Unit-4

* Web security:-

Requirements:

It provides the security to the data which is transmitted through the network.

Client-Server Connection

→ Client sends a request to the server and accepts the request and provides the services.

→ There are three protocols one of the protocol is SSL (Secure Socket Layer)

→ In SSL it includes differents protocols

1. SSL record protocol
2. Hand Shake protocol
3. Change cipher Specification protocol.
4. Alert protocol.

This four are said to be as SSL protocol Stock.

*** SSL (Secure Socket Layer):

Security over network and data which is transferred between web browser and server.

Connection and session:

The connection should be established between client and server and it is a transport to provide the service

Session:

It is an association between client and server

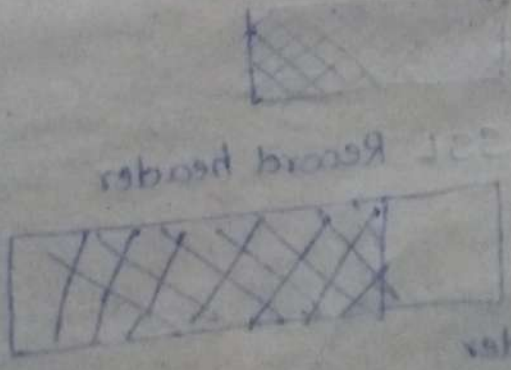
which is created by Handshake protocol.

* SSL parameters:

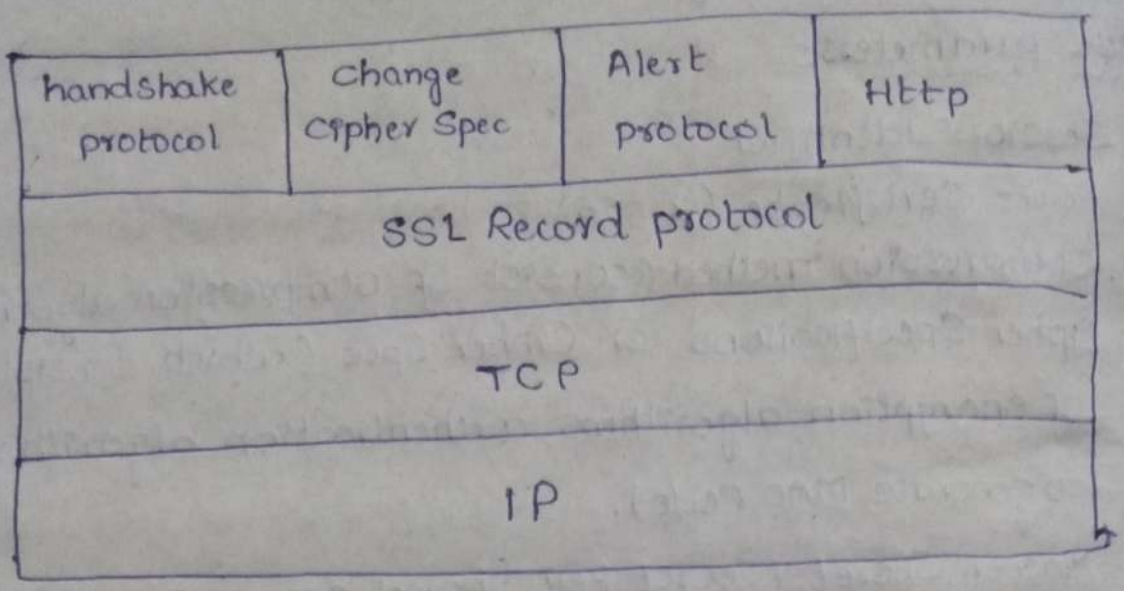
1. Session Identifier
2. Pear's Certificate (X.509)
3. Compression method (consist of compression algorithms)
4. Cipher Specifications or Cipher Spec (which consists of encryption algorithms, authentication algorithms to generate MAC Code).
5. Master Secret (Secret key shared among client and Server).
6. IS Resemble (It consits with a flag).

