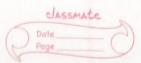
Assignment



Name: Abhiroop Mukharjee

Enrolment No.: 510519 109

Q) why should me trust digital contificate?

- Digital Certificates are made to signify that the association between pho's public key and it's owner is legitimate and is not false.

We should trust digital cartificates as they have the bublic key and coressponding owner has been tested for it's authenticity be trusted Cartification Authorities (CA) like Verisign & and Entrust.

Q2) How does CA sign a digital certificate?

→ given that an user gives wants to get a digital cartificate for his/har public key, the Certification Authorities tests the person and coressponding public key with a "proof of possesstion" test.

- This test can be done in two ways

i) > End User gives two things to the Certification Authority

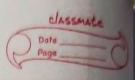
a) His/Her public key

by his/her private key

The CA decripts the ciphertent and checkes that the decrypted plaintent match with the public key.



The state of the s
(i) Vser sands his lhow public key to CA, CA encrypts some
data with it and gives it back to user
data with it and gives it back to user > User then decrypts the cipherdate and gives decrypted data by by to CA
data back to CA
Both data original data and decrypted data should match for passing the test
match for passing the test
-> After Verification, The CA signs the certificate in following
Add basic details like owner, his publickey, issuer, expiry date etc
(i) Encrypt it vans (A's private less
(i) Encrypt it using (A's private key (ii) append (A's digital certificate to the cipher text
Now the Aigital certificate is Signed with CA's knowtheatic
has public key.
direct A metallity of and made willing in the
the and olded probabilities has much all about
deat metassand to Tond"
and the same of th
and will have all the second to the second t
much but also in the red alles and a second
att and all has both at the contract And the
and all the desired the second



- Os) How can we verify a digital certificate?
 - The war wants to veily a digital certificate,
 - (i) pass all fields except last one (Digital signature of Certification Authority) to a message digest algorithm

 We have to use the same message digest algorithm

 the CA used, which can be easily found out via

 Internet Et mix (CA itself documents this)
 - (ii) The message-digest algorithm calculates the hash, Let this hash be MDa
 - (ii) Now we extract digital signature of CA from the last parameter and using it find the public key of CA
 - (v) We now decrypt the remaining field of contificate using public key of CA
 - 1 let the digusts inside the decorpted message be MD2
 - a if MD, = MD2 , then we can confirm that the digital contificate is issued by the CA.