Module 4

Authentication Protocols & Digital signature schemes

Authentication Schemes

- One-way authentication: In one-way authentication, only one entity verifies the identity of the other entity.

Client → verify → Server

- Mutual or Two way: In mutual authentication, both communicating entities verify each other's identity.

Client → verify → Server

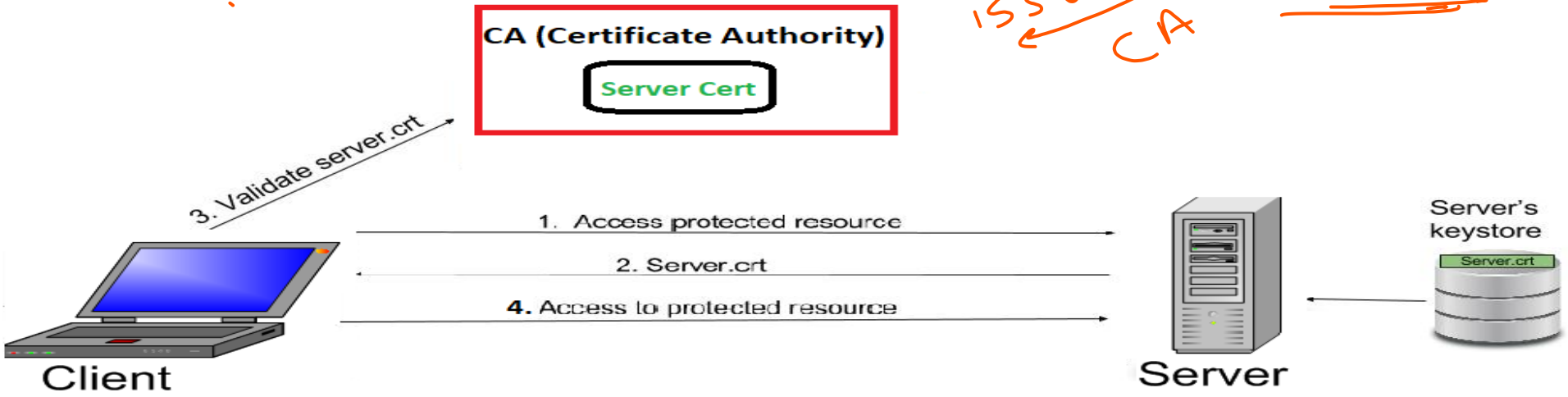
← verify ←

One way Authentication Scheme-Example

- In one way SSL, only client validates the server to ensure that it receives data from the intended server.
- For implementing one-way SSL, server shares its public certificate with the clients.

