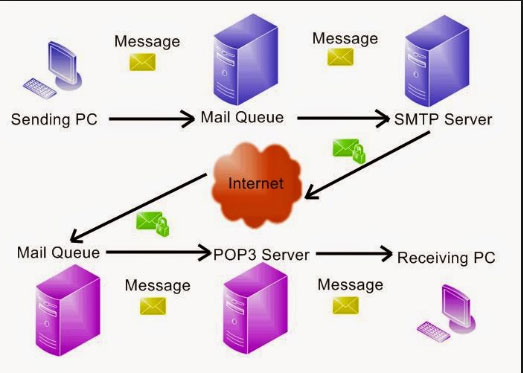
**Câu 1.Trình bày về mô hình truyền/nhận thư điện tử. Các thành phần chính trong hệ thống, mối quan hệ giữa các thành phần đó ?**

* Mô hình truyền/nhận thư điện tử:



* Web Mail (Phần mềm thư điện tử qua Web): loại phần mềm thư điện tử không cần phải cài đặt mà nó được cung ứng bởi các máy chủ (web server)
* MUA (Mail User Agent) –Email Client: Là loại phần mềm thư điện tử được cài đặt trên từng máy tính của người dùng.
* MTA (Mail Transfer Agent): là máy chủ thư điện tử, nhằm cung ứng các dịch vụ thư điện tử
* Cách thức truyền tin:
* Soạn thảo: nhập các trường chính như: chủ đề, nội dung, đối tượng nhận gửi, thông tin phần định dạng,…
* Thư sẽ được chuyển đổi sang một định dạng chuẩn xác định bởi RFC 822 (Standard for the Format of ARP Internet Text Messages)
* Thư sau khi chuyển đổi sẽ gồm hai phần: phần tiêu đề (header) và phần thân (body)
* Quá trình gửi thư
* MUA kết nối tới MTA trên Mail Server
* MUA cung cấp thông tin cho MTA: định danh đối tượng gửi, nhân thư, DNS,…
* Máy chủ thư sẽ thực hiện các thao tác: Định danh đối tượng nhận, thiết lập kết nối truyền thư

**Câu 2.Trình bày một số giao thức truyền/nhận thư cơ bản: SMTP, MINE, IMAP, POP3; tìm hiểu và cho ví dụ về mã hóa base64.**

* 1. **SMTP:**
* SMTP là giao thức tầng ứng dụng, SMTP được đánh giá là một giao thức truyền thông điệp thư đáng tin cậy và có hiệu quả cao
* SMTP chạy trên tầng TCP/IP, sử dụng port 25.
* **Định dạng bản tin**

SMTP: giao thức để trao đổi các bản tin thư điện tử

RFC 822: chuẩn định dạng bản tin dạng văn bản

* Header lines, ví dụ

– To:

– From:

– Subject:

khác *Lệnh SMTP*

* body

– bản tin, ký tự ASCII

**Thủ tục làm việc SMTP:**

Mỗi phiên làm việc SMTP gồm các phần sau:

– Khởi tạo phiên (Session Initiation)

– Khởi tạo Client (Client Initiation)

– Truyền thư (Mail Transactions)

– Kết thúc phiên và kết nối (Terminating Session and Connections)

**Các trạng thái của SMTP:**

– Khi Client gửi 1 lệnh SMTP tới Server, client nhận trả về 1 mã trạng thái cho máy gửi biết điều gì đã xảy ra.

– Với thông điệp đáp trả có gắn 3 con số ở đầu dòng để thể hiện từng trạng thái riêng.

**Hạn chế của SMTP:**

– Chỉ sử dụng với dữ liệu dạng ASCII 7 bit.

– Không có cơ chế xác thực

– Thông điệp gửi đi không được mã hóa

– Dễ bị tổn thương (bởi spam, mất định danh người gửi)

**Giải pháp:**

– SMTP mở rộng

– MIME (Mở rộng thư tín Internet đa mục tiêu)

* 1. **Giao thức MINE**

MIME (Multipurpose Internet Mail Extension): RFC 2045, 2046.

* Là một chuẩn Internet về định dạng cho thư điện tử. Hầu như mọi thư điện tử Internet được truyền qua giao thức SMTP theo định dạng MIME. Vì gắn liền với chuẩn SMTP và MIME nên đôi khi thư điện tử Internet còn được gọi là thư điện tử **SMTP/MIME**.
* MIME cho phép gửi các thông điệp trên internet mà không chỉ thuần là văn bản, có thể gửi mail kèm ảnh, link, ….
* MIME không chỉ dùng cho mail mà có thể dùng cho các message nói chung, ví dụ như trong http
* Thêm các dòng trong Header của bản tin khái báo kiểu nội dung MIME : MIME version, method sử dụng để mã hóa dữ lieeuk, kiểu dữ liệu đa phương tiện, kiểu con, khai báo tham số, dữ liệu đã mã hóa
* Biến đổi dữ liệu non-ASCII sang dạng ASCII
  1. **Phương pháp mã hóa base64**

Gồm các bước chính sau:

* Chia file nhị phân thành nhiều nhóm nhỏ dài 3byte
* Mã hóa từng nhóm 3byte thành 4 ký tự ASCII 7bit in ấn như sau:
* Gộp 3 byte thành 24bit liên tiếp, chia thành 4 nhóm 6bit có giá trị từ 0-63.
* Mỗi nhóm 6bit tương ứng với 1 ký tự in ấn như sau:

0-25 -> A-Z

26-51-> a-z

52-61-> 0-9

62-> +

63-> /

Ví dụ:



* 1. **Giao thức POP3**

**Tổng quan giao thức:**

* POP3 ( Post Office Protocol ver 3) là giao thức tầng ứng dụng, dùng để truy nhập và lấy thư điện tử từ mailbox trên máy chủ thư tín thông qua kết nối TCP/IP, port 110.
* Trước POP3 có 2 phiên bản ra đời trước là: Năm 1984 sử dụng POP, 1988 sử dụng POP2. Đến nay, POP3 được sử dụng thông dụng nhất và được xác định trong RFC 1939.

**Hoạt động của POP3**

* POP3 client xác thực thành công với server, server có khóa và mở được maildrop thích hợp. Client có thể truy nhập tới mailbox của mình trên server để kiểm tra, nhận thư…
* Nếu Maildrop không mở (-ERR), server đóng kết nối or client gửi lệnh xác nhận và bắt đầu lại từ đầu
* Thiết lập kết nối TCP ở công 110
* Client gửi lệnh QUIT tới server thì trạng thái Trasaction chuyển sang Update.
* Server gửi goodbye tới client và đóng kết nối TCP, kết thúc phiên làm việc.
  1. **Giao thức IMAP**
* **Tổng quan giao thức:**
* IMAP (Internet Messages Access Protocol) được phát minh bởi Mark Crispin năm 1986 tại trường ĐH Stanford.
* IMAP là giao thức hoạt động ở tầng ứng dụng, cho phép Client truy nhập email trên một Server từ xa.
* IMAPv2 được phát minh năm 1987, IMAPv4 được phát minh năm 1994, được miêu tả trong RFC 2060 sử dụng port 143/tcp.
* IMAPv4 email được lưu trữ trên mail server và có thể truy cập từ bất kì máy email client IMAP4 nào trên mạng.
* IMAP4 có thể thực hiện các thao tác như: tạo, xóa, sửa đổi tên mailbox, kiểm tra mail mới, update mail cũ (trong RFC 2822), thiết lập và xóa cờ trạng thái

**\* Mục đích sử dụng IMAP:**

* Tương thích đầy đủ với các chuẩn thông điệp Internet (MIME)
* Cho phép truy nhập & quản lý thông điệp từ nhiều máy tính khác nhau
* Hỗ trợ truy nhập đồng thời tới các mailbox dùng chung
* Phần mềm bên Client không cần biết kiểu lưu trữ file của Server

**Câu 3.Tìm hiểu cơ bản về S/MINE và PGP**

1. **Giao thức S/MINE**

* S/MIME (Security/Multipurpose Internet Mail Extensions (MIME): Là một phiên bản cho giao thức MIME hỗ trợ mã hóa.
* SMIME đưa vào hai phương pháp an toàn cho email dựa trên mã hóa bất đối xứng và PKI.

- Mã hóa email: Động tác mã hóa = mã hóa message bằng public key của người nhận. Giải mã bằng private key của người nhận.

- Xác thực email: Động tác ký = mã hóa message bằng private key của người gửi. Xác thực = dùng public key của người gửi giải mã bản tin.

* Các phiên bản S/MIME
* Phiên bản S/MIME v1: năm 1995, nhưng không được công bố chính thức.
* Phiên bản S/MIME v2 được IETF chính thức công bố vào tháng 3/1998 là một tiêu chuẩn Internet tại RFC 2311 và RFC 2312 . S/MIME đã trở thành một trong những tiêu chuẩn hàng đầu về bảo mật thông điệp.
* Phiên bản S/MIME v3 được IETF đề xuất vào tháng 6/1999 nhằm tăng cường khả năng của S/MIME, bao gồm RFC 2632 , RFC 2633 và RFC 2634, được cập nhật mới đây nhất tại RFC 5751 tháng 1/2010.
* Trong Thông tư số 01/2011/TT-BTTTT ngày 04/01/2011 của Bộ Thông tin và Truyền thông Công bố Danh mục tiêu chuẩn kỹ thuật về ứng dụng công nghệ thông tin trong cơ quan nhà nước quy định Bắt buộc áp dụng tiêu chuẩn S/MIME v3.2 và được xếp vào nhóm Tiêu chuẩn về an toàn thông tin.

1. **Giao thức PGP**

* PGP (Pretty Good Privacy):

- Là một chương trình cung cấp tính năng mã hóa và xác thực cho dữ liệu. PGP thường được sử dụng để ký, mã hóa, và giải mã văn bản, e-mail, các tập tin, thư mục và phân vùng đĩa toàn bộ để tăng tính bảo mật của thông tin liên lạc e-mail.

- Được tạo ra bởi Phil Zimmermann vào năm 1991.

- PGP còn được sử dụng khá phổ biến cho nhiều đối tượng cũng như các ứng dụng khác ngoài e-mail.

* PGP sử dụng các thuật toán:   
  • Mã hóa đối xứng: DES, 3DES, AES, v.v.

• Mã khóa KCK: RSA, ElGamal.

• Hàm băm: SHA-1, MD-5, v.v.

• Chữ ký: RSA, DSS, ECDSA, v.v

**GTAMT\_AT1603\_VŨ HỒNG PHÚC\_AT160245**