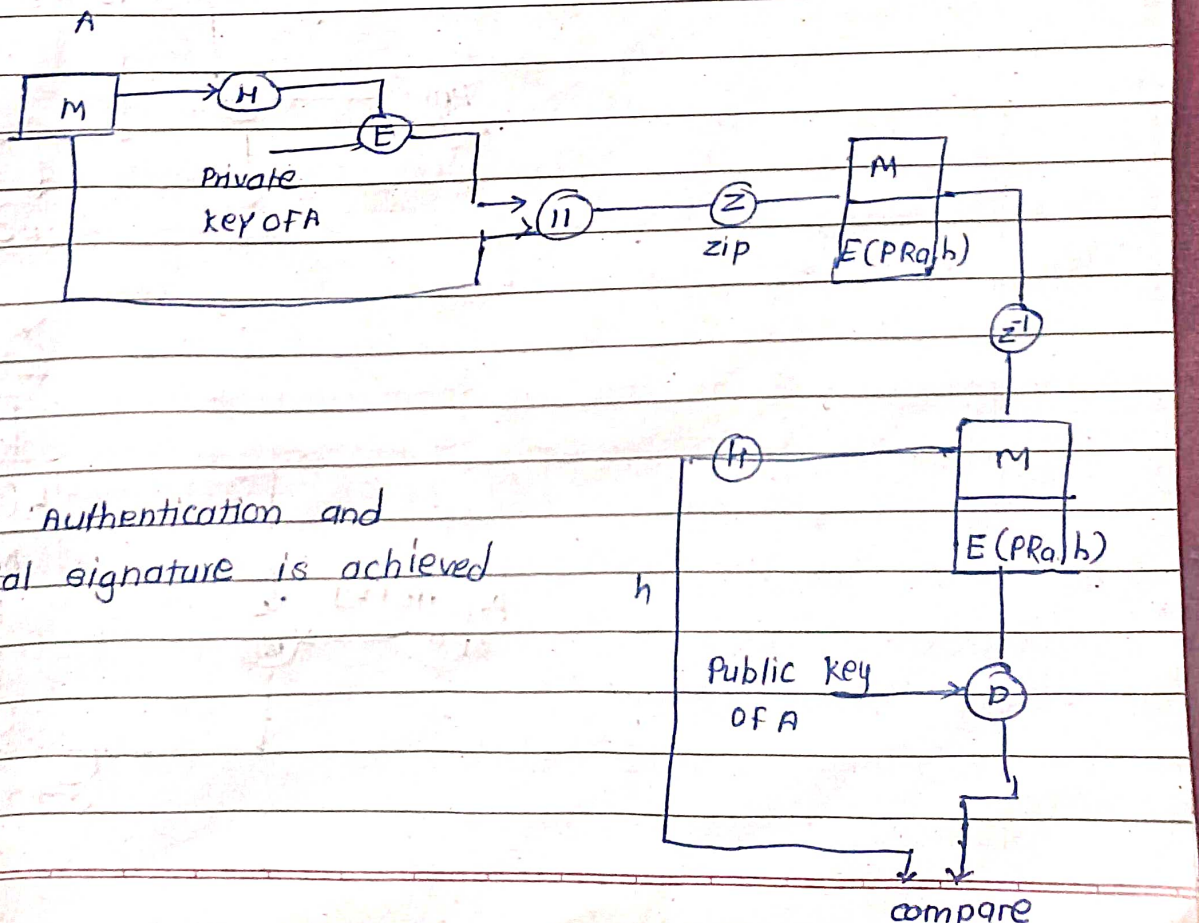
* Module 5 *

PAGE No.
DATE

① Email security.
- email is most widely used and regarded network services
- But lack of inbuilt mechanism for ensuring integrity, confidentiality and authencity of messages
- email messages are usually plaintext so it is easy to read during transmission

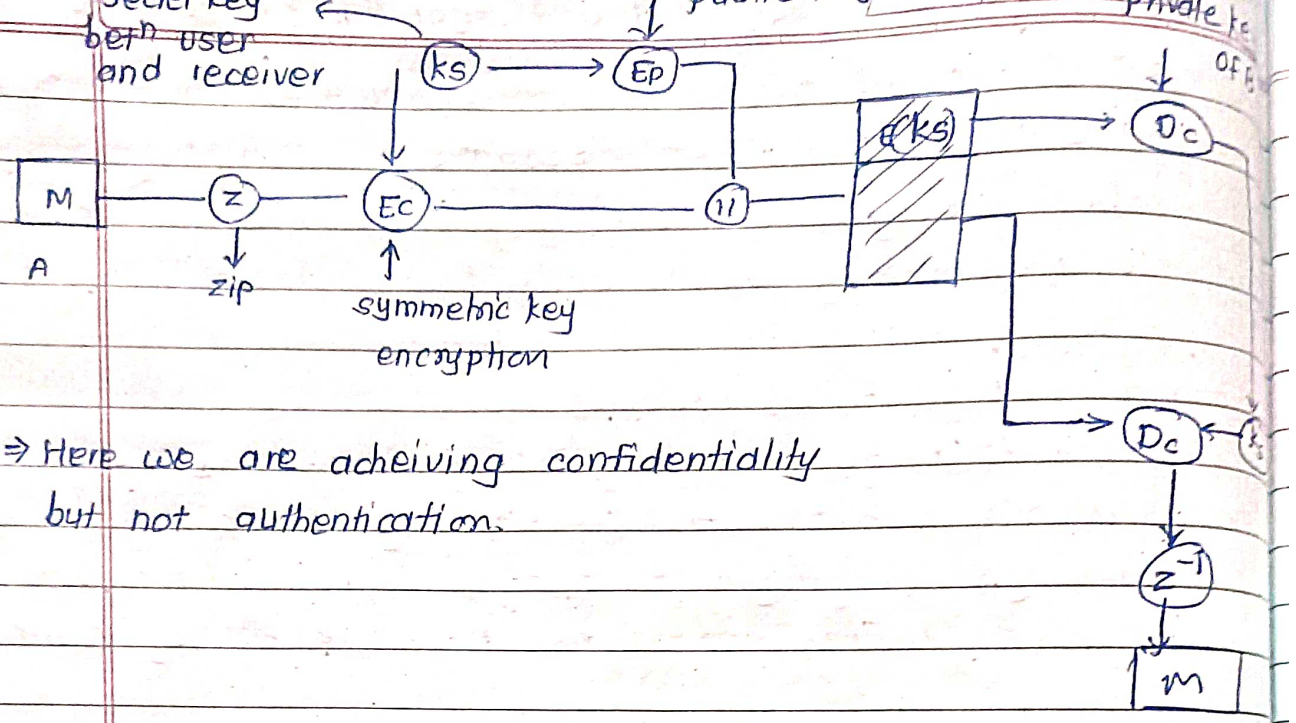
• enhancement in email security
① confidentiality: protection from disclosure
② Authentication: verify the identity of sender of msg
③ message integrity: protection from modification
④ Non-repudiation: protection from denial by sender

① PGP: Pretty good privacy
- confidentiality, authentication and digital signature service are provided
- Additional services like email compatibility and email compression is provided



