\

UNIT-3

Syllobus -:

1.) Security Services in E-Mail

2.) Established keys

3.) Privacy in E-Mail

4.) PGP

5.) Digital Signature

6.) Mime, S-Mime

7.) ~~Certificate and key revocation~~

→ Security Services -:

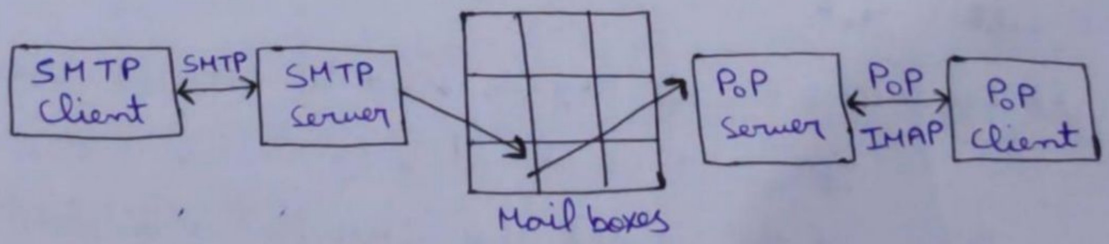
E-Mail uses basic 4 types of protocols -:

Used as Mail Sub. Protocol From C→S] ① Simple Mail Transfer Protocol (SMTP)

Used to Pull the msg. from Mail boxes] ② Post office Protocol (PoP)

Same as PoP] → ③ Internet Mail Access Protocol (IMAP)

④ Multipurpose Internet Mail Extension (MIME)
(Used to Encode Non-text messages such as Media)



=) Services :

- Privacy, of Content
- Authentication, of Sender
- Integrity, of the msg. content
- Non-Repudiation, No Denial of Sender/Receiver
- Proof of Submission, Sender proofs that he has send the mail

- Proof Delivery, Proof that receiver has got the mail
- Message Flow confidentiality, Details of the mail sent is hidden from 3rd user/person
- Anonymity, Identity of sender is hidden from receiver
- Containment, keeping msgs in a security zone
- Audit, event log (ability to record events, so that later it can be find out who has send the message to whom)
- Accounting, Maintenance of usage statistics
- Self Destruct, Message is been destructed after a lifetime or being received by the receiver
- Msg Sequence Integrity, E-Mails are received in the order in which they are sent

→ Established keys -: There are 3 types of Established keys:

i) Public key - The Public key is used to encrypt the data

It can be used by anyone

It is used to encrypt the plain text and convert it into cipher text

ii) Private key - The Private key is used to decrypt the data

It cannot be shared, only receiver can see this key

It is used to decrypt the cipher text into plain text

iii) Secret key - The secret key is used for both Encryption and (same) decryption

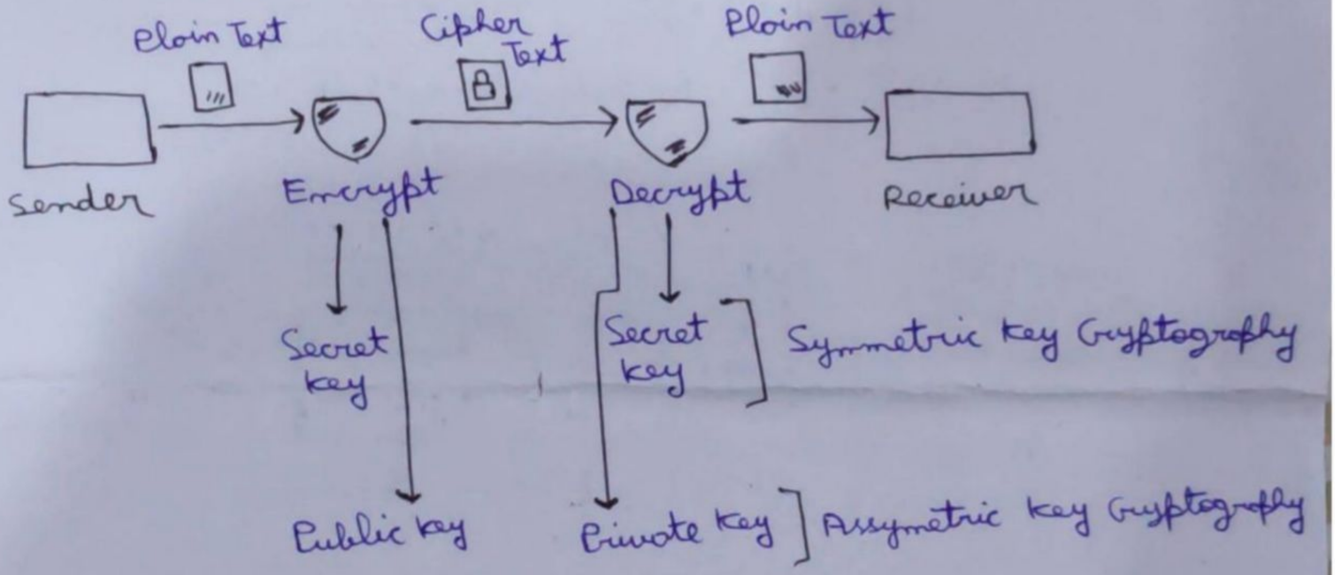
It is also called as Symmetric key (Cryptography)

