UNIT-3

Syllabus -:

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 -:

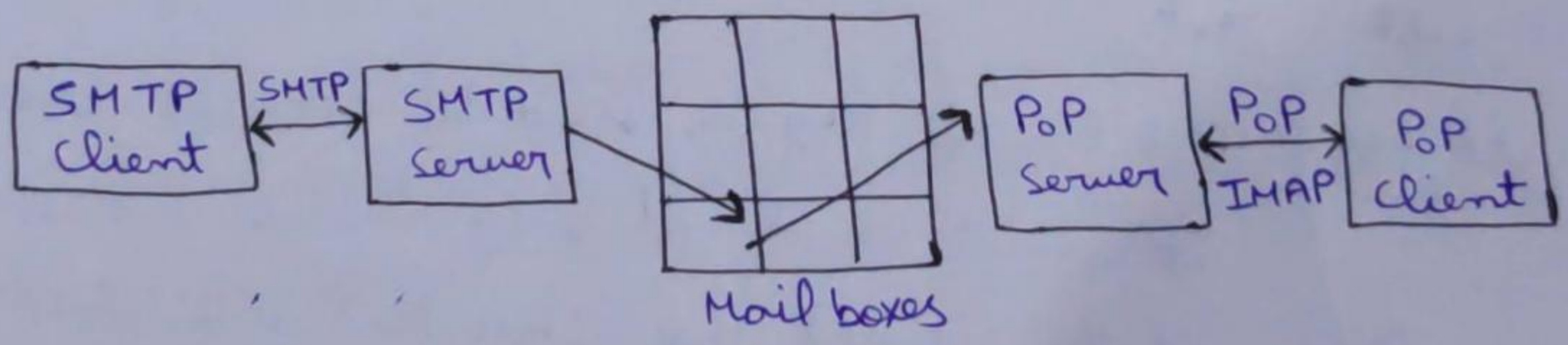
E-Mail uses basic 4 types of protocols -:

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

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

③ Internet Mail Access Protocol (IMAP) — Same as PoP

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, Maintenence 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

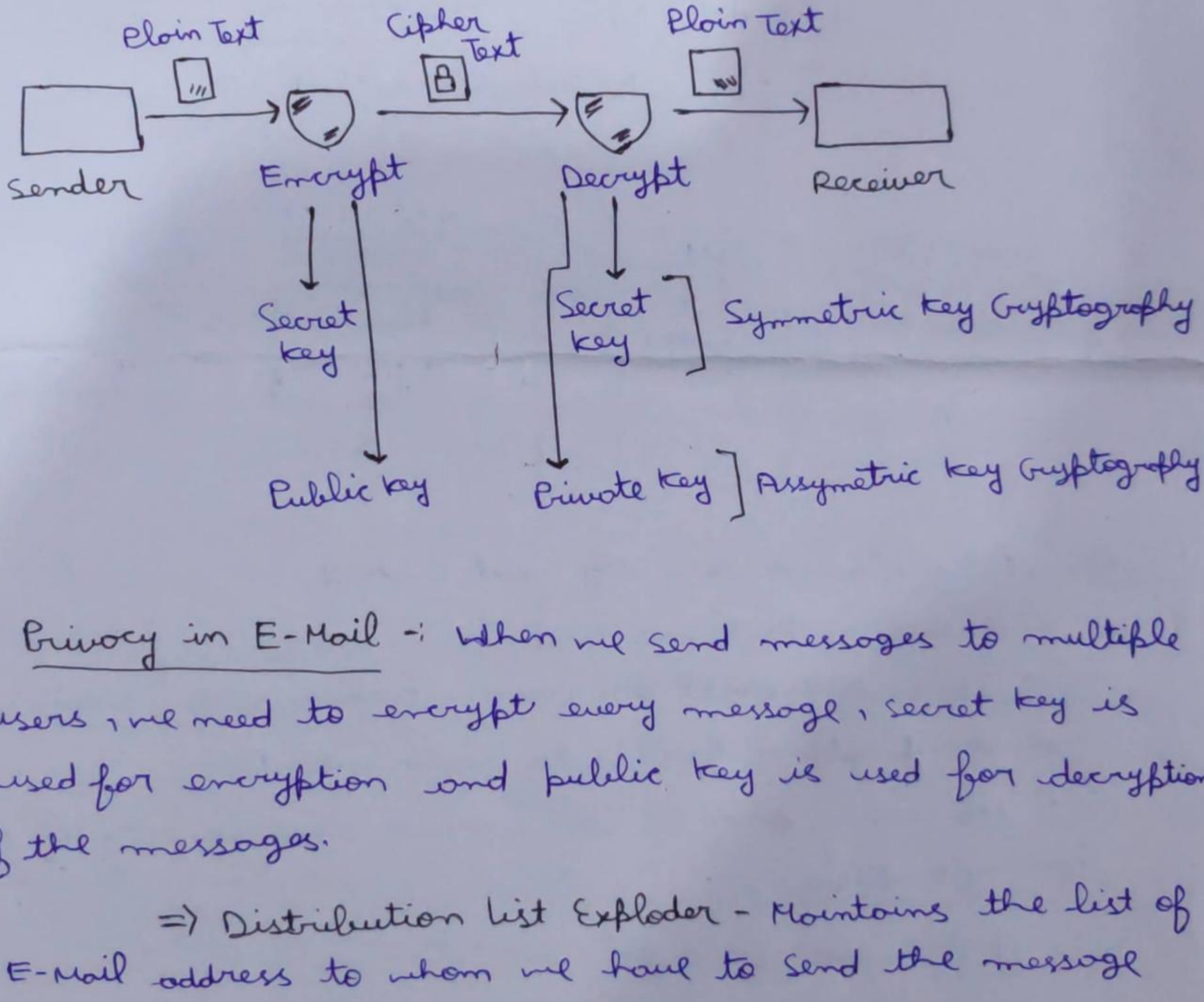
ii) Private key - The Private key is used to decrypt the data
It cannot be shared, only receiver can see this key
It is used to decrypt the cipher text into plain text