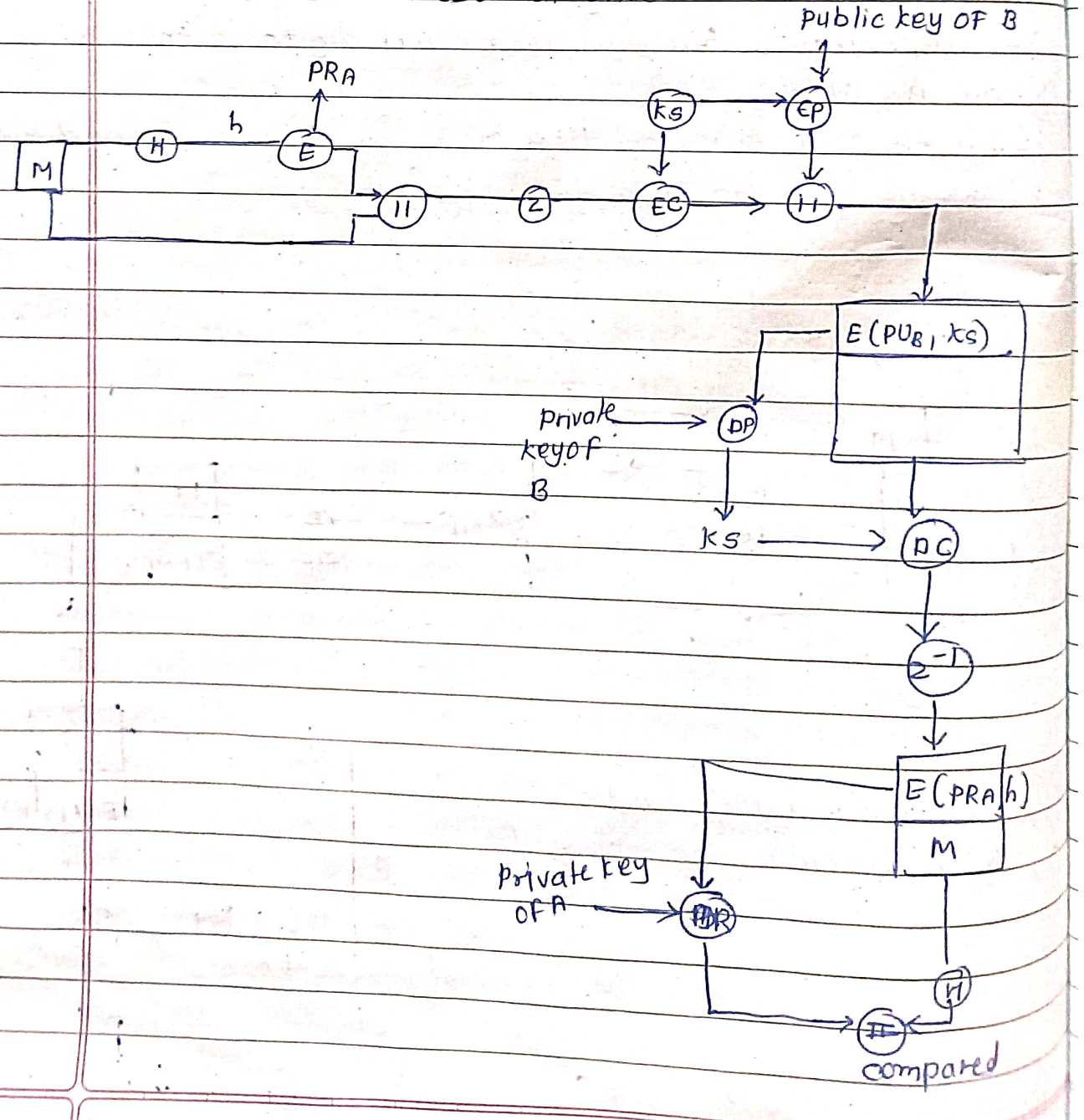
∴ Here Authentication and digital signature is achieved

In previous diagram, message is in the plain text so we don't get confidentiality... Here we using symmetric key between user and receiver



⇒ Here we are acheiving confidentiality but not authentication.

To achieve all three services at once



* Pretty Good privacy
- widely used de-facto secure email
- developed by phil Zimmermann
- multi-platform support
- Provides confidentiality, authentication, integrity and non-repudiation for email
- widely adopted.

PAGE No.
DATE / /

* PGP operations:

① Authentication:- It ensure that message is from verified user

① sender create the message
② Generate message hash:
- It uses SHA-1 to compute 160-bit hash value of msg
③ sender encrypt the hash value using private RSA key. this is digital signature
④ Then message & digital signature sent to receipent
⑤ Decrypt the hash using public RSA key (sender) and recover hash value and then apply hash function on msg
⑥ If both hash match:
- The message is authentic

② confidentiality:- only authorized people can access people.

1. The sender can create plaintext message. The 128 bit random no. is generated as session key for sym. encryption
2. Then encrypt the message using session key and symmetric encryption algorithm such as IDEA, 3DES
3. session key is encrypted using recipient public RSA key. This ensure that only the recipient private RSA key can decrypt the session key
4. Attach encrypted message and encrypted session key.
5. Then again decrypt the session key and then decrypt the encrypted msg with the help of session key.
6.

(b) Confidentiality and Authentication:

- PGP can provide both confidentiality and authentication simultaneously by combining the processes of digital signatures and encryption

- steps:

① plaintext message → hash function → encryption using private key → digital signature → combine digital signature and message → encrypt it using symmetric key encryption [128 bit session key used]

↳ Also encrypt the session key using public key of receiver

→ Transmit encrypted message, encrypted session key

→ Recipent uses private key of receiver to decrypt session key

→ Then use session key to decrypt message

→ Then decrypt the signature.

Then recipent calculates the hash of decrypted message

→ If the two hash matches, sender and message is authentic

(c) PGP compression

- compression is done before the encryption process and after signing the message.