Both sender and receiver share the same secret key

⇒ Advantages and Disadvantages of Secret key

- Easy Implementation
- less complex as compared to Public, Private key

•) If the secret key (used for both encryption and decryption) comes in the hands of attacker, he can easily decrypt the msg and modify it [loss of Data Integrity and confidentiality]



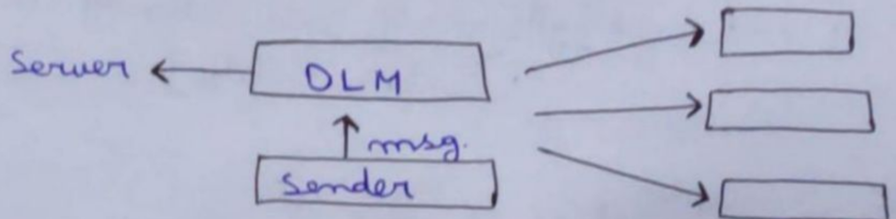
→ Privacy in E-Mail -: When we send messages to multiple users, we need to encrypt every message, secret key is used for encryption and public key is used for decryption of the messages.

⇒ Distribution List Exploder - Maintains the list of E-Mail address to whom we have to send the message

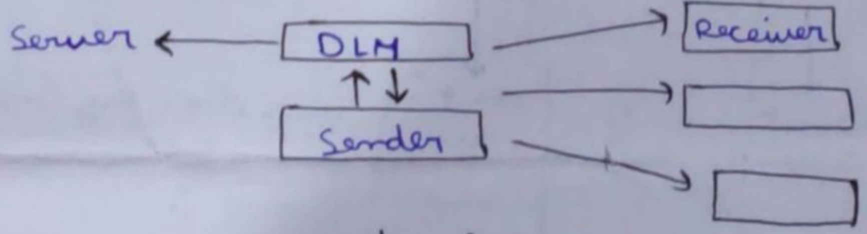
Two types:

1.) Remote Explode method - In this method, DLM server is responsible for sending messages to multiple receivers. Not much trusted

2) Local Explode Method - In this process, DLM tells the email addresses to which the mail message has to sent and the sender itself is responsible for sending the messages to receivers