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]



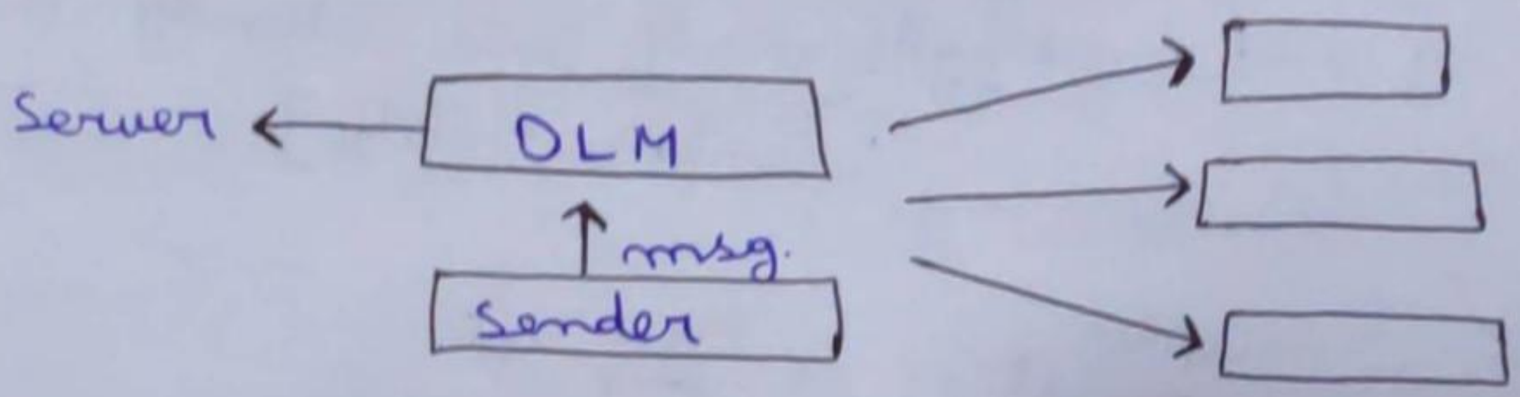
→ Privacy in E-Mail -: When we send messages to multiple users, we need to encrypt every message, secret key is used for encryption and public key is used for decryption of the messages.

