E-Mail

Email (Electronic mail) is a digital method by using it we exchange messages between people over the internet or other computer networks. With the help of this, we can send and receive text-based messages, often an attachment such as documents, images or videos, from one person or organization to another.

It was one of the first applications developed for the internet and has since become one of the most widely used forms of digital communication. It has an essential part of personal and professional communication, as well as in marketing, advertising and customer support.

Email Architecture:-

Basics of email:-

1) An email address: This is a unique identifier for each user, typically in the format of name@domain.com.

2) An email client: This is a software program used to send, receive and manage emails, such as Gmail, Outlook or Apple mail.

3> An email server:- This is a computer system responsible for storing and forwarding emails to their intended recipients.

Key Components:

1> User Agent (UA):-

-> Software applications used to send and receive emails (eg: Outlook, Gmail, ~~?~~)

-> Responsible for:-

- * Composing messages
- * Reading received emails
- * Managing User mailboxes.

2> Mail transfer Agent (MTA):-

-> Servers responsible for transferring emails between domains or servers.

-> Functions:-

- * Receives outgoing emails from the UA.
- * Routes the emails to the recipients server using protocols like SMTP.
- * Pushing emails from sender to receiver.

3> Mail Access Agent (MAA):-

-> The MAA allows users to connect to their mailboxes on a server.

→It provides functionalities like:-

* Reading emails stored on the server.

* Managing folders

* Synchronizing email content across devices.

→It works along side protocols like IMAP and POP3.

4) Mail storage:-

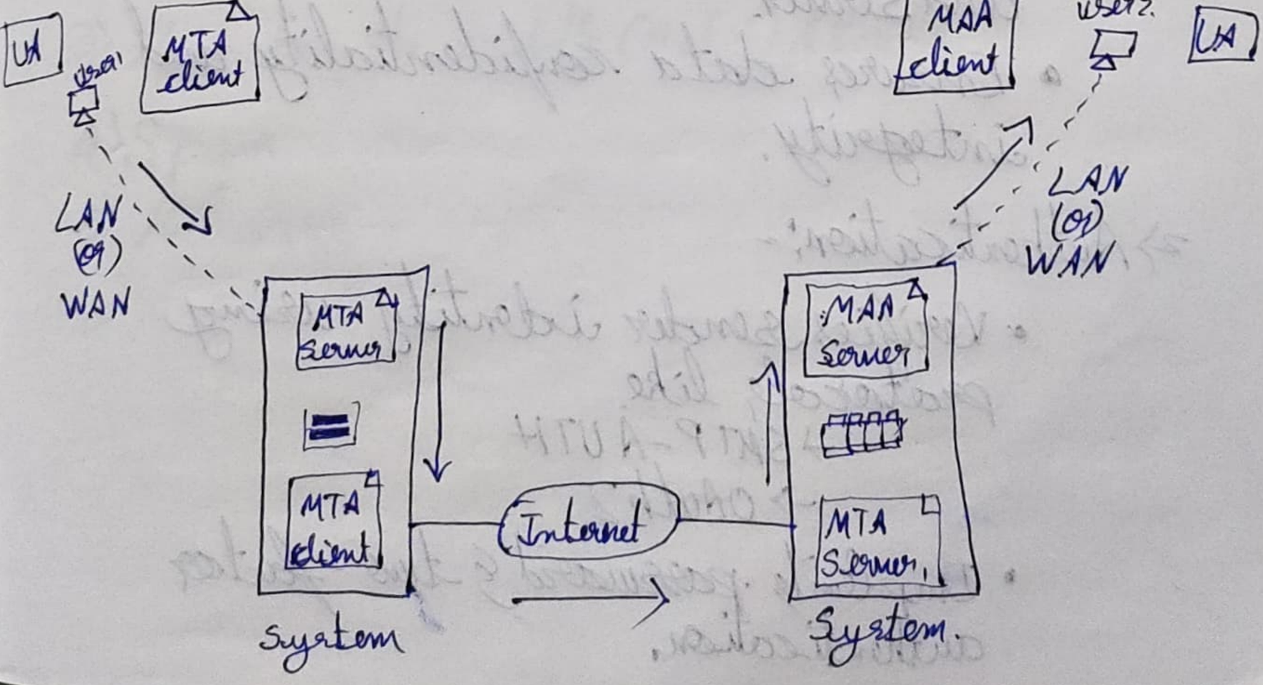
→Stores emails securely on the server for access by recipients.

→Uses access control and encryption for data protection.

5) DNS (Domain Name System):

→Converts domain names to IP addresses.

→Identifies mail servers for specific domains using MX (Mail Exchange) records



Protocols Used

→ SMTP (Simple Mail Transfer Protocol).

→ POP3 (Post office Protocol V3)

→ IMAP (Internet Message Access protocol)

Email Security Mechanisms & Policies.

The email policies and Security Mechanisms are a set of regulations and standards for protecting the privacy, accuracy and accessibility of email communication within the organization. An email security policy & security Mechanisms should include the following essential components:-

1) TLS/SSL:-
- Encrypts communication between client and server.
- Ensures data confidentiality and integrity.

2) Authentication:-
- Verifies sender identity using protocols like
  → SMTP-AUTH
  → OAuth2.
- Implents password & two-factor authentication.

3> Encryption:-

- End-to End Encryption ; Secure message content from sender to recipient.
- Common standards:-
  - → PGP (Pretty Good Privacy)
  - → S/MIME (Secure/ Multipurpose Internet Mail Extention)

4> Virus protection.