Remote Exploder method



Local Explode method

PGP -: · Also known as Pretty Good Privacy

· Father of PGP was Phil Zimmermann

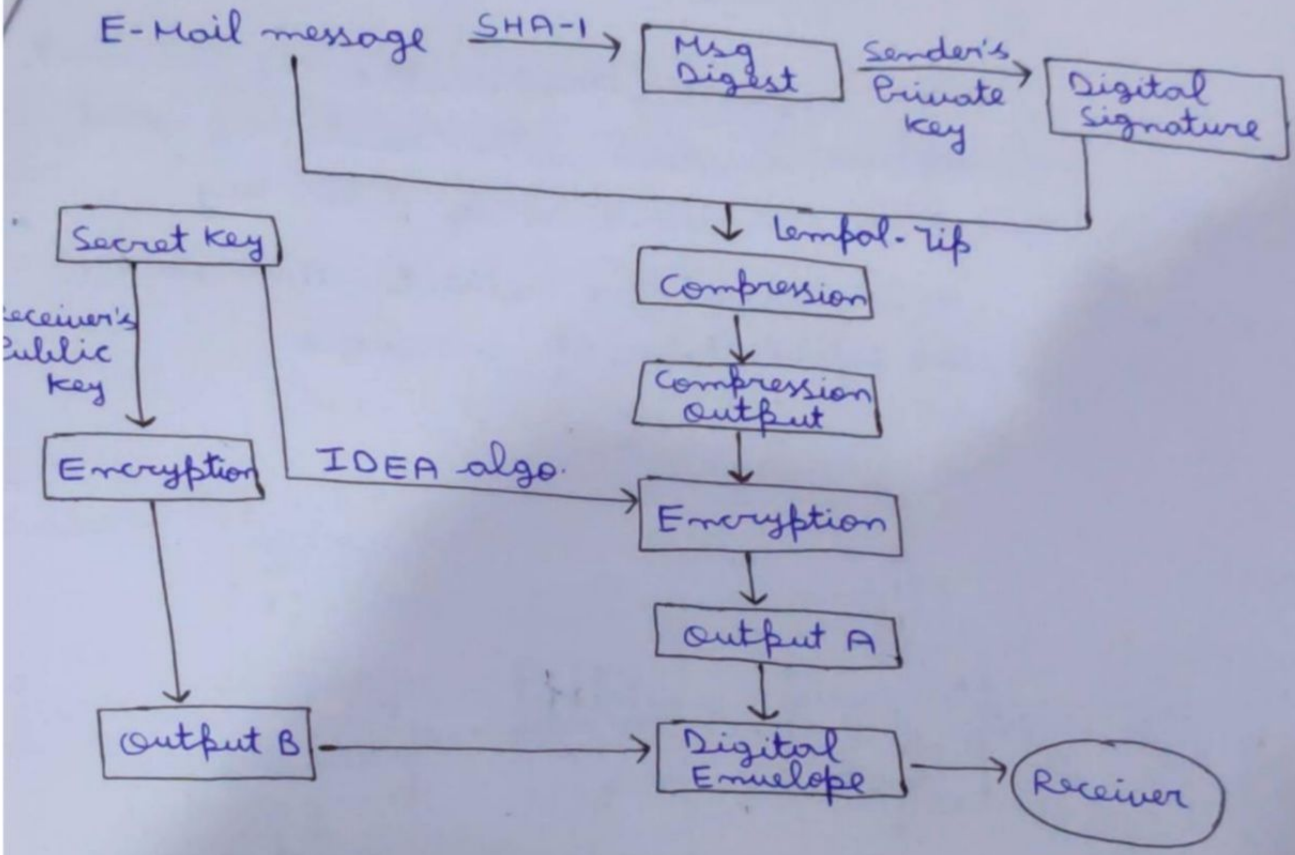
· It is a Encrypt program which provides privacy and authentication for data communication

· Its main aim is to increase the Security of E-Mail communication

· It Provides :

- Authentication through the use of Digital Signature
- Confidentiality through the use of Symmetric block encryption
- Compression by using the ZIP algo.