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

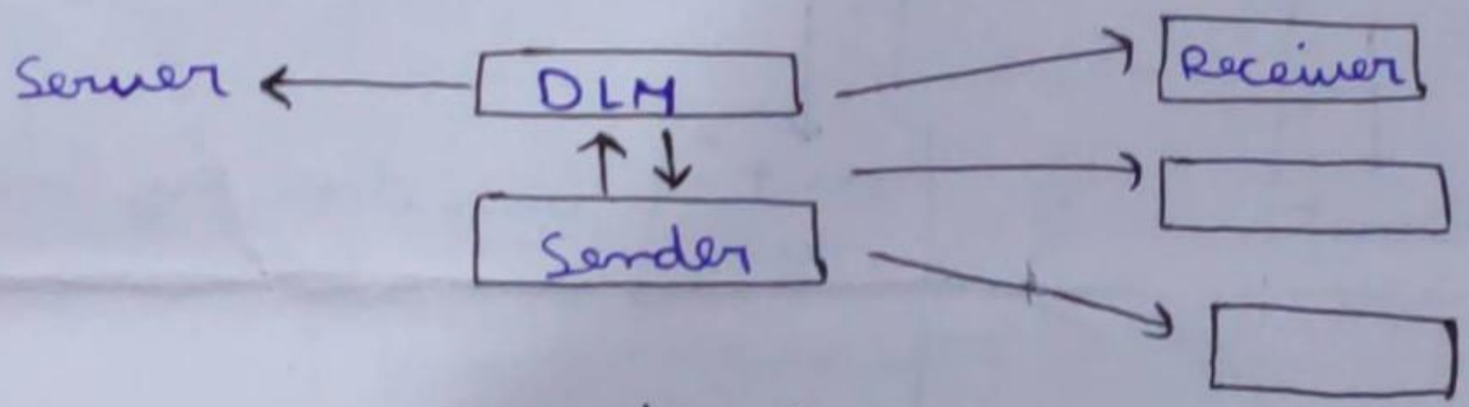
Two types:

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 be 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

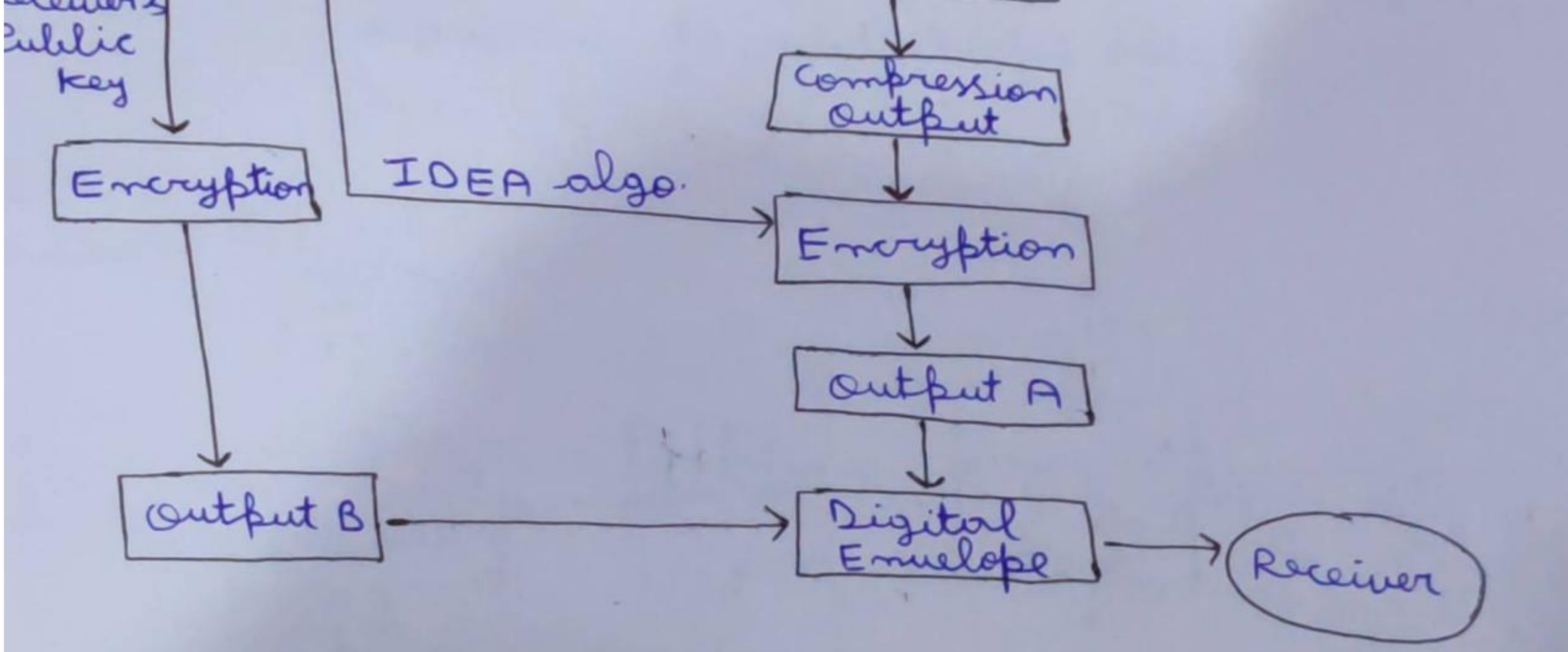
• It is a Encrypt program which provides privacy and authentication for data communication