* Connection state parameters

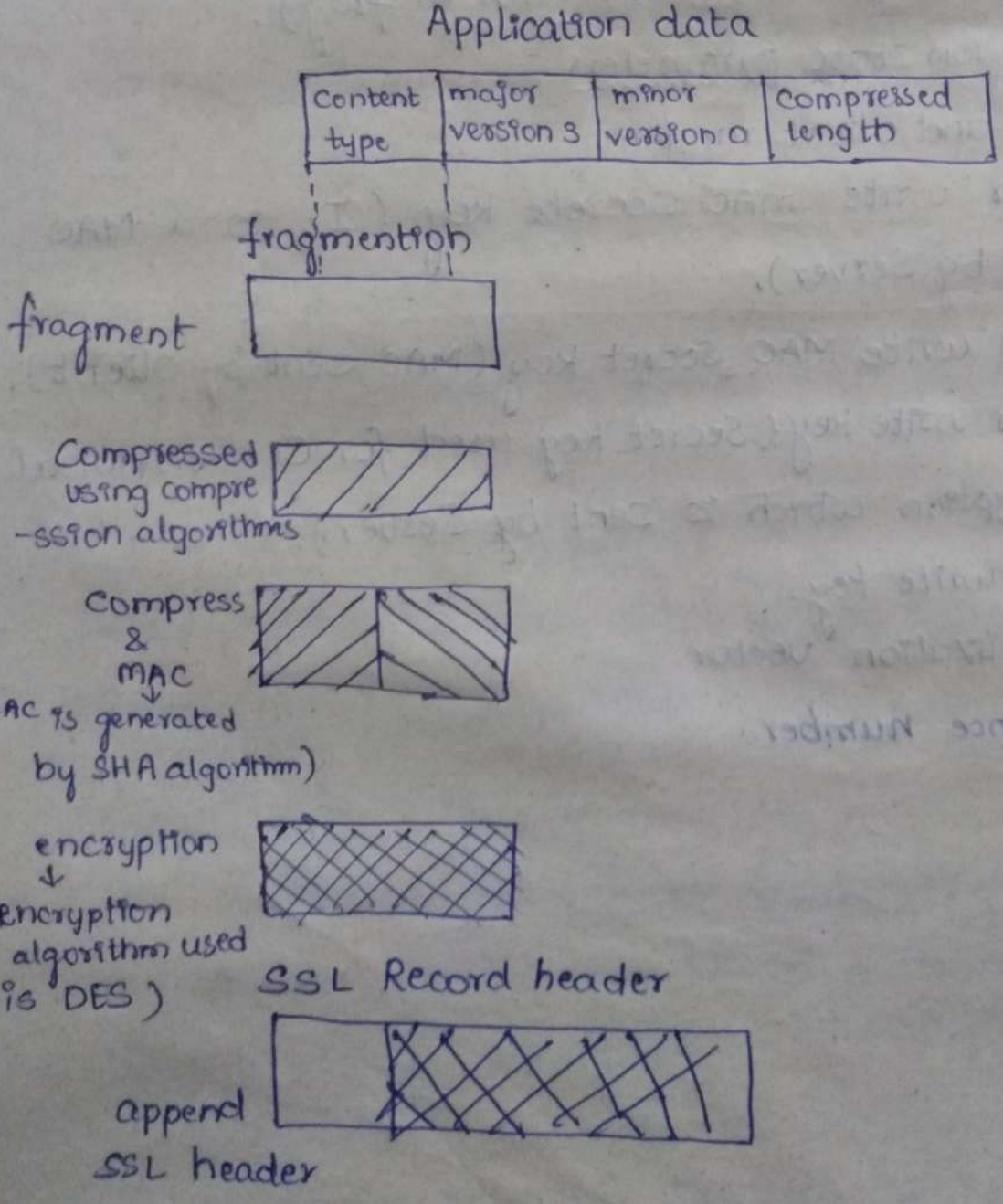
1. Server and client random
2. Server write MAC Secrete key (It is a MAC Sent by Server).
3. Client write MAC Secret key (MAC sent by Client).
4. Server write key (Secret key used for Conventional Encryption which is sent by Server).
5. Client write key.
6. Initialization vector
7. Sequence number.