issued by CA

X.509



One way Authentication Scheme-Example

SSL

1. Client requests for some protected data from the server on HTTPS protocol. This initiates SSL handshake process.

2. Server returns its public certificate to the client along with server hello message.

Server $\xrightarrow[\text{Hello Msg}]{\text{Certificate}}$ Client

3. Client verifies the received certificate through certification authority (CA) for CA signed certificates.

Client $\xrightarrow{\text{verify}}$ Certificate $\xrightarrow{\text{Using}}$ CA

One way Authentication Scheme-Example

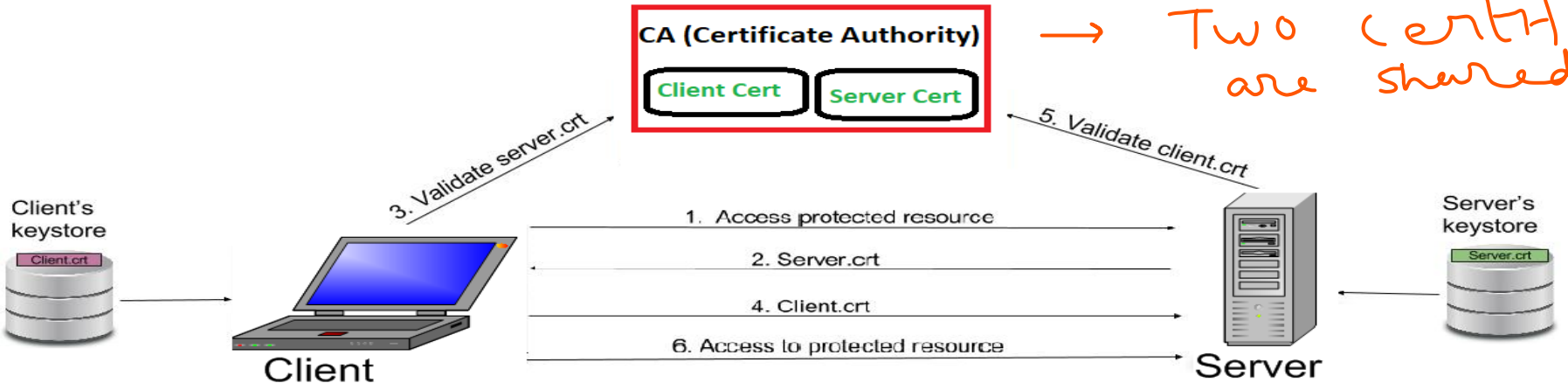
Steps of Handshake Protocol of SSL

4. SSL client sends the random byte string that enables both the client and the server to compute the secret key to be used for encrypting subsequent message data.
   - The random byte string itself is encrypted with the server's public key.

5. After agreeing on this secret key, client and server communicate further for actual data transfer by encryping/decrypting data using this key.

Two way Authentication Scheme-Example

- In two-way SSL, both client and server authenticate each other to ensure that both parties involved in the communication are trusted.
- Both parties share their public certificates to each other and then verification/validation is performed based on that.



→ Two certificates are shared

Two way Authentication Scheme-Example

1. Client requests a protected resource over HTTPS protocol and the SSL handshake process begins.

2. Server returns its public certificate to the client along with server hello.

3. Client verifies the received certificate through certification authority (CA) for CA signed certificates.

Two way Authentication Scheme-Example

4. If Server certificate was validated successfully, client will provide its public certificate to the server.

Client provides its public certificate only if server certif. is valid

5. Server verifies the received certificate through certification authority (CA) for CA signed certificates.

6. After completion of handshake process, client and server communicate and transfer data with each other encrypted with the secret keys shared between the two during handshake.

Signature

It is a proof to the recipient that the doc comes from the correct entity.

Example – Banks → Sign Cheque

Cheque → Account No., Date, Pay to, Amount
(Document)

Signature → Manual Signature is done on the document
↓
matched with the original one stored in a file/db

Digital signature

- A signature on a document, when verified, is a sign of authentication which means the document is authentic
- An electronic signature can prove the authenticity of the sender of the message
- This type of signature is known as Digital Signature

Conventional Vs Digital signature

	Conventional	Digital
Inclusion	It is included in the document	The signature is a separate document Message + Signature is sent to the reciever
Verification Method	Signature on the document is compared with the signature on the file	Signature is not stored anywhere so to verify it, the recipient needs to apply a verification technique to the combination of message and signature

Conventional Vs Digital signature

Alice — Bob
msg
+sign
interc
Eve

	Conventional	Digital
Relationship	One to many 1 sign can be used for multiple documents	One-to-One For every msg the sign is different
Duplicity	A copy of the signed document can be distinguished from the original one in a file	There is no such distinction Attack: Interception, Replay Interception of msg & sign and then replaying it after sometime

Process

- The sender uses a **signing algorithm** to sign the message
- The message and the signature is sent to the receiver
- The receiver receives the message and the signature and applies the **verifying algorithm** to the combination
- If the result is true, then the message is accepted else it is rejected

msg + Sign

Signing Algorithm

Process

- Need for keys

Conventional sign → It is like a Private key broz it belongs to user

If anybody wants to verify then they can use the sign that is stored in a file.

Stored sign → Public key → Used for verification

- Signing the Digest

I/P → Msg (Arbitrary length)
↓
Hash Function
↓
O/P → Msg Digest (Fixed length)

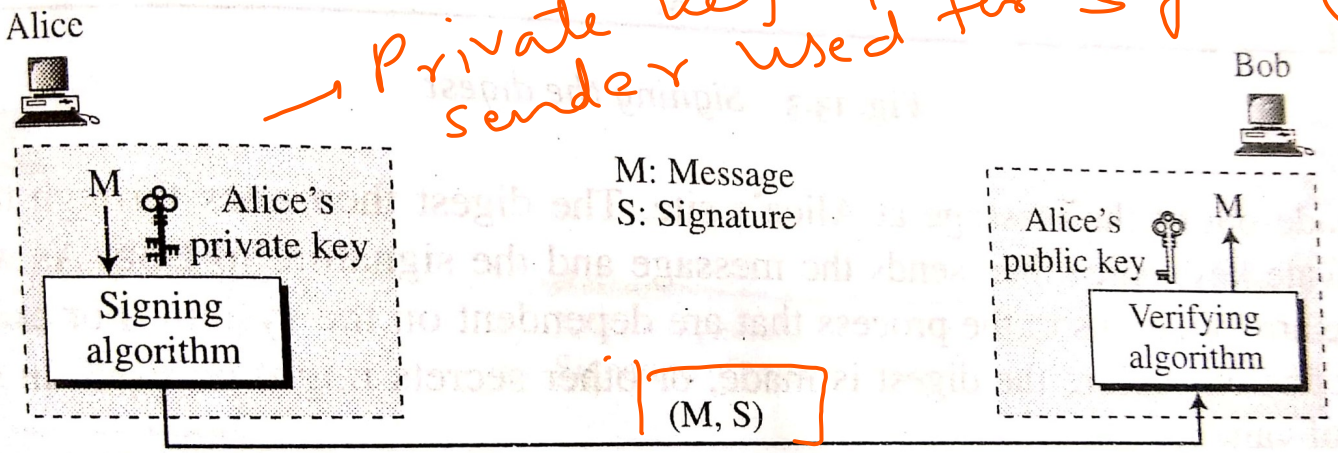
Sender → Private key

Recipient → Public key

Need for keys

- The sender uses its private key to sign the document
- The receiver uses the public key of the sender to verify the document

Private key of sender used for signing



Public key of sender is used for verification

Fig. 13.2 *Adding key to the digital signature process*

Signing the digest

- Asymmetric key encryption are inefficient when dealing with long messages
- In digital signature system, the messages are generally very long
- So, the solution is to sign a digest of the message which is much shorter than the message

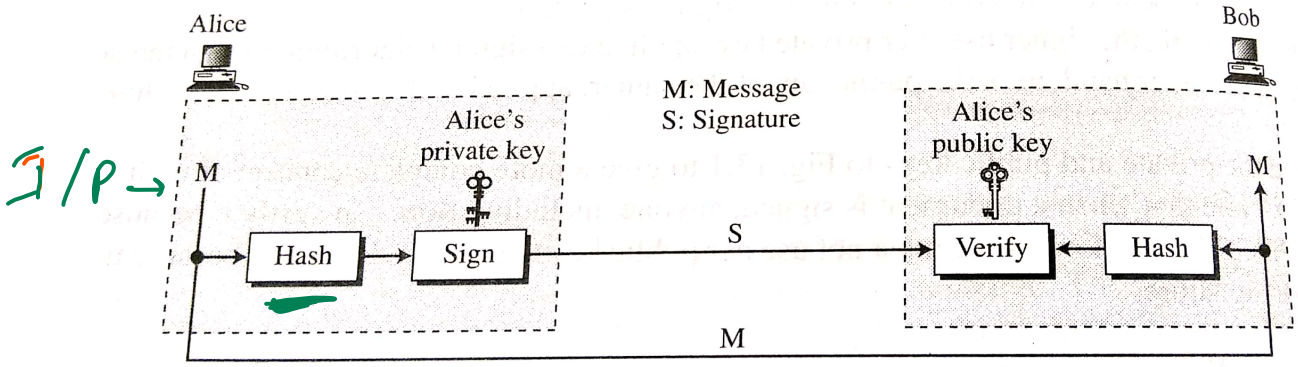


Fig. 13.3 *Signing the digest*

Sender's Public Key is used for verification

Signing the digest

- At the sender's side, the message digest is created
- The digest then goes through the signing process using the sender's private key
- The message and the signature is sent
- At receiver's side, the digest is created for the received message using the same hash function
- Calculations are done on the signature and the digest
- The verification process applies criteria on the result of the calculation to determine authenticity of the signature
- If authentic, the message is accepted, else it is rejected

Services of digital signature

- Message Authentication
- Message Integrity
- Nonrepudiation
- Confidentiality