THADOMAL SHAHANI TSEC ENGINEERING COLLEGE

ASSIGNMENT NO. 2

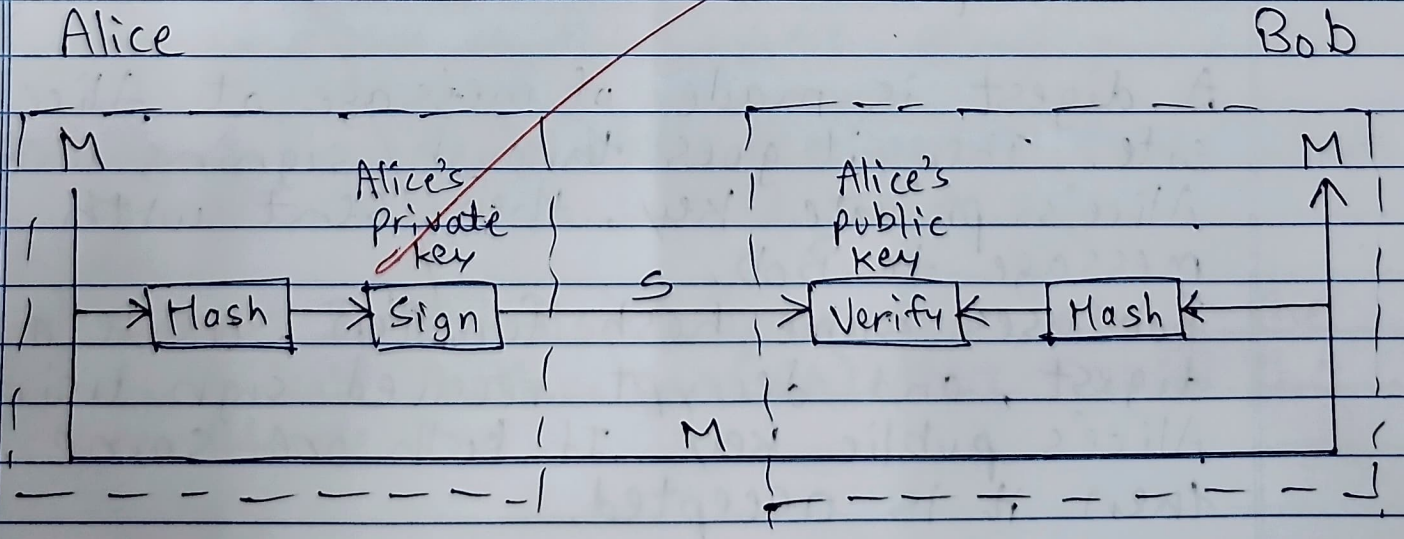
Q. Write short notes on Digital Signature and Digital certificate

→ 1> Digital Signature :-

It is a mathematical technique used to validate the authenticity and the integrity of a message sent.

Process :

The sender uses a signing algorithm to sign the message. The message and the signature are sent to the receiver. The receiver receives message and signature and applies verifying algorithm to combination. If the result is true, the message is accepted ; otherwise, it is rejected.



Need for keys:

The signer uses its private key to sign the documents, no one else has this key. The public key of the sender is used to verify the sign. Anyone can use it to verify the signature of the sender.

Signing the Digest:

Asymmetric key cryptosystems are very inefficient when dealing with long messages. Solution is to sign the digest of message, which is much shorter than the message.

A digital signature can directly provide:
- message authentication
- message integrity
- nonrepudiation

A digest is made of message at Alice's site. Then it goes through signing with Alice's private key, then sent with message to Bob.
Bob uses same hash function, create a digest, and decrypt received sign using Alice's public key. If both are same, then it is accepted.

2> Digital Certificate :-

A digital certificate, also known as a public key certificate, or an identity certificate, is an electronic document associates a public key with an entity (such as an individual, organization, or website). Digital certificates are issued by Certificate Authorities (CAs) and are used in public key cryptography to verify the identity of parties involved in the online communications and transactions.

Components of Digital Certificate:

1> Public Key: The most crucial component of a digital certificate, used for encryption and digital signatures.

2> Identity Information: This includes details about entity or individual to whom certificate is issued, such as their name, country.

3> Valid Period: Specifies the period during which certificate is considered valid.

4> Issuer Information: Information about the Certificate Authority (CA) that issued the certificate.

5) Digital Signature : A cryptographic sign created by the CA to bind the public key to the identity information.