→ Working of PGP

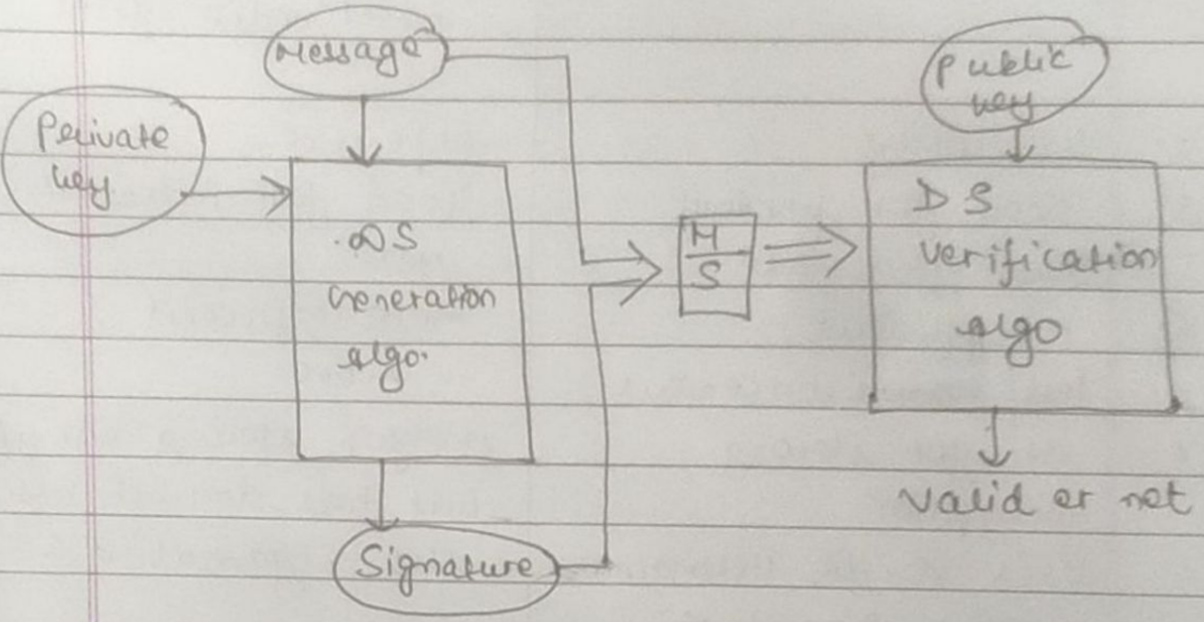


1. The E-Mail Message is converted into Message Digest by using SHA-1 algorithm
2. With the help of Sender's Private-key, we generate Digital Signature
3. By using Lempal. Zip algo. (Compression algo), E-Mail message and Digital Signature is compressed
4. Compression output is generated
5. Now. the compression output is Encrypted using Secret key by the help of IDEA algo. At output A, we have the Encrypted message
6. The Secret key is encrypted using Receiver's Public key. and Output B is generated
7. By output A and B, Digital Envelope is generated and that is finally sent to the receiver

key => sequence of no. which has to be complex/unique

* Digital signature :-

proof in the hand of receiver that the documents received, it is coming from a verified/correct entity



Sender

has info. of its own private key and public key as well as public key of receiver

Receiver

has info. of its own private key and public key as well as public key of sender

If sender is encrypting any message at its end by using private key then it can only be decrypted by receiver's end by using sender's public key.

If the receiver is able to decrypt the message in a meaningful way by using sender's public key then we can say that message is coming from valid entity

	PGP	S/MIME
(1)	Designed for processing plain text	designed to process email as well as multimedia files
2.	less costly	expensive
3.	Good for personal and office use	good for industrial use.
4.	less efficient	more efficient
5.	less ~~[illegible]~~ convenient	more
6.	st. for strong encryption	st. for strong encryption but has drawbacks.
7.	uses Diffie Hellman Digital signature	uses Elgamal DS
8.	high overhead	low overhead

* Anomaly Detection :-

→ ~~[illegible]~~ Anomaly detection is the identification of rare events, items or observations which are suspicious because they differ significantly from stand. behaviours or patterns.

→ ~~anomaly detection~~

→ Companies use anomalous activity detection to define system baseline, identify deviations from that baseline and investigate inconsistent data.

→ Types :-

(I) Supervised ⇒ labelled set data

(II) Semi- supervised

(III) Unsupervised ⇒ unlabeled | unstructured data

* S/MIME Protocol :

MIME Protocol :

Multipurpose Internet Mail Extension

Previously emails could be sent only in
NVT 7-bit ASCII format
(i.e, audio / video / images etc could not be sent)

∴ MIME is introduced
which allows us to transfer non ASCII da
over mail.

S/MIME Protocol :

→ Secure MIME extension to MIME
→ encrypts mail and provides security
→ allows us to digitally sign on our mail
→ Uses asymmetric key cryptography
uses diff. keys for encryption
and decryption

Functions :

(i) Authentication
(ii) Messag integration ⇒ no modification
(iii) Non-Repudiation
(iv) Privacy
(v) Data Security

Services :

(i) Digital Signature (ii) Message encryption