCIENCE & TECHNOLOGY

"T3-Examination, May-2018"

Semester:6th
Subject:Network Security & Cryptograhy
Branch: CST
Course Type: Core
Time: 3 Hours
Max.Marks: 80

Date of Exam:24/05/2018
Subject Code:CSH329-T
Session: I
Course Nature: Hard
Program: B.Tech
Signature: HOD/Associate HOD:

PART-A

All questions are compulsory.

Q1(a). What do you mean by DOS attack? (10*2=20)
(b). Briefly explain web security threats.
(c). Discuss the following term in brief
(i) Authentication (ii) Data Integrity
(d). Briefly explain HTTPS.
(e). Define birthday attack.
(f). What services are provided by IPSec?
(g). What is a VPN?
(h). Difference between Firewall and antivirus.
(i). What is phishing used for.
(j). What is the NAT?

PART-B

Attempt any two questions.

Q2(a). In RSA, given N=187 and the encryption Key (E) as 17, Find out the corresponding private key (D). (10)
(b). Briefly explain the knapsack algorithm. (5)

Q3(a). Describe about Encryption and write the applications which uses IDEA. (10)
(b). Briefly explain Secure Socket Layer (SSL). (5)

Q4(a). Explain the Time Stamp based protocol in detail. (10)
(b). What do you mean by MD5? Explain with example. (5)

****

PART-C

Attempt any two questions.

Q5(a). List the characteristics of a good Firewall implementation. (8)

(b). What are the applications and advantages of IP security. (7)

Q6(a). Explain VPN architecture in detail. (8)

(b). What is the main difference between a DDOS attack and a DOS attack? Briefly explain. (7)

Q7. Write a short note on: (5*3=15)

(a). Phishing and Pharming attack

(b). Unbreakable Code

(c). Single Sign on

****