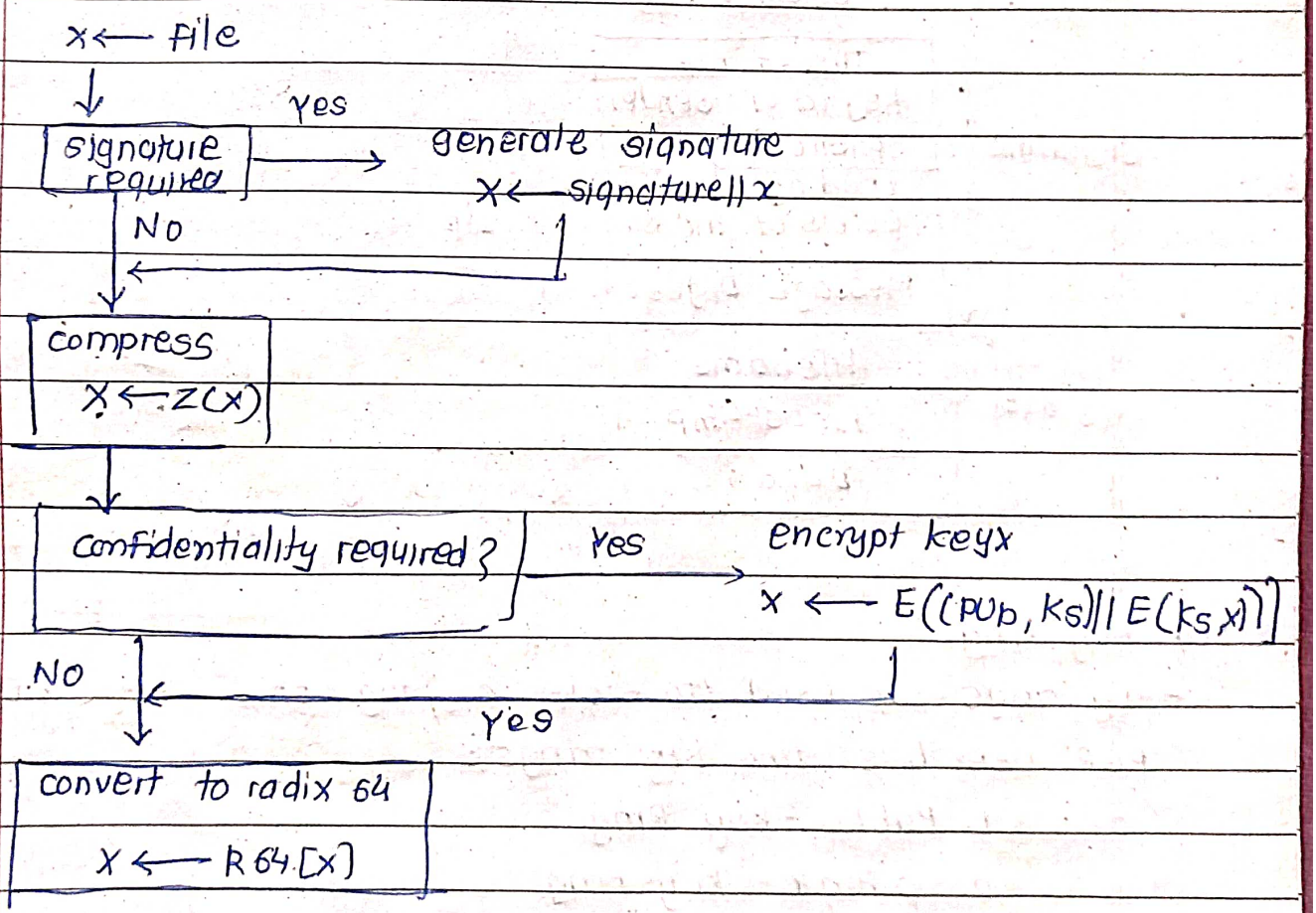
- this will significantly reduce the size for message fo

- use zip algorithm for compression.

PAGE No.
DATE / /

⑤ PGP- compatibility:
- while using pgp we deal with binary data to send but email was only designed for text.
- so PGP must encode raw binary data into printable ASCII characters.
- It uses radix-64 algorithm, maps 3 bytes to 4 printable chars.
- PGP also segment the data if it is too big.

Generic transmissions Diagram

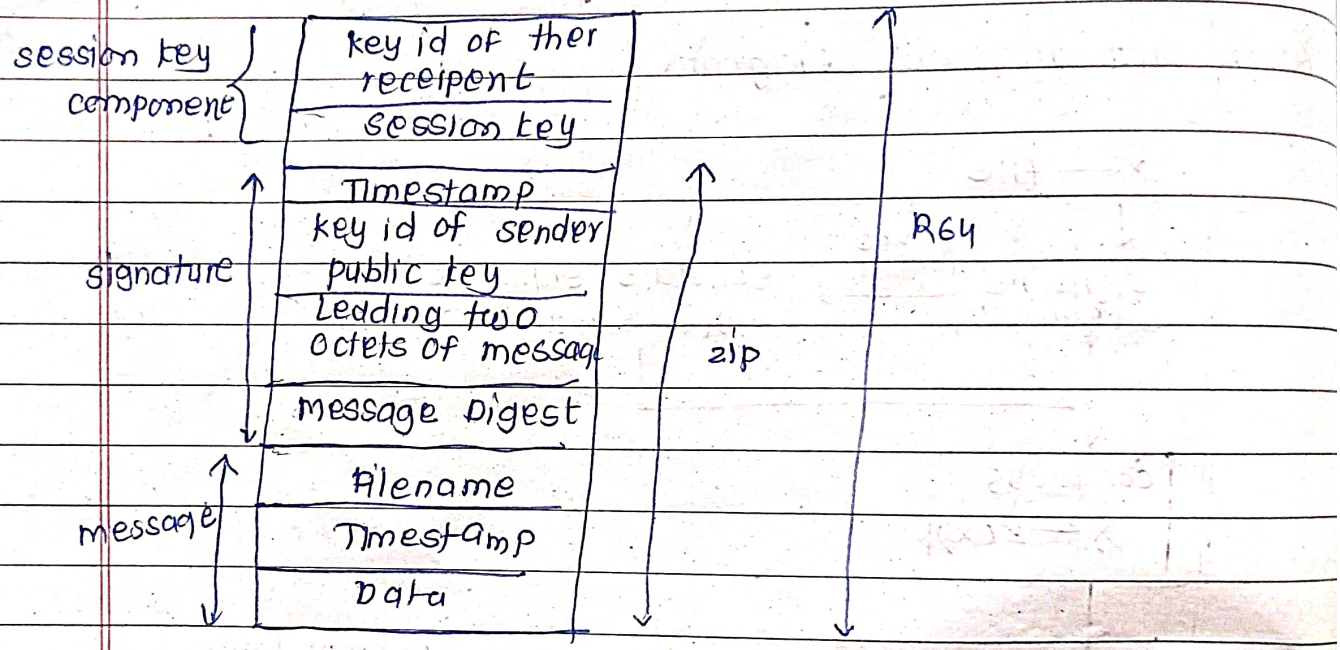


* PGP- session keys:
- PGP require a unique session key for each encrypted msg to maintain confidentiality and security.
- The session key is temporary, randomly generated key used to encrypt the message using symmetric key encryption algorithm.
- The session key itself get encrypted using recipient public key (asymmetric encryption).

* PGP public and private keys:
- PGP employs asymmetric cryptography where public key is used for encryption and private key for decryption

- PGP uses key identifier rather than transmitting full public key. It takes least significant 64 bits of the key
- Also use key id in signatures

* PGP message format:



* PGP key rings:
- key rings are used to store cryptographic keys. Every PGP user has two key rings:
    1. Public-key Ring
    2. private-key ring
- The public-ring used to stores the public keys of other PGP users that are known to the user. each public key is indexed by its key ID
- The private-ring stores the private key for the user which are needed for decrypting messages and signing message. It is also indexed by key-id

* PGP message Generation and PGP message Reception

* Secure/multipurpose internet mail Extensions?
- extension of MIME (multipurpose internet mail extensions)
- originally developed to extend RFC822 (MIME)

PAGE No.
DATE / /

- MIME provide support for varying content types and multi-part messages
- S/MIME added security enhancement like providing end-to-end encryption
- S/MIME uses asymmetric encryption.
- have S/MIME support in many mail agent such as MS outlook, Mozilla, Mac mail

• S/MIME functions:
① enveloped data: encrypted content & associated keys
② signed data: encoded message + signed digest
③ clear-signed data: cleartext message + encoded signed digest
④ signed and enveloped data:
- nesting of signed & encrypted entities.