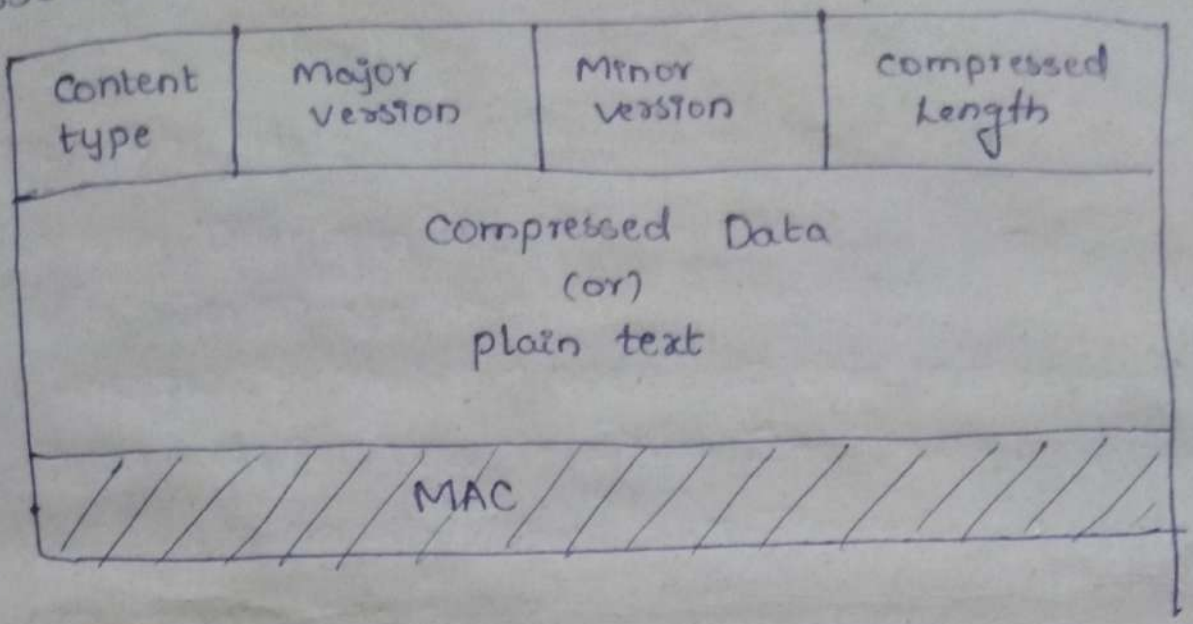
SSL protocol



* SSL Record protocol



SSL Record protocol.

