Date: / /

Ques 1 :→

kerberos :→

→ It is a Computer network authentication protocols that work on the basis of tickets to allow node communication over a na-secure network to prove their identity to one another in a secure manner.

→ kerberos builds on Symmetric key Cyptography and requires a trusted third party.

kerberos principales

1. A service or user name
2. An instance name
3. A realm name.

Recurirments :→

1 Secure
2. Reliable

Date: / /

3. Transparent

4. Scalable.

~~X.50~~

X.509 :→

→ It is the part of X.500 Directory service

→ Issued in 1988. revised in 1993 and 1995

→ Defines a framework and Authentication service using the X.500 directory

→ Repository of public key certificates

→ Based on use of public key cryptography and digital signatures

→ Recommends use of RSA.