**FEATURES OF EMAIL SYSTEM**

* COMPOSING AND SENDING/RECEIVING A MESSAGE
* STORING/FORWARDING/DELETING/REPLYING TO MESSAGE WITH FACILITIES LIKE CC AND BCC
* SENDING A SINGLE MESSAGE TO MORE THAN ONE PERSON
* SENDING TEXT,VOICE,GRAPHICS,VIDEO

EMAIL COMBINES THE BEST FEATURES OF THE TELEPHONE SYSTEMS AND POSTAL SYSTEMS AND IS VERY CHEAP.

**FUNCTIONS OF EMAIL**

* EMAIL PERFORMS THE FOLLOWING 5 FUNCTIONS AND USES TCP/IP AS THE UNDERLYING PROTOCOL
* COMPOSITION: THE EMAIL SYSTEM PROVIDES FEATURES IN ADDITION TO BASIC TEXT EDITOR FEATURES SUCH AS AUTOMATIC INSERTION OF THE EMAIL ADDRESS WHEN REPLYING TO A MESSAGE.
* TRANSFER:THE MAIL SYSTEM TAKES UPON ITSELF THE RESPONSIBILITY OF MOVING THE MESSAGE FROM THE SENDER TO THE RECEIVER BY ESTABLISHING CONNECTIONS BETWEEN THE TWO COMPUTERS AND TRANSFERRING THE MESSAGE USING TCP/IP
* REPORTING: THE SENDER NEEDS TO KNOW IF THE EMAIL MESSAGE WAS SUCCESSFULLY DELIVERED TO THE RECEIVER OR NOT. THIS REPORTING IS DONE BY THE EMAIL SYSTEM.
* DISPLAYING: DISPLAYS INCOMING MESSAGES TO INFORM THE USER WHEN AN EMAIL MESSAGE HAS ARRIVED.
* DISPOSITION: THIS INCLUDES FEATURES SUCH AS FORWARDING,ARCHIVING AND DELETING MESSAGES THAT HAVE BEEN DEALT WITH.

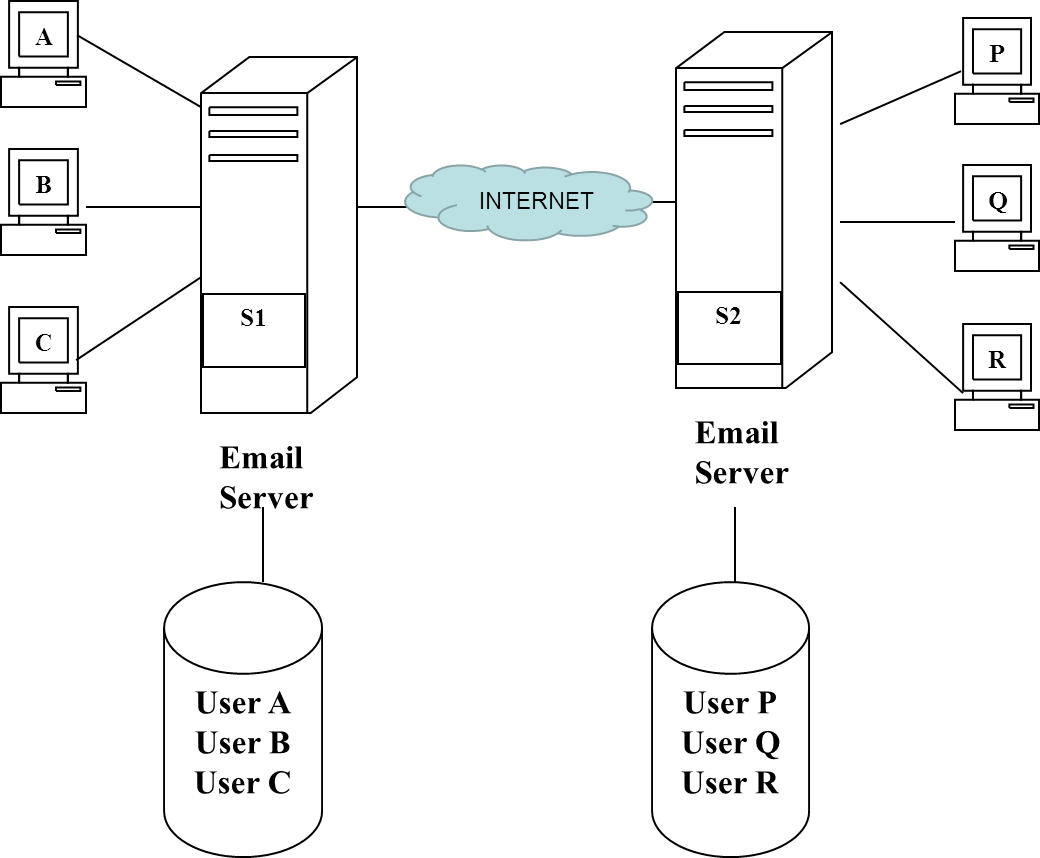
**MAIL BOX**

ASSOCIATED WITH EMAIL IS AN ELECTRONIC MAIL BOX

.AN EMAIL MAILBOX IS A STORAGE AREA ON THE DISK OF A COMPUTER THAT IS USED FOR STORING RECEIVED EMAILS.(SIMILAR TO POSTAL MAIL BOX)

EMAIL COMMUNICATION IS ASYNCHRONOUS ; HENCE A SPECIAL COMPUTER IS GIVEN THE RESPONSIBILITY OF STORING THE EMAILS BEFORE THEY ARE FORWARDED. THIS COMPUTER ALONG WITH THE SOFTWARE IS CALLED A EMAIL SERVER.

THERE IS A MAILBOX ON THE EMAIL SERVER FOR EACH CLIENT CONNECTED TO IT AND WANTING TO USE THE EMAIL FACILITY. IT IS ALWAYS ON . THERE ARE ALWAYS TWO EMAIL SERVERS THAT PARTICIPATE IN ANY EMAIL COMMUNICATION.



* When a user A wants to write an email to P, A creates a message on his PC and sends it. It is first stored on its email server (SI), From there, it travels through the internet to the email server of P (i.e, S2). It is stored in the mailbox of P on the hard disk of S2. When P logs on, his PC is connected to his server (S2) and he is notified that there are new messages in his mailbox. P can then read them one by one, redirect them, delete them or transfer them to his local PC (i.e., download).

**SPOOLING**

THE EMAIL SERVICE HAS A FEATURE CALLED SPOOLING,

THAT ALLOWS A USER TO COMPOSE AND SEND AN EMAIL MESSAGE EVEN IF HIS NETWORK IS CURRENTLY DISCONNECTED OR THE RECIPIENT IS NOT CURRENTLY CONNECTED TO HIS END OF THE NETWORK. WHEN AN EMAIL MESSAGE IS SENT, A COPY OF THE EMAIL IS PLACED IN A STORAGE AREA ON THE SERVER’S DISK, CALLED SPOOL.

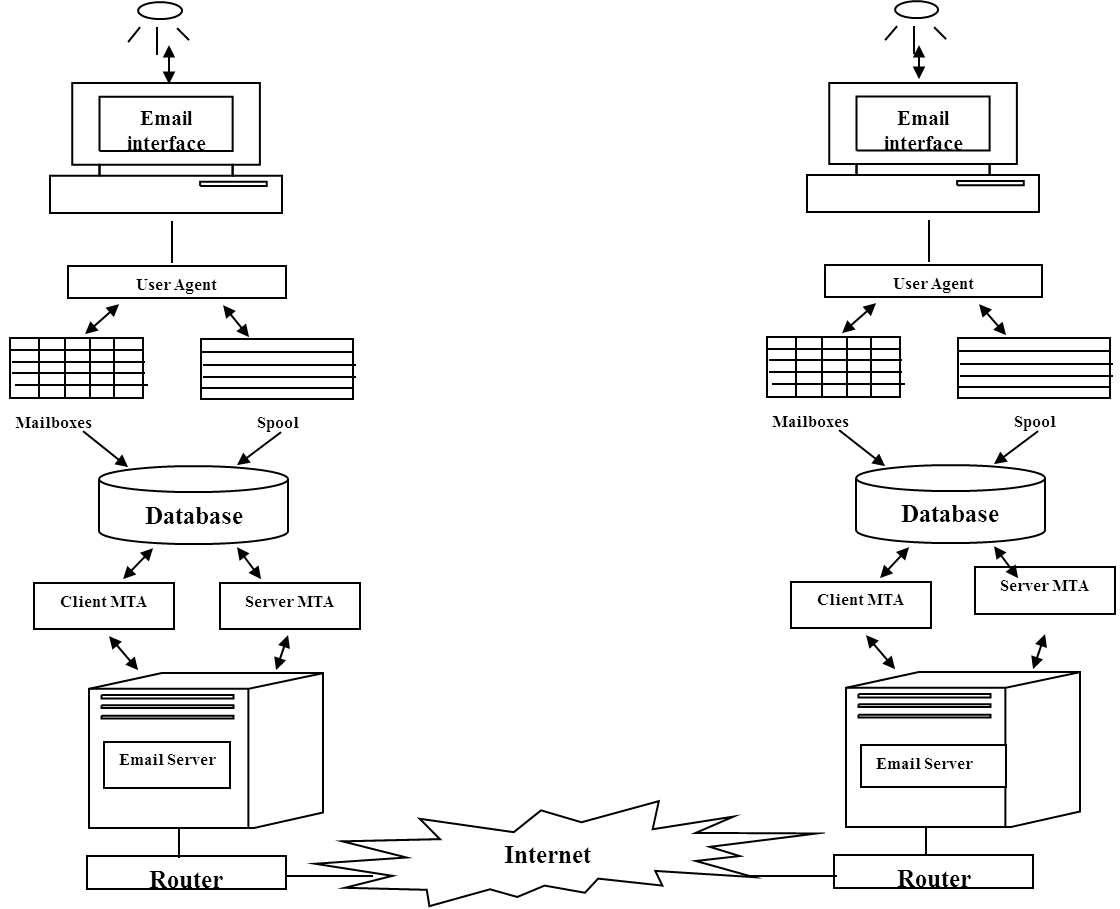
A SPOOL IS A QUEUE OF MESSAGES. THE MESSAGES IN A SPOOL ARE SENT ON A FIRST COME FIRST SEARCHED BASIS. THAT IS, A BACKGROUND PROCESS ON THE EMAIL SERVER PERIODICALLY SEARCHES EVERY MESSAGE IN A SPOOL AUTOMATICALLY AFTER A SPECIFIED TIME INTERVAL, AND AN ATTEMPT IS MADE TO SEND IT TO THE INTENDED RECIPIENT. FOR INSTANCE, THE BACKGROUND PROCESS CAN ATTEMPT TO SEND EVERY MESSAGE IN A SPOOL AFTER EVERY 30 SECONDS

* IF THE MESSAGE CANNOT BE SENT DUE TO ANY REASONS SUCH AS TOO MANY MESSAGES IN THE QUEUE, THE DATE AND TIME WHEN AN ATTEMPT WAS MADE TO SEND IT IS RECORDED. AFTER A SPECIFIED NUMBER OF ATTEMPTS OR TIME INTERVAL, THE MESSAGE IS REMOVED FROM THE SPOOL AND IS RETURNED BACK TO THE ORIGINAL SENDER WITH AN APPROPRIATE ERROR MESSAGE. UNTIL THAT TIME, THE MESSAGE REMAINS IN THE SPOOL. IN OTHER WORDS, A MESSAGE CAN BE CONSIDERED AS DELIVERED SUCCESSFULLY ONLY WHEN BOTH THE CLIENT AND THE SERVER CONCLUDE THAT THE RECIPIENT HAS RECEIVED THE EMAIL MESSAGE CORRECTLY. TILL THAT TIME, COPIES OF THE EMAIL MESSAGE ARE RETAINED IN BOTH THE SENDING SPOOL AND RECEIVING MAILBOX.
* THUS, THE EMAIL SOFTWARE ITSELF IS DIVIDED INTO TWO PARTS: CLIENT PORTION AND SERVER PORTION. THE CLIENT PORTION ALLOWS YOU TO COMPOSE A MESSAGE, AND ALSO DISPLAY A RECEIVED MESSAGE. THE SERVER PORTION ESSENTIALLY MANAGES THE MAILBOX TO STORE THE MESSAGES TEMPORARILY AND DELIVER THEM WHEN DIRECTED.
* EACH ELECTRONIC MAILBOX ON THE SERVER HAS A UNIQUE EMAIL ADDRESS. THIS CONSISTS OF TWO PARTS – THE NAME OF THE USER AND THE NAME OF THE DOMAIN. THE @ SYMBOL JOINS THEM TO FORM THE EMAIL ADDRESS AS SHOWN BELOW
* USERNAME@DOMAIN NAME

[SDSGOA@GMAIL.COM](mailto:SDSGOA@GMAIL.COM)

GOOGLE ,HOTMAIL,YAHOO,REDIFF ARE SOME POPULAR NETWORKS WITH MANY EMAIL SUBSCRIBERS

**EMAIL COMPONENTS AND ARCHITECTURE**



* **The user agent** is the user interface client email software (such as Microsoft OutlookExpress, Lotus Notes, Netscape Mail, etc.) that provides the user facilitates for reading an email message by retrieving it from the server, composing an email message in a Word-processor like format, etc.
* Mailbox There is one mailbox per user, which acts as the email storage system for that user.
* Spool. It allows storing of email messages sent by the user until they can be sent to the intended recipient.
* Mail transfer agent The mail transfer agent is the interface between the email system and the local email server.

**SIMPLE MAIL TRANSFER PROTOCOL SMTP**

* SMTP USES WELL KNOWN PORT 25
* CONSISTS OF USER AGENT(UA) AND MAIL TRANSFER AGENT(MTA)
* SMTP PERFORMS TWO TRANSFERS:

A) FROM THE SENDERS COMPUTER TO THE SENDERS SMTP SERVER B)FROM THE SENDERS SMTP SERVER TO THE RECEIVERS SMTP SERVER.

THE SECOND TRANSFER IS DONE EITHER BY POST OFFICE PROTOCOL(POP)

OR INTERNET MAIL ACCESS PROTOCOL(IMAP)

SMTP IS ASYNCHRONOUS i.e IT ALLOWS DELAYED DELIVERY.

DELAY CAN HAPPEN AT EITHER END.(RECEIVER OR SENDER)

**STAGE 1:: A user Y sends an email for another user X. This email travels from the SMTP client of Y via the Internet to the SMTP server of X (*described later)*. The SMTP server at the ISP of user X receives and stores this email in the user’s mailbox.**

**Stage 2: When the user X connects to the Internet the next time, its POP client inquires with the POP server of his ISP for any new email messages. The POP server of the ISP sends the new email for X (which was sent by user Y) in response.**

SMTP COMMANDS AND RESPONSES

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **COMMAND** | | **EXPLANATION** | | |
| HELLO | | CLIENT IDENTIFIES SERVER USING CLIENT’S DOMAIN NAME | | |
| MAIL FROM | | CLIENT IDENTIFIES ITS EMAIL ADDRESS TO THE SERVER | | |
| RCPT TO | | CLIENT IDENTIFIES THE INTENDED RECEPIENTS EMAIL ADDRESS | | |
| **RESPONSE** | | **EXPLANATION** |
| 2yz | | Positive completion reply |
| 3yz | | Positive intermediate reply |
| 4yz | | Transient negative reply |
| 5yz | | Permamant negative completion reply |

* SMTP PHASES  
  SMTP MAIL TRANSFER HAPPENS IN 3 PHASES
* PHASE 1 : CONNECTION ESTABLISHMENT
* PHASE 2 : MESSAGE TRANSFER
* PHASE 3 : CONNECTION TERMINATION
* **PHASE 1**

1. CLIENT MAKES ACTIVE TCP CONNECