Semester: VI Subject: CSS Academic Year: 2023 - 2024

SSL → SECURE SOCKET LAYER:

It is an internet protocol for secure exchange of information between Web Browser and Web Server.

The services provided by SSL are as follows:

→ Authentication
→ Confidentiality

It uses 3 protocols:

→ Handshake Protocol
→ Record Protocol
→ Alert Protocol

Handshake Protocol:

It undergoes 4 steps:

* Establish security capabilities.
* Server authentication and Key Exchange.
* Client authentication and Key Exchange.
* Finish.

Step 1: Establish security capabilities:

Client Hello:

The client Hello consists the following:-

→ Version Number.
→ Random Number of Client (RNc) → It is generated based on date and timestamp.

Semester: VI Subject: CSS Academic Year: 2023-2024

→ Session id → if id = 0 then connection not yet established.
if id = non-zero then connection is established.

→ Cipher suite : It consists of all cryptographic algorithms supported by the client.

→ Compression method : The compression algorithm that client supports.

The client will send all the above information to server.

Server Hello :

The server hello consists of the following :

→ Version Number → The server will choose the version.

→ Server generated Random Number (RN_s).

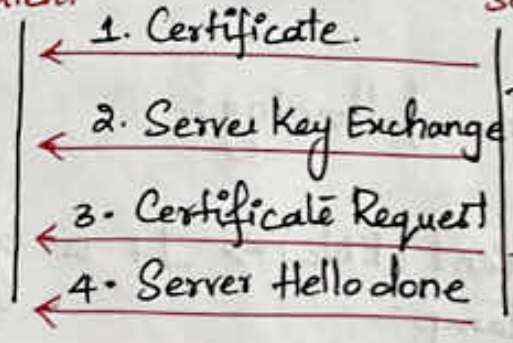
→ Server session id.

→ Cipher suite → Choose single cipher suite which the server selects from the list send earlier by the client.

→ Compression Algorithm → Server selects from the list that is sent by the client.

The above informations are send to client.

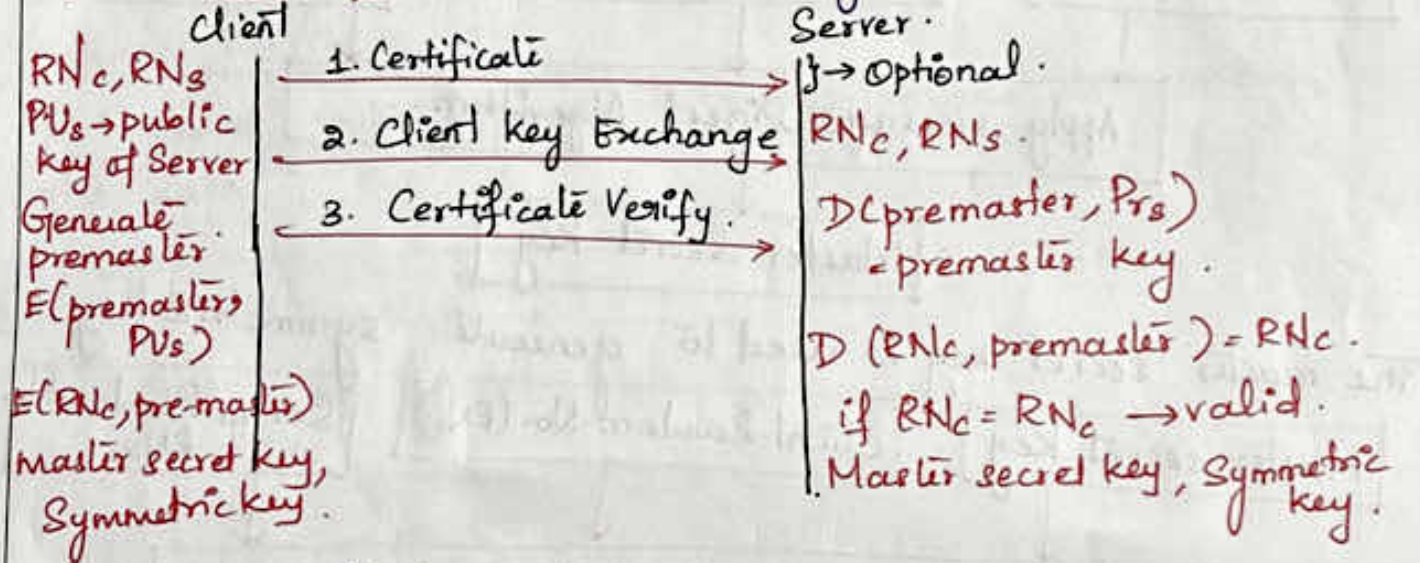
Step 2 :- Server Authentication and Key Exchange.



Semester: VI Subject: CSS Academic Year: 2023-2024

1. Server sends Digital Certificate which contains public key of server.
2. If server does not send certificate then only the public key is send by the server.
3. The server can request for client digital certificate.
4. Client can now verify and proceed.

Step 3: Client Authentication and Key Exchange.



(2) Client Key Exchange:

→ Client creates pre-master key.

→ Premaster-key is encrypted by public key of server and encrypted pre-master key is send to Server.

→ Server will decrypt using his own private key.

(3) Certificate Verification:

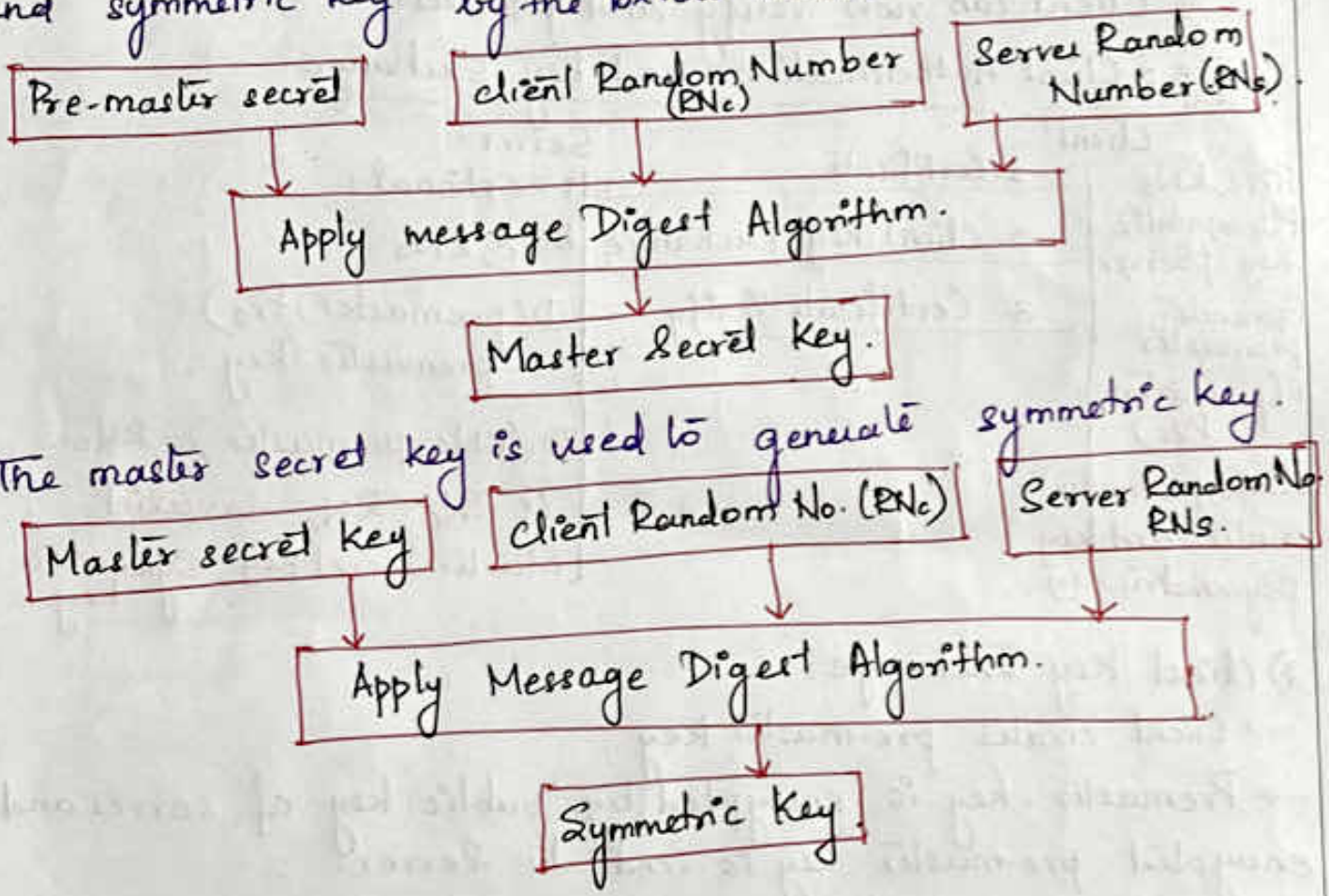
→ Encrypt random number of client using pre-master key and send to server.

Semester : VI Subject : CSS Academic Year: 2023-2024

→ The server will decrypt it using pre-master key and get the random number of client

→ If RN_c is equal to the random Number which he has already received, then it is right client.

Both client and server will generate master secret key and symmetric key by the below method:



The master secret key is used to generate symmetric key.

Semester: VI Subject: CSS Academic Year: 2023-2024

Step 4: Finish.

RNc, RNs, PVs, premaster key, Master secret key, Symmetric key.

Client

1. Change cipher specification →
2. Finished →
3. ← Change Cipher specification
4. ← Finished.

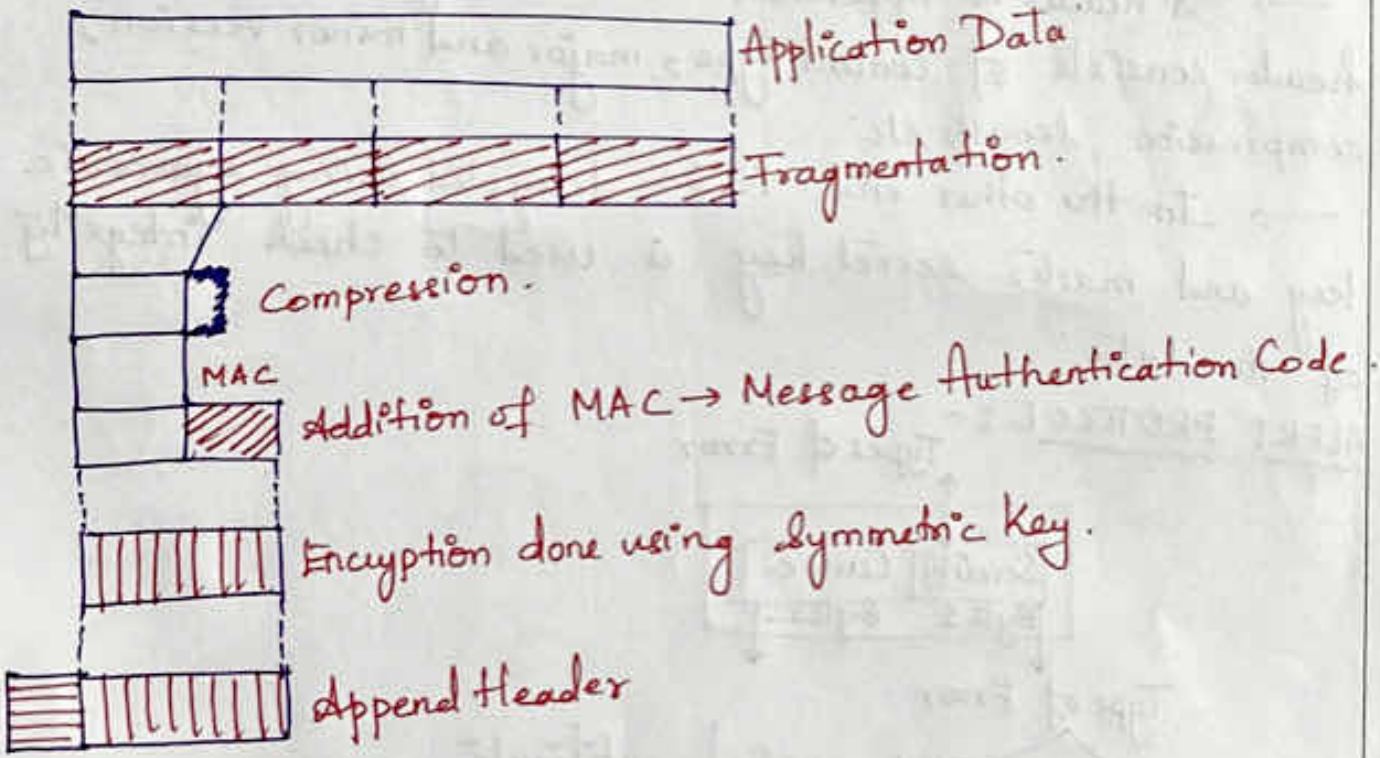
Server.

RNc, RNs. premaster, master secret key, Symmetric key.

After generating all required keys, the final confirmation message is send to both client and server.

RECORD PROTOCOL:

The record protocol does not encryption and decryption of the data.



Semester : VI Subject : CSS Academic Year: 2023-2024

The following steps are followed in record protocol.

→ The Application data is divided into fragments using fragmentation technique.

→ Apply compression algorithm on fragmented data to compress the data.

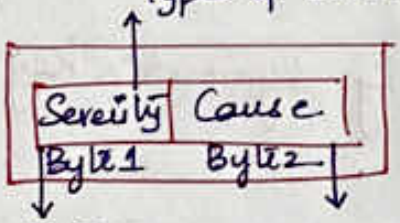
→ MAC is generated through the compressed data. The master secret key is used to generate MAC. The MAC is appended to check the integrity of message.

→ The data along with the MAC is encrypted using the generated symmetric key.

→ A header is appended to the encrypted data. The header consists of content type, major and minor version, compression length etc.

→ In the other end it is decrypted using symmetric key and master secret key is used to check integrity of the data.

ALERT PROTOCOL :-



Type of Error

Warning
Bad record MAC.
Decompression failure
Handshake failure.

Fatal →
- No certificate
- Bad certificate
- Certificate expired.

Semester : VI Subject : CSS Academic Year: 2023-2024

→ When either the client or the server detects an error the detecting party sends an alert message to the other party.

→ If it is fatal error then communication is closed.

→ If it is warning, then error is resolved and it is continued.