5> DKIM (Domain Keys Identified Mail).

→ Adds a cryptographic signature to validate the sender's domain.

6> SPF (Sender Policy framework):

Security challenges;

1> Phishing Attacks.

2> Spoofing

3> Man-in-the-middle (MITM) Attacks.

4> Spam.

5> Malware.

S/MIME

S/~~M~~MIME (or) Secure/Multipurpose internet Mail Extension is a technology widely used by corporations that enhances email security by providing encryption, which protects the content of email messages from unwanted access.

-> It provides encryption, digital signatures, and message integrity, ensuring secure e-mail exchange.

-> Based on MIME standard, which defines the format of emails that support text, attachments images and multimedia.

S/MIME Uses

S/MIME can be used to:-

-> check that the email you sent has not been tampered with by a third party.

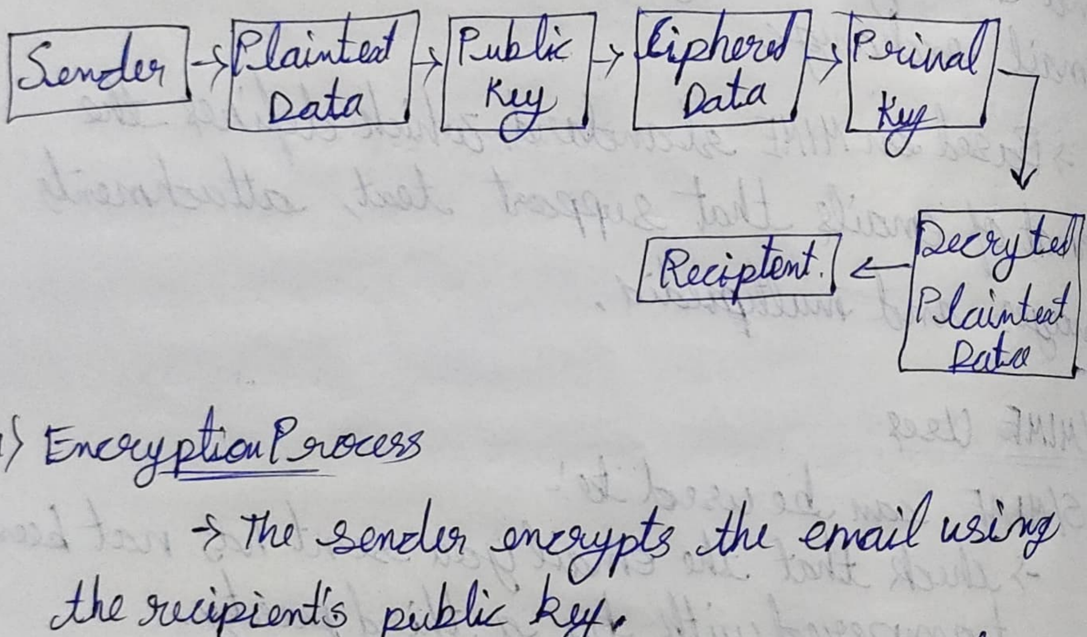
-> Create digital signatures to use when signing emails.

-> Encrypt all emails.

-> Check the email client you're using.

How S/MIME Works:-

To operate, S/MIME employs mathematically related public and private keys. This technology is based on asymmetric cryptography. Because the two keys are mathematically related, a message that was encrypted with the public key (which is, of course, published) can only be decrypted using the private key (which is kept secret).



1> Encryption Process

→ The sender encrypts the email using the recipient's public key.

→ The recipient decrypts the email using their private Key.

2> Digital Signature Process:-

→ The sender creates a digital signature by hashing the email content and encrypting the hash with their private Key.

→ The recipient verifies the signature using the sender's public key.

3> Certificate Verification:-

→ Both sender and recipient rely on X.509 certificates issued by a trusted CA.

→ Certificates ensure the public keys belong to the claimed identities.

Combonents of S/MIME

1> Public key Infrastructure (PKI):-

- S/MIME relies on PKI for encryption and digital signature verification.
- Includes public/Private key pairs and certificates.

2> Certificate Authorities (CAS):-

- Trusted entities that issue and manage X.509 certificates.
- Examples:- DigiCert, GlobalSign, Let's Encrypt.

3> Email clients:-

- Support S/MIME for secure email exchange (e.g: Microsoft Outlook, Thunderbird).

Key features of S/MIME:-

1) Encryption:-

- Protects the email content from being read by unauthorized parties.
- Ensures confidentiality by encrypting the message body & attachment,

2) Data integrity:

- Message encryption & digital signatures offers data integrity services as a result of the operations that make encryption possible.

3) Certificate-Based security:

- Uses X.509 certificates to validate identities,
- Certificates are issued by trusted Certificate authorities (CAs).

4) Interoperability:-

- Works with most modern email clients & servers Eg:- Outlook, Gmail, Apple Mail

Steps to enable S/MIME in Email clients:-

1) Obtain an S/MIME certificate from a trusted CA.

2) Install the certificate on your email client.

3) Configure your email client to use S/MIME for sending & receiving emails,

4) Exchange public keys with recipients to enable encryption.

Advantages of S/MIME:-

1) Strong Security.
2) Wide adaption.
3) End-to-End Encryption.
4) Authentication.

Disadvantages of S/MIME:-

1) Certificate Management.
2) Cost.
3) Complexity.
4) Dependance on PKI.