• 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

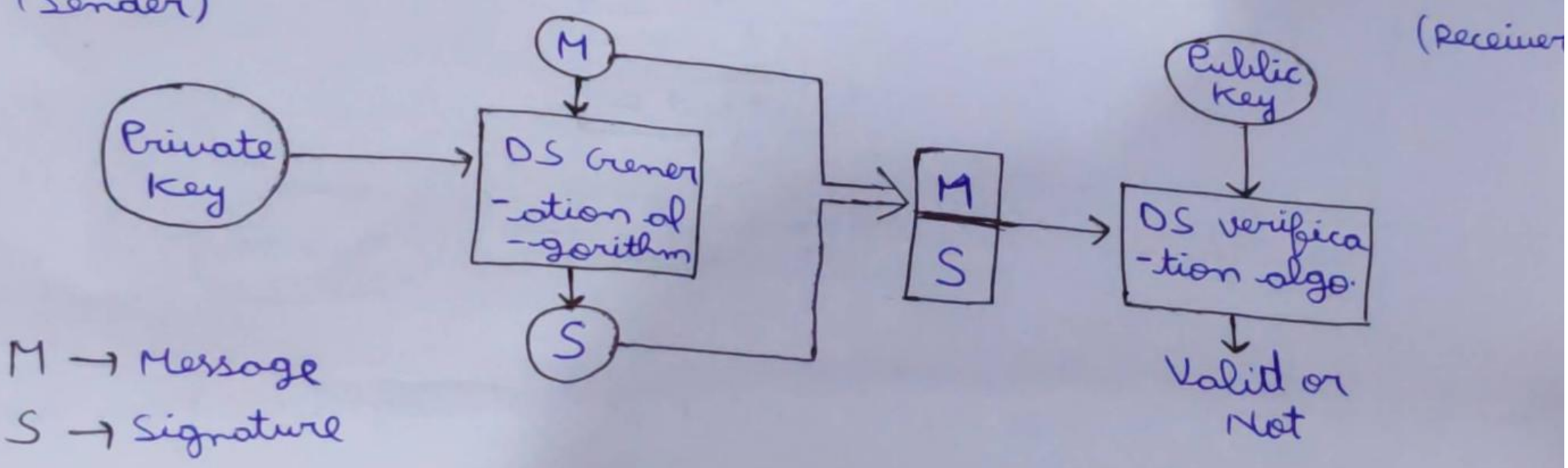
⑥ The Secret key is encrypted using Receiver's Public key, and Output B is generated

⑦ By output A and B, Digital Emuelope is generated and that is finally sent to the receiver

⇒ Digital Signature -: • Signature is a proof in the ↓ of the receiver

↳ • It is an Assymmetric key in which Encryption is done with Private key and Decryption is done using Public key