• cryptographic Algorithms:

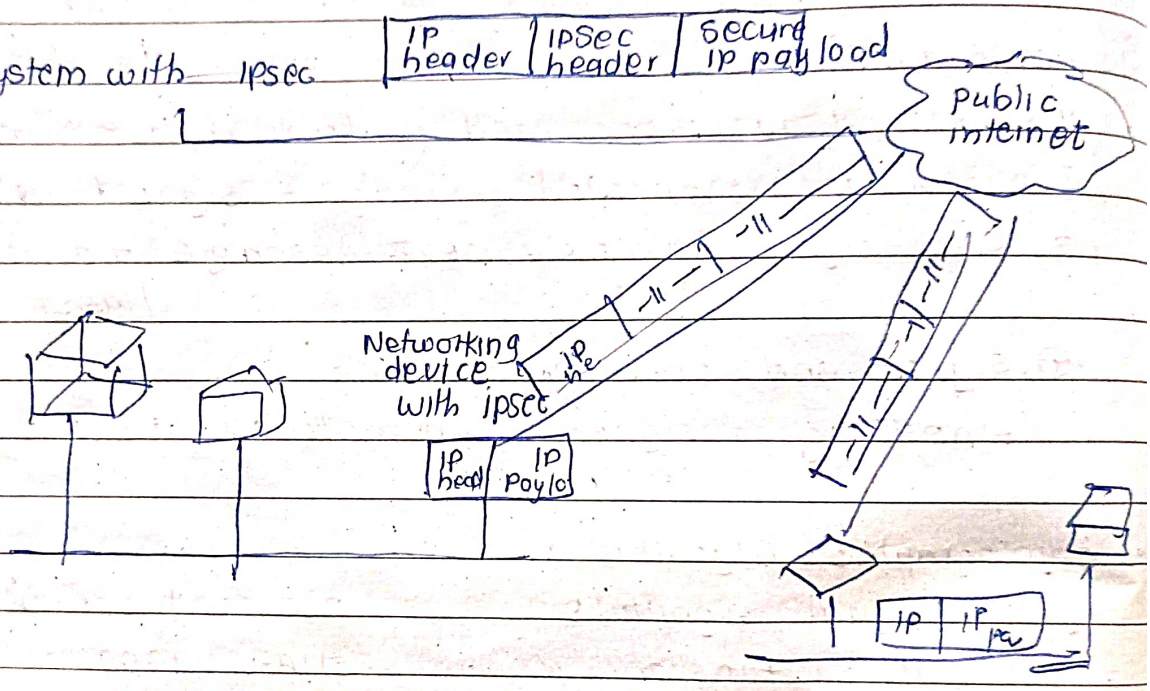
Digital signature	DSS (with SHA-1), RSA
Hash function	SHA-1, MD5
session key encryption	RSA
message encryption	AES
MAC	HMAC

- S/MIME secures MIME entity with a signature, encryption or both.
- have range of content type:
① enveloped data ② signed-data ③ clear-signed data
④ registration request ⑤ certification only message

- S/MIME uses X.509 V3 certificates
- each client has list of trusted CA's certs

- IPSec is comprehensive framework used to secure internet Protocol communications by implementing at network layer

- It has various applications such as almzme, PGP, Kerberos SSL/HTTPS
- It is general ip security mechanism
- Provides authentication, confidentiality and key management
- Applicable to use over LAN, across public and private WANS



Benefits of IPSec:
- In a router provides strong security to all traffic crossing the perimiter
- In a router is resistant to bypass
- below transport layer hence transpaient to applications
- can be transpaient to end users
- can provide security provide to end user.
- Secure routing architecture

* IPsec architecture: having two header extension
  ① Authentication header.
  - Provide authentication and data integrity for the entire ip packet. (include header and payload)
  - It ensure that packet has not been altered during transmission.

- defined in numerous RFC's
  - including RFC 2401/2402/2406/2408
- mandatory in IPV6 not in IPV4

PAGE No. :
DATE / /

•] ipsec services:
1. Access control
2. connectionless integrity
3. Data origin authentication
4. confidentiality
5. limited traffic flow confidentiality

•] security associations:
- It present one-way relationship between sender and receiver that provide security services for traffic flow between them
- Security associations are unidirectional, for bidirectional flow, two SA needed
- It is defined by its 3 parameters:
  1. security parameter index (SPI)
  2. Ip destination address
  3. security protocol identifier
- There exist additional no of parameters like seq. no, AH and EH
- have a database to store security associations

•] Authentication header:
- AH tells that ip packet has not been altered during transit
- AH authenticate the source of the packet to ensure it truly came from the claimed sender.
- AH implement sequence no. to countermeasure to protect against replay attack
- parties must share secret key
- based on use of MAC

Next header	Payload Length	Reserved
security parameter index		
sequence NO		
Authentication data		

PAGE No.
DATE / /

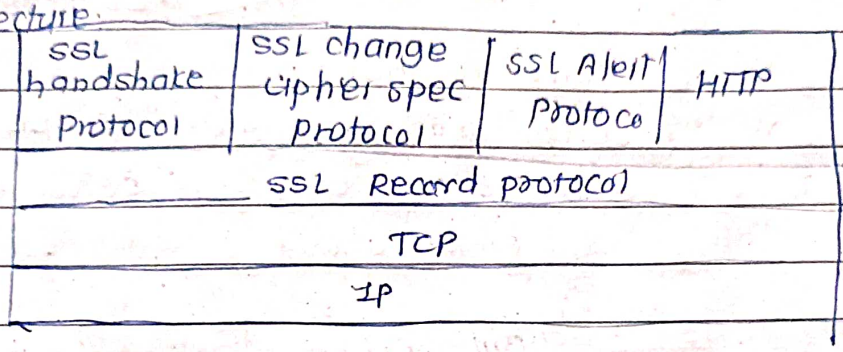
* Modes of operation:
  - Transport Mode:
    - In the transport mode, only the payload of ip packet is encrypted or authenticated and ip header is left intact
    - In case of AH, only the payload is protected by MAC
    - In case of ESP, the payload is encrypted and authenticated.
    - The original ip header not encrypted so it can visible to intermediate routers
    - Typically used for end-to-end communication between host
  - Tunnel Mode.
    - In this model, entire ip packet is encrypted and encapsulated inside new ip packet. This creates an outer ip header and inner ip packet
    - Tunnel mode is typically used for site-to-site VPN's. Commonly used in VPN tunnels
    - Due to full encryptions making it ideal for securing traffic over untrusted networks.
    - Hide internal details from the intermediate routers and all

combining security Associations:
- SA can implement either AH or ESP
- To implement both need to combine SA's
  - form security association bundle
  - may terminate at different or same endpoint
- issue of authentication and encryption order

* Web - security:
- web know widely used by bussiness, goverment, individuals
- web have variety of threats:
  ① integrity ③ denial of service
  ② confedential ④ authentication