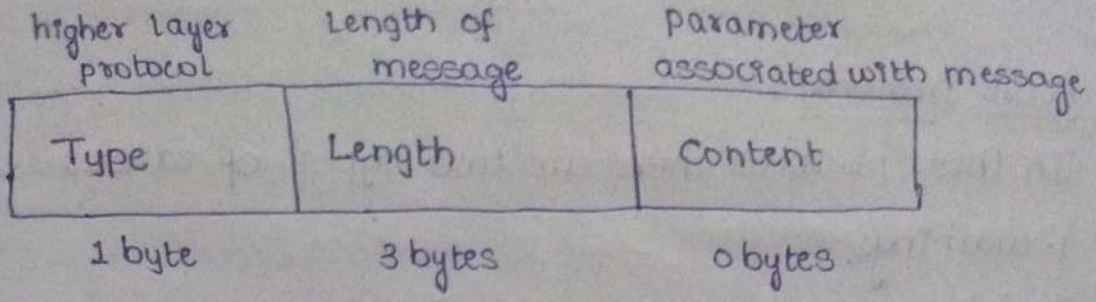


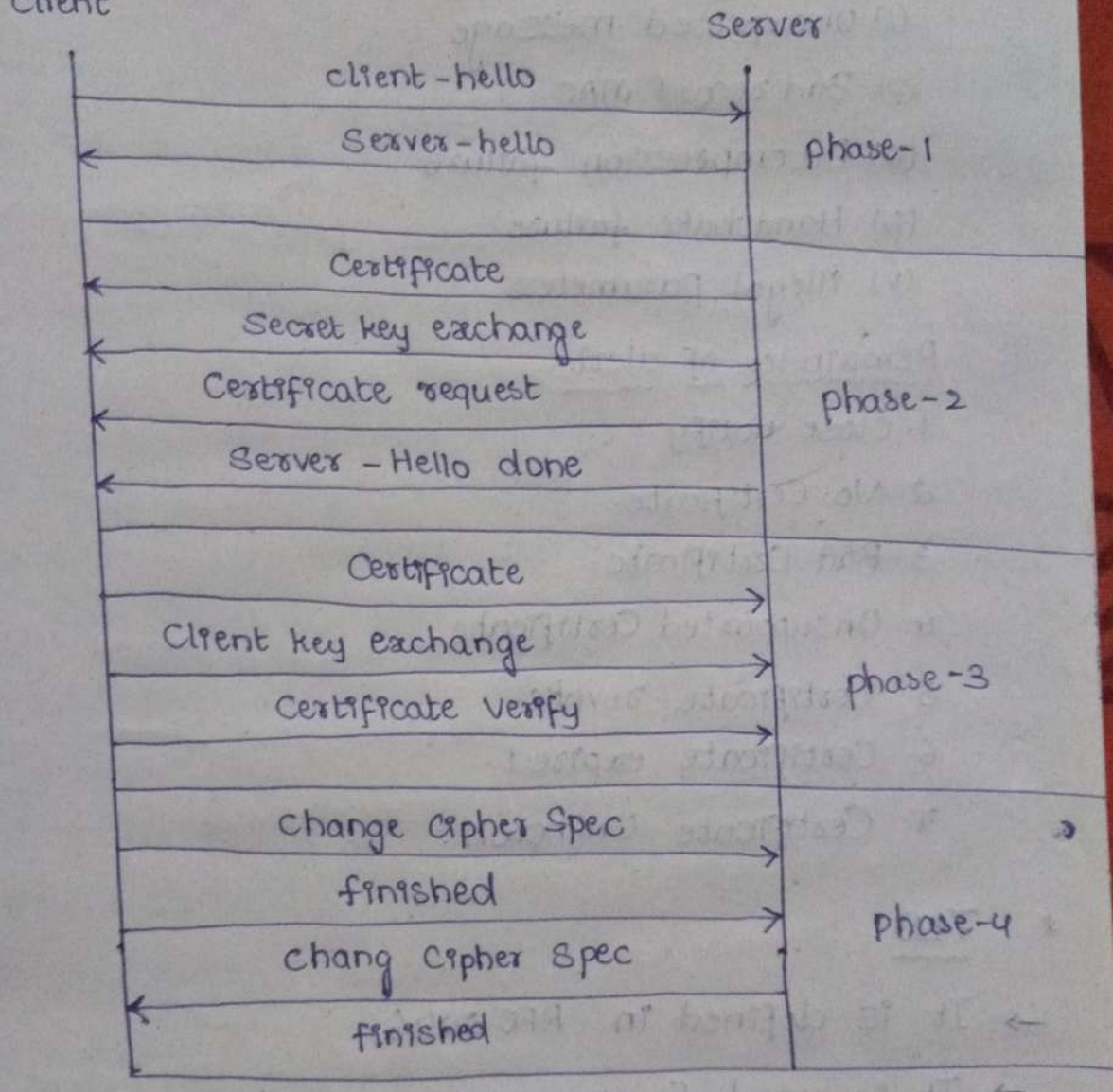
Calculation of MAC:

Hash (MAC - Write - Secret || pad 2 ||
hash (MAC - write - Secret || pad 1 ||
Seq - num || SSL Compressed Length || SSL
Compressed type || SSL compressed fragment)

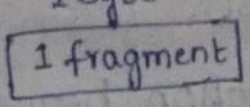
pad-1 - 00110110
pad-2 - 00110110

Handshake Protocol:





Change Cipher Spec protocol:



pending state to current state

* Alert protocol:

In this protocol there are two types of errors

1. warnings.
2. fatal errors.
   - (i) Unexpected message
   - (ii) Bad record MAC
   - (iii) Decompression failure
   - (iv) Handshake failure.
   - (v) Illegal parameters

Remainder of alerts.

1. Close notify
2. No Certificate.
3. Bad Certificate.
4. Unsupported Certificate.
5. Certificate revoke.
6. Certificate expired.
7. Certificate Unknown.

* TLS

→ It is defined in RFC 2246.

→ It is used for providing security in Transport layer.

→ It is derived from SSL.

→ Provide a secure connection between client and server.

→ TLS is used by http, SMTP.

* working:

→ User's client-server handshake mechanism.

→ There is a key exchange between client and server. (key exchange is done by diffie hellman key exchange algorithm).

→ TLS protocol will be opened on encryption channel (encryption is done by DES and RC4 algorithms).

→ It also ensures that messages are not altered.

→ RFC2246 is similar to SSL Version 3.

* SET (Secure Electronic Transaction):

It is a security provided on credit card which contains with an personal information and financial information.

Services:

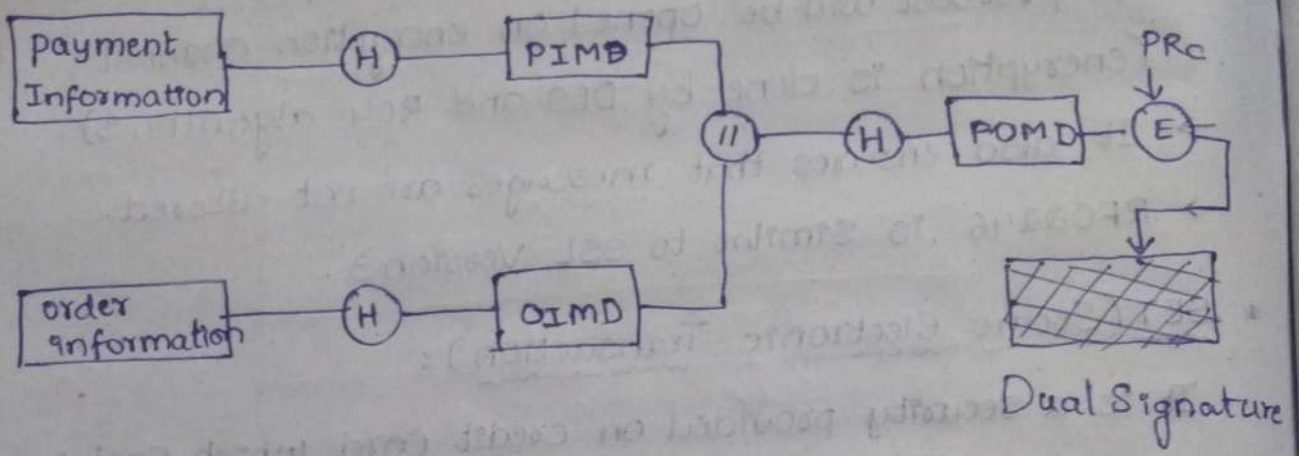
1. Confidentiality
2. Integrity
3. Card holder authentication
4. Merchant authentication.

Set participants:

1. Card holder.
2. merchant who sell the product.
3. issuer (bank of card holder)
4. acquirer (financial institute established or related to merchant accept payment from any bank).
5. Payment gateway (Master Card or VISA Card).
6. Certificate authority (It is a trusted third party give certificate to card holder).

Dual Signature: It is verified by merchant and bank.

If a data is encrypted by sender's private key payment information should be given to bank and order information send to merchant.



Dual Signature

PIMD - payment information message digest

OIMD - Ordered information message digest

POMD - payment order message digest

E - Encryption using SHA

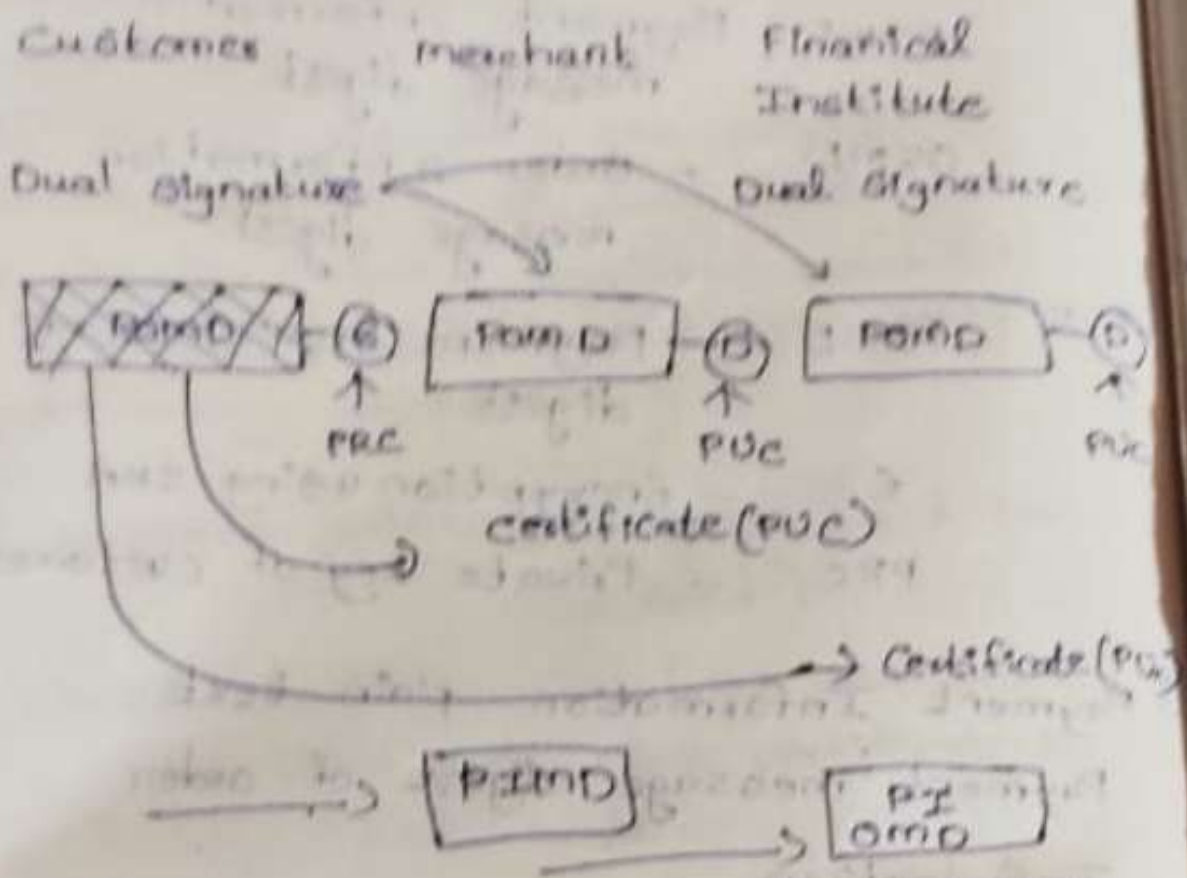
PRC - private key of Customer

→ Payment information plain text of payment message digest of Ordered information.