• It is used for Authentication and Non-Repudiation of messages

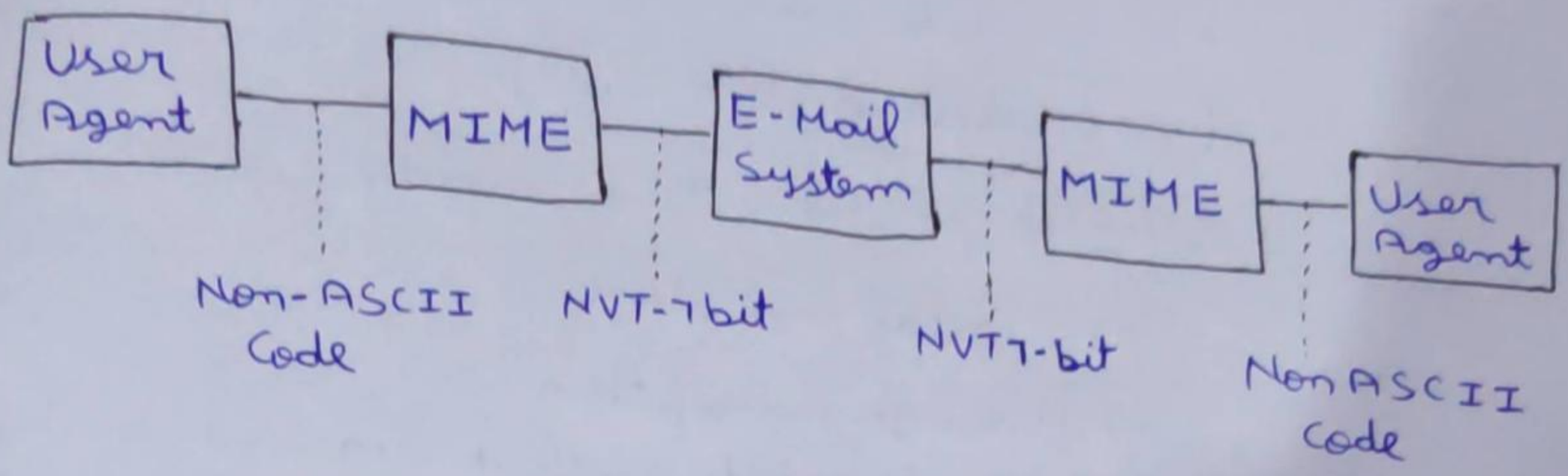


⇒ MIME -: • Stands for Multi Purpose Internet Mail Extension

• It is a protocol that allows user to exchange different kinds of data files on the Internet such as audio, video and images

• Now, since the E-Mail sents only text message, in the form of NVT 7-bit ASCII format, so the purpose of MIME is to Convert the Non-ASCII code into ASCII format so that images, audio and video files could be transferred from one user to another through E-Mails.

Working of MIME :



→ MIME Header -

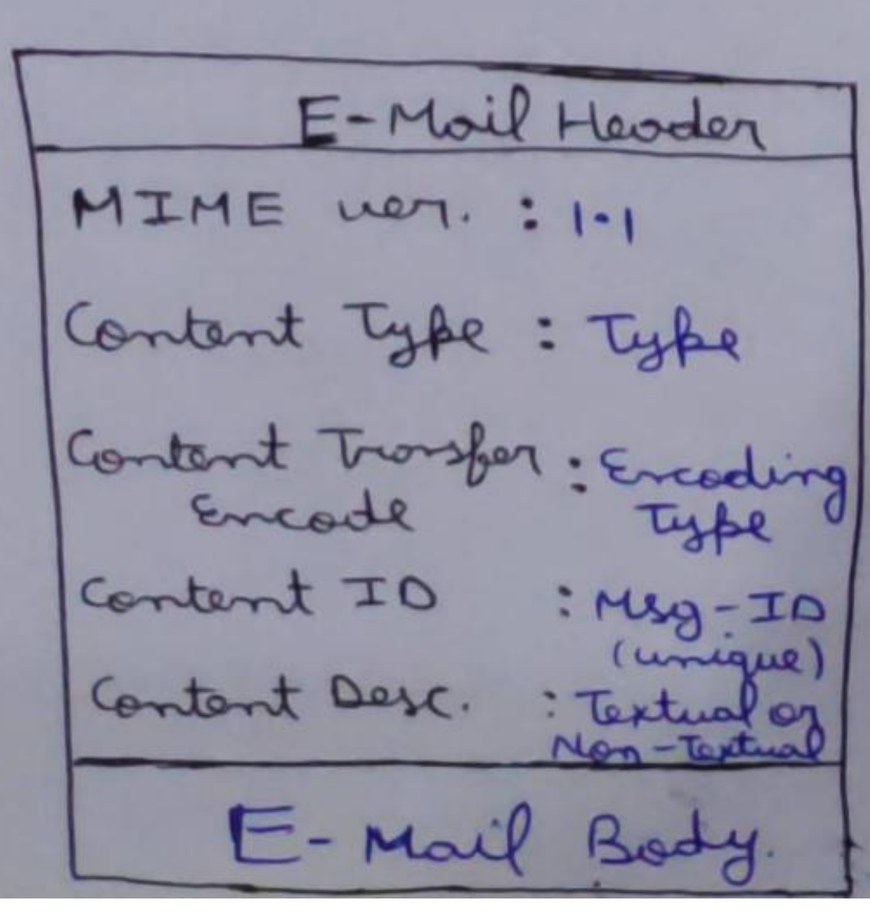
i) MIME version, Current version of MIME used

ii) Content Type, It defines the type of data used in the message (audio, video etc)

iii) Content Transfer Encode, It defines the method used for Encoding

iv) Content ID, It helps in uniquely identifying the message

v) Content Description, It defines whether the body is actually textual / non-textual



→ S/MIME : • Stands for Secure Multipurpose Internet Mail Extension, extension of MIME

• It provides security for commercial E-Mail (by Encrypting the mail)

• S/MIME provides two security services

a.) Digital Signature

b.) Message Encryption

• It is a widely accepted method for sending digitally Signed and Encrypted messages

Functions of S/MIME :

① Authentication

② Message Integrity

③ Non-Repudiation

④ Privacy

⑤ Data Security (using Encryption)