PAGE No.
DATE / /

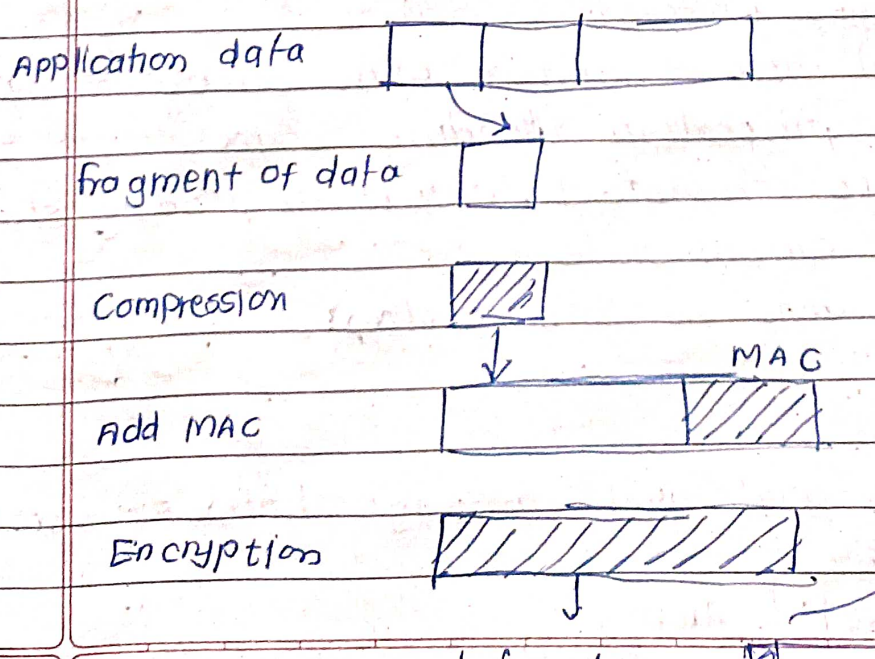
* Secure socket layer
- Tidnsport layer security service
- used to provide web security for the data transferred between browsers
- originally developed by Netscape
- uses TCP to provide end-to-end service
- Architecture:



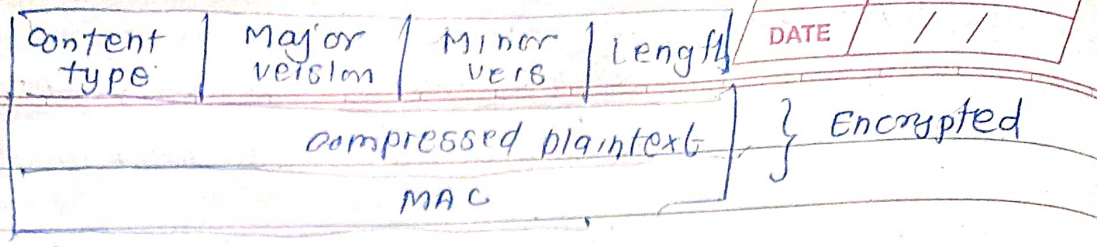
SSL connection:
- A transient peer-to-Peer communication link associated with 1 SSL session.

2-SSL session:
- An association between client and server.
- created by handshake protocol
- define d set of cryptographic parameters

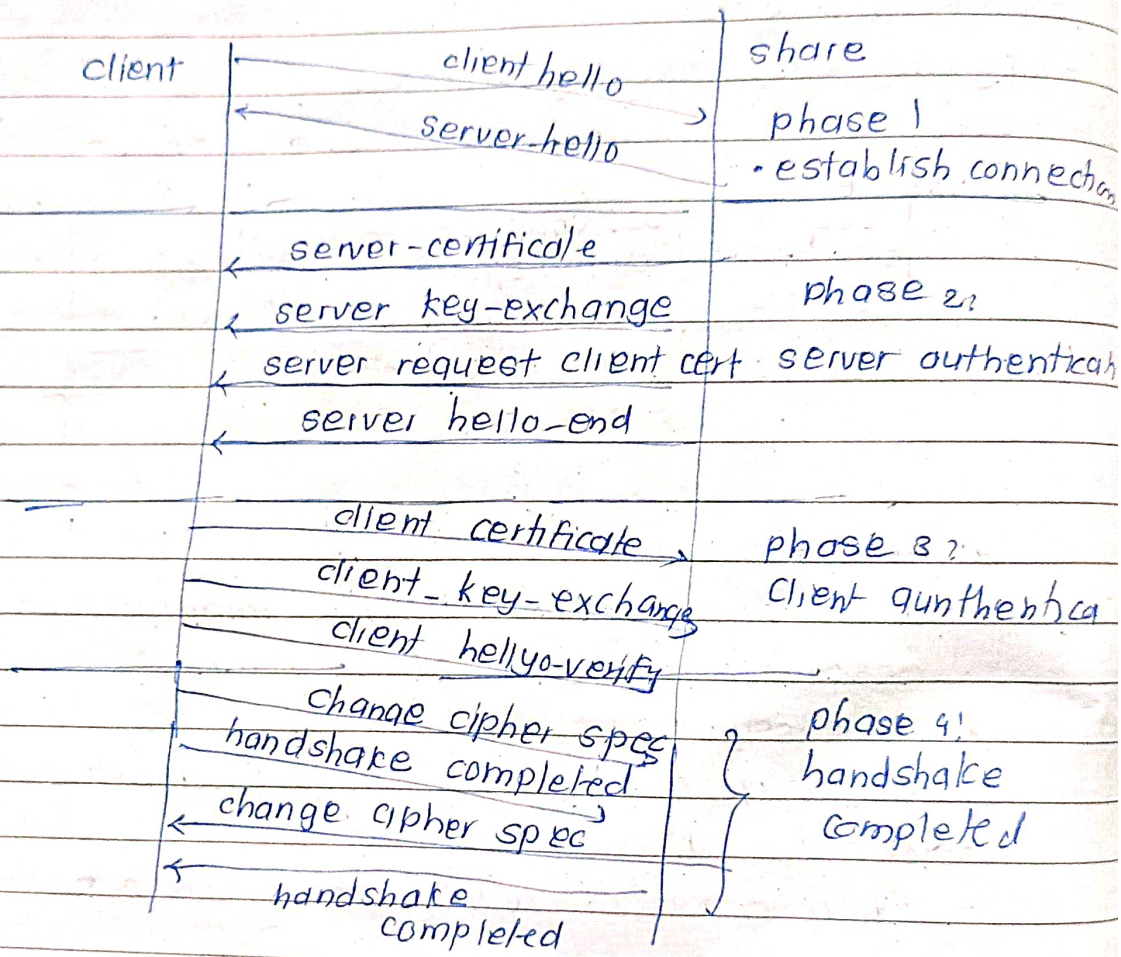
① SSL Record protocol:



- SSL header consist of



② Handshake protocol:
- used to establish a session between client and server



③ chang cipher spec protocol.
- SSL record protocol output until completion of handshake protocol in Pending state
- As handshake completed, output in pending state copied into current state.
- This all is done by this protocol

④ Alert protocol:
- It is use to send alert message between users
- It has 2 field

we have two levels:

① warning: connection is resumed

② fatal: connection get terminated.

