



AJEENKYA

D Y PATIL UNIVERSITY

End Term Examinations (April/ May 2019)

School: School of Engineering

Program: B.Tech. - CTIS

Course: Network Security Basics

Course Code: CSC 228

Semester: IV

Max Marks: 30

Duration (mins): 60

Note- 1. Figures to the right indicates full marks.

2. Attempt any three questions.

- Q1. a) Explain the following triads: Security triad, Information Security triad and hacker's triad. (5)
b) Alice and Bob want to establish a secret key using the Diffie-Hellman Key Exchange protocol. Assuming the values as $n=11$, $g=7$, $x=3$, $y=6$. Find out the values of A, B and the secret key (K1 and K2). (5)
- Q2. a) Describe the concept of Public Key Infrastructure (PKI). (5)
b) Explain Kerberos with the help of diagram. (5)
- Q3. a) Define the following terms with respect to firewall: White-listing and Black-listing. (2)
b) Define switch and its types. Why does switch differs from Hub? (8)
- Q4. a) What is Secure Socket Layer (SSL) and explain the various protocols used in it. (5)
b) Explain Virtual Private Network (VPN). How does VPN service differs from proxy service? (5)
- Q5. a) Define Intrusion Detection System and Intrusion Prevention System. (2)
b) Explain the types of Intrusion Detection System. (3)
c) Explain Digital Signature and why does it differ from asymmetric key cryptography? (5)

*****ALL THE BEST*****