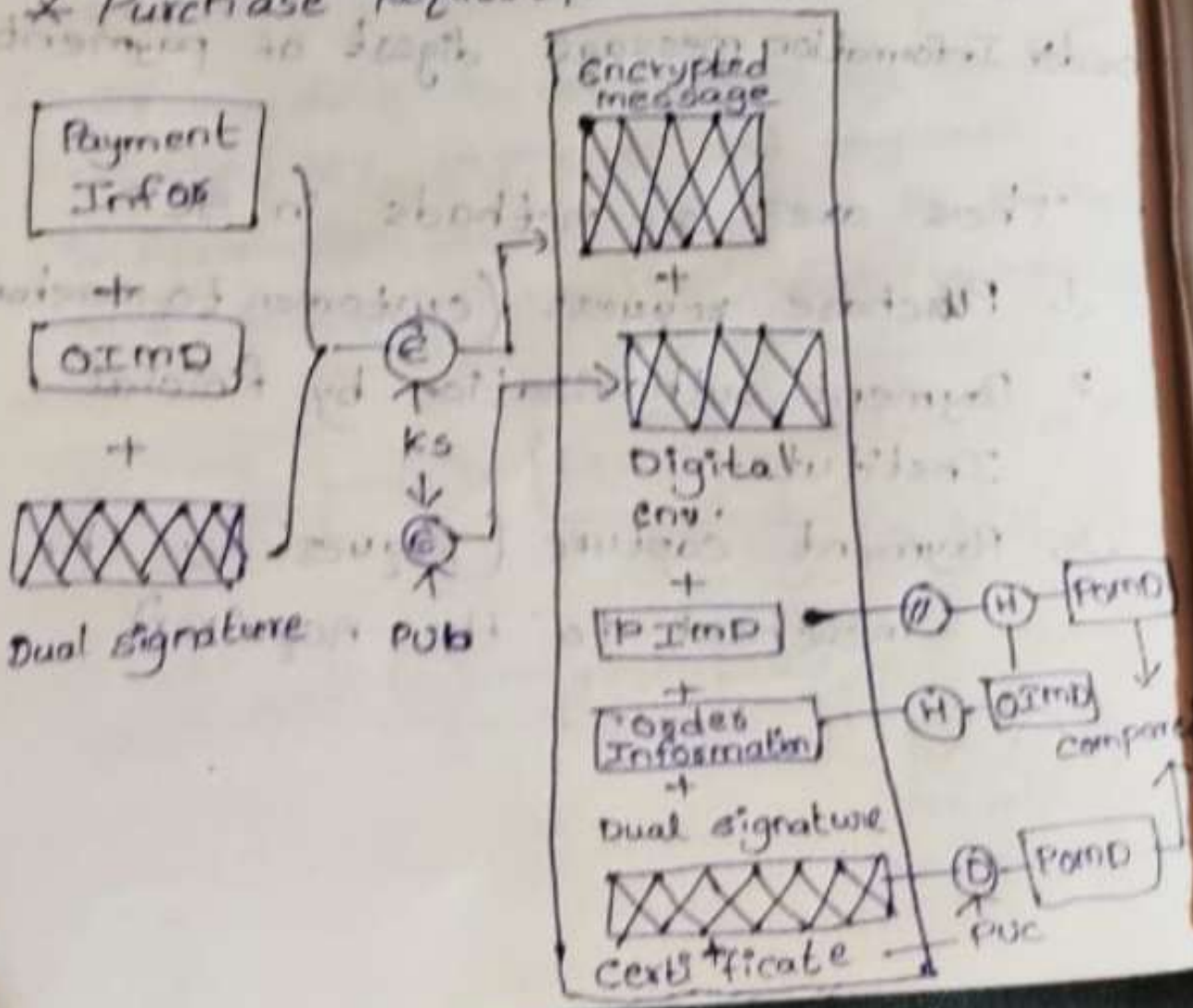
→ Order information, of plain text of order info msg digest of payment.

→ There are three methods in SET:

1. purchase request (customer to merchant).
2. Payment authorization by financial institute.
3. Payment Capture (Request by the merchant to the acquirer)



* Purchase Request:



PUb - Public key of bank
H - Hash
D - Decrypt

* Payment Authorization:-