THADOMAL SHAHANI TSEC ENGINEERING COLLEGE
Om Shete
TE C92
2103163

Assignment No : 2

Q.1 Write short note on digital signatures and digital certificates.

⇒

- **Digital Signatures**

⇒ A digital signature is a hash value that has been encrypted with the sender's private key.

- The act of signing means encrypting the the message's hash value with a private key
- So the sender computes and encrypts the hash value with her private key.
- At the receiving end, you decrypt the hash value with sender's public key. Now, because no one knows the private key of the sender, altering the hash value and resigning with the private key of the sender is not possible.

Processing applied on message	Security Property achieved
Encryption	Confidentiality
Hashing	Integrity
Digitally signing	Integrity, authentication, non-repudiation.
Encryption and digitally signing	confidentiality, integrity, authentication, non-repudiation

- **Applications:**

1) Sending and receiving secure emails.
2) Signing documents.

163

THADOMAL SHAHANI TSEC ENGINEERING COLLEGE

- Properties of digital signature :-

1) Integrity
   ⇒ Via hash value calculation
2) Authentication
   ⇒ Via the ability to prove sender's identity by decrypting hash with the sender's known public key
3) Non-repudiation
   ⇒ Sender cannot deny sending the message because she used her private key to encrypt the hash.

- Digital certificate
  ⇒ Digital certificates is issued by a trusted third party which proves senders identity to the receiver and receiver's identity to the sender.
- A digital certificate is a certificate issued by a Certificate Authority (CA) to verify the identity of the certificate holder.
- Digital certificates is used to attach the public key with a particular individual or an identity.

THADOMAL SHAHANI
TSEC
ENGINEERING COLLEGE

- Digital Certificate Contains :-

1) Name of certificate holder
2) Serial number which used to uniquely identify a certificate
3) Expiration dates
4) Copy of certificate holder's public key.
5) Digital signature of certificate issuing authority.

163