There are several alerts (level: warning)

① No certificate
② certificate expired
③ unknown certificate
④ certificate Revoked
⑤ close Notify
⑥ unsupported certificate

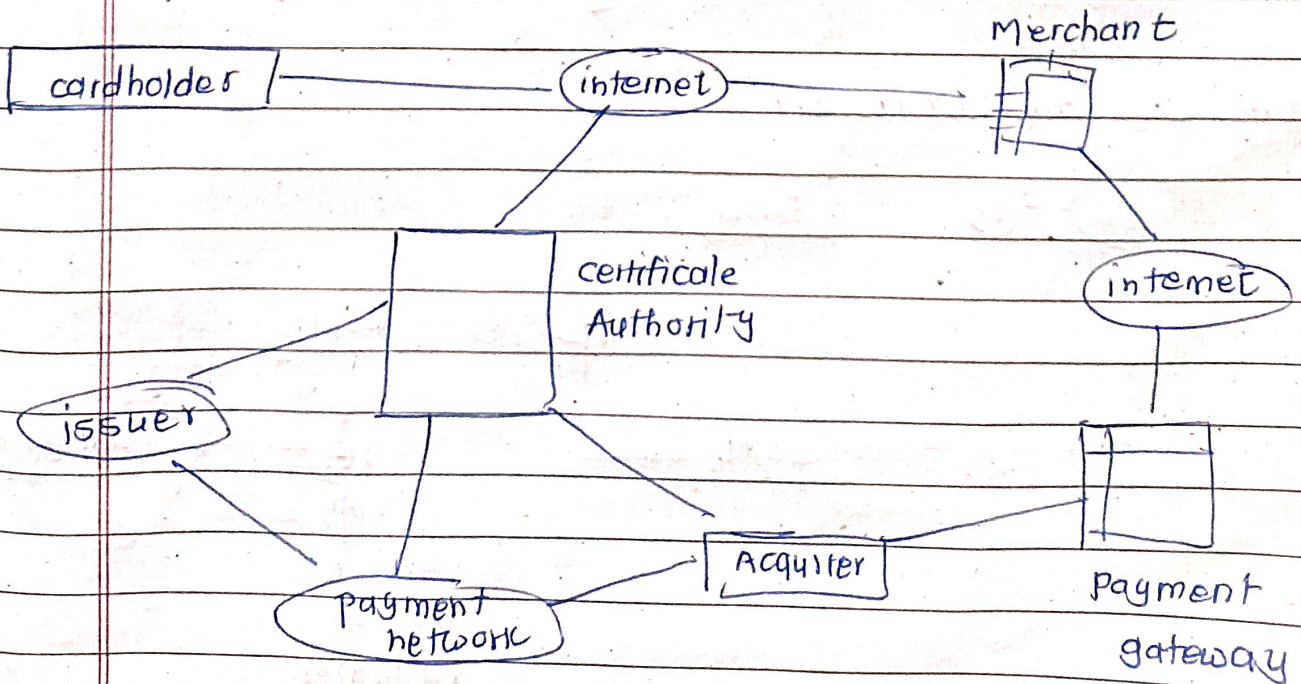
fatal issue

① Handshake failure
② Decompression failure
③ unexpected message
④ illegal parameters
⑤ Bard record MAC

* Transport security layer: (TLS)
  - uses HMAC for MAC
  - has additional alert codes
  - some changes in certificate types and negotiations
  - changes in crypto computation and padding

* Secure Electronic transactions:
  - It is used to secure credit card transactions
  - developed by mastercard, visa and other companies
  - open encryption and security specification
  - not a payment system

SET components:



set transactions:

1. customer opens account
2. customer receives certificate
3. merchants have their own certificates
4. customer places an order
5. merchant verified
6. order and payment are sent
7. merchant request payment authorization
8. merchant confirms order.
9. merchant provide goods or service
10. merchant request payment

Dual signature:

customer create dual messages

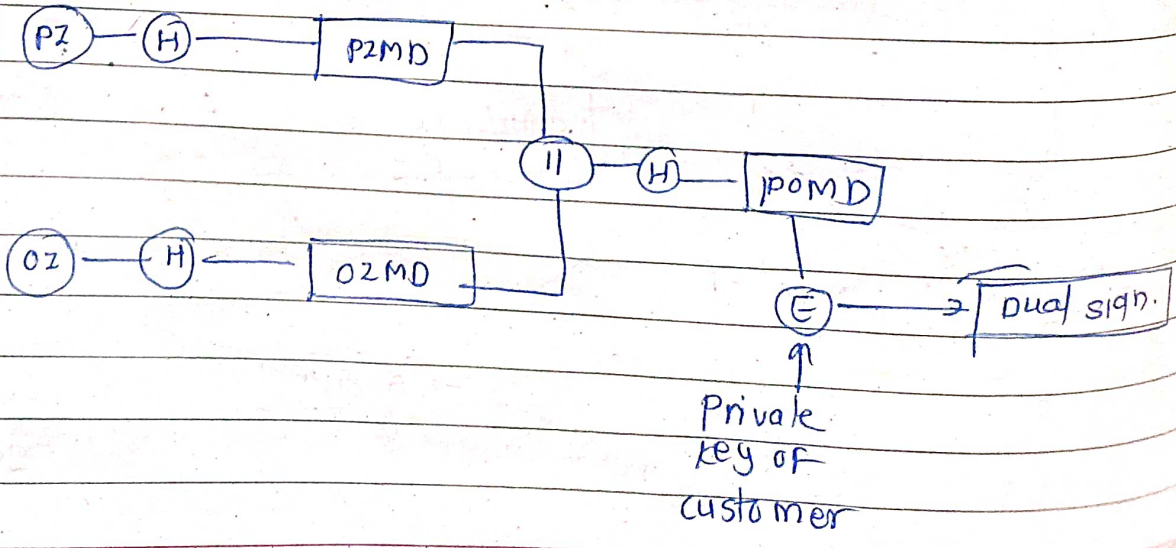
1. order information for merchant
2. payment information for bank

- neither party have details of one another but must know they are linked

Payment capture:

- merchant sends payment gateway a payment capture request.
- gateway check request
- then causes fund to transfered to merchant account
- notifies merchant using capture response

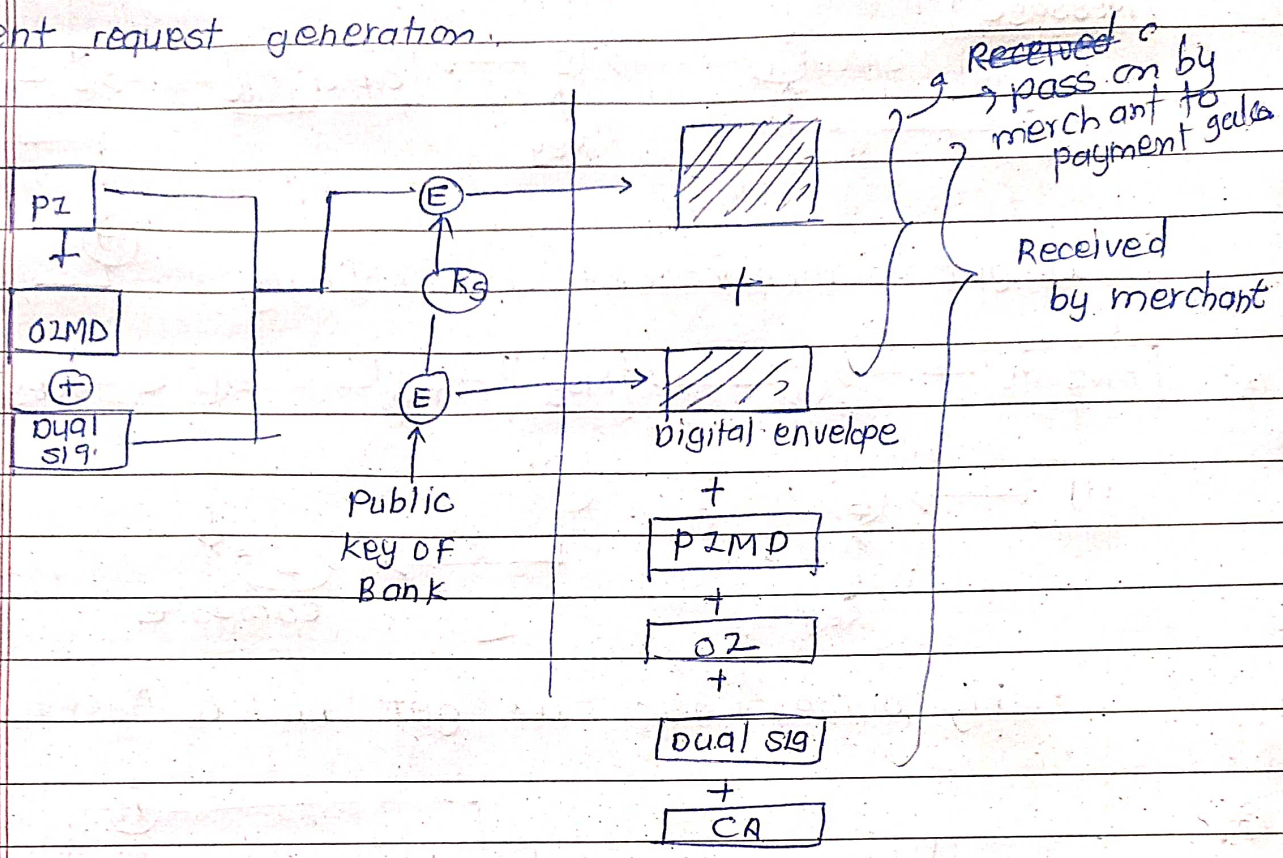
Dual signature (extension)



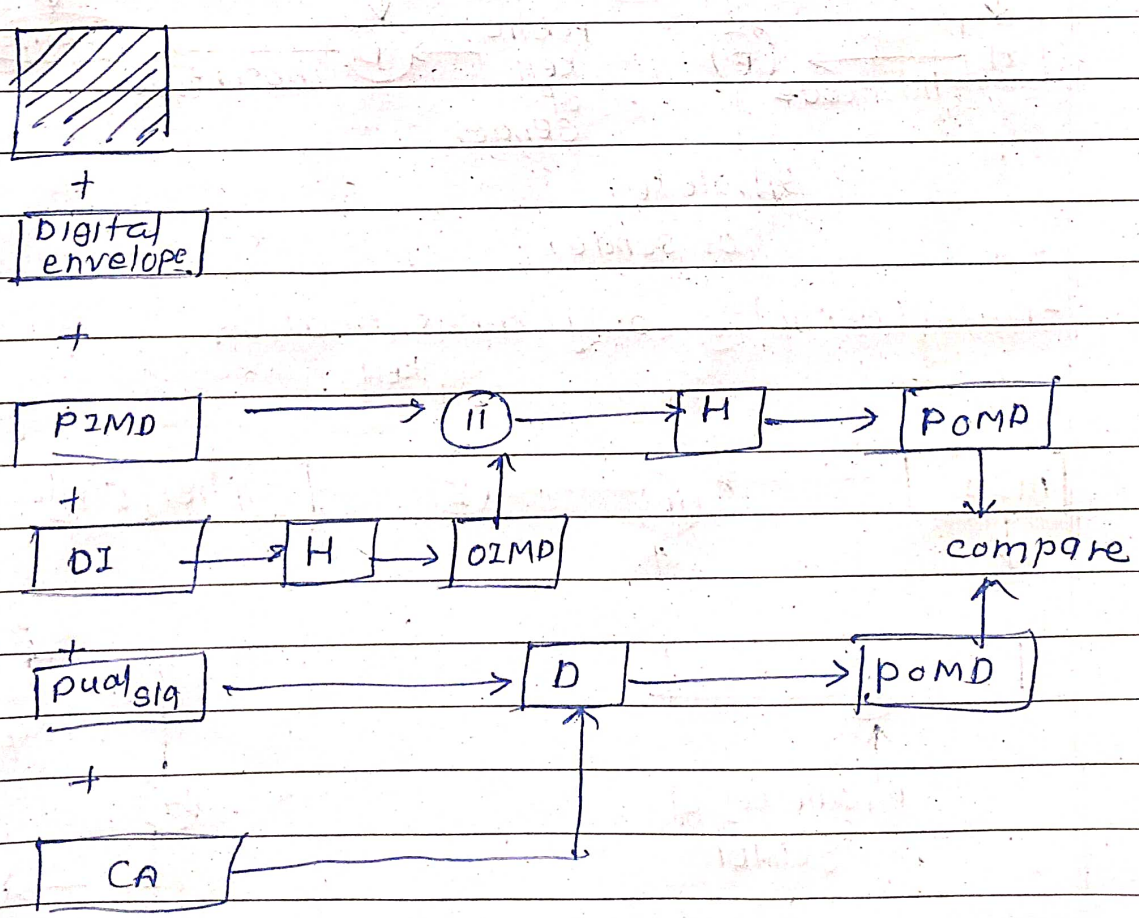
① Purchase request generation
② purchase request validation
③ Payment capture

PAGE No.
DATE / /

* Payment request generation.



* Payment request validation:

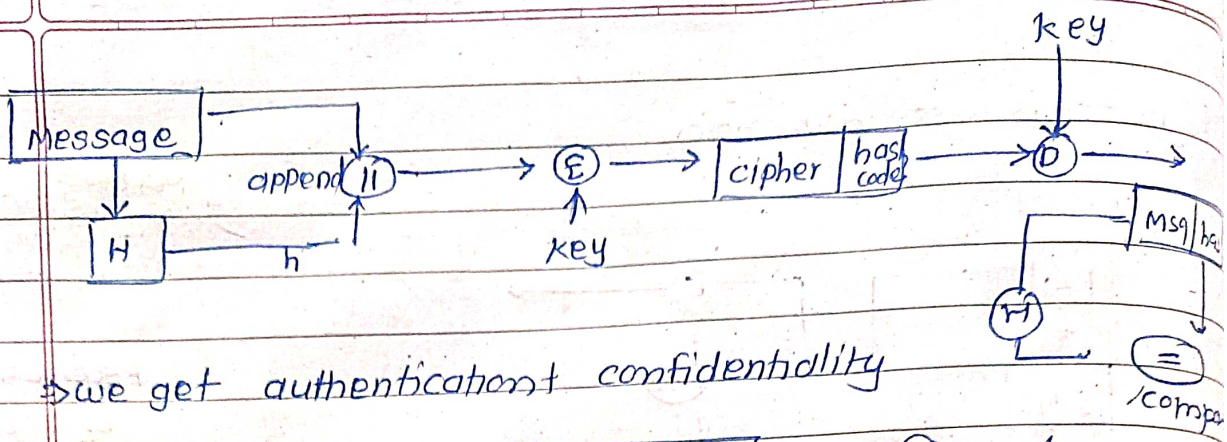


* Hash functions :

- There are 6 situations :

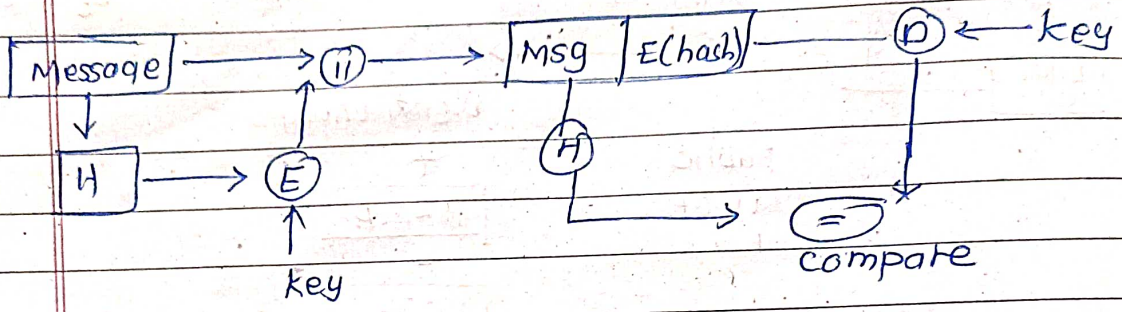
PAGE No.
DATE / /

①



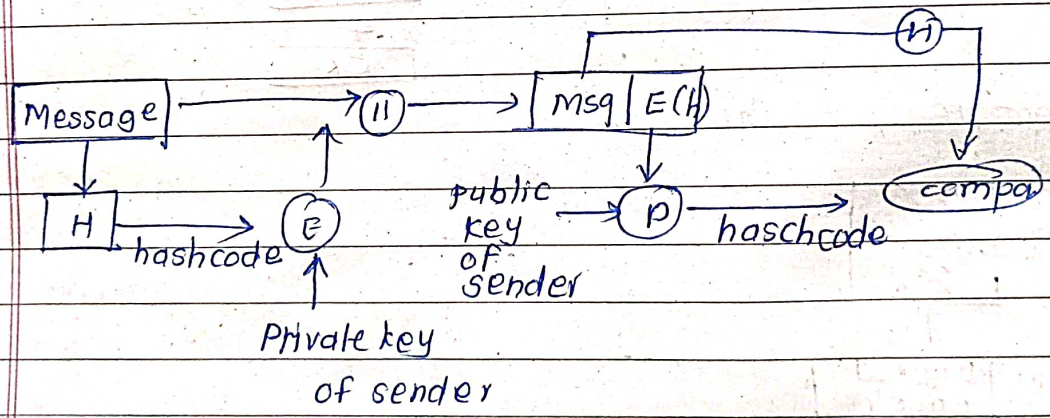
⇒ we get authentication + confidentiality

②



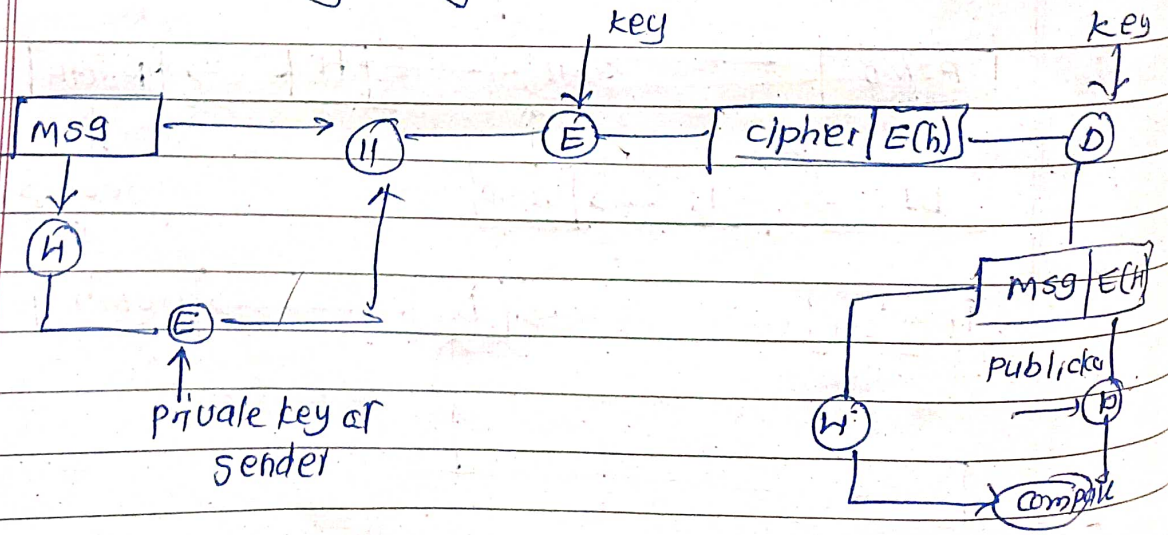
∴ only authentication we get not confidentiality.

③



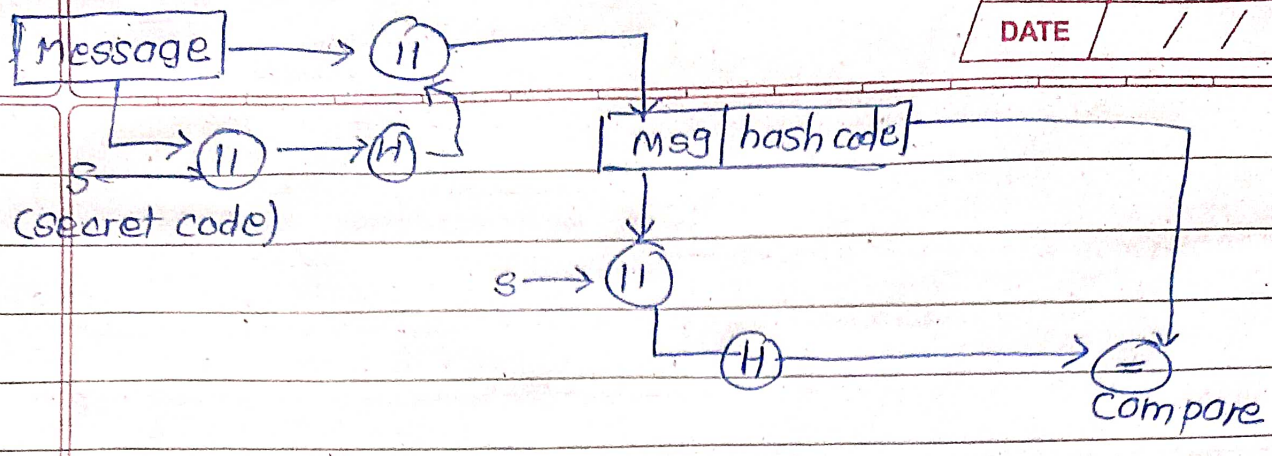
- no confidentiality, only authentication

④



⇒ Here we get authentication and confidentiality

(5)



- No confidentiality and only authentication.

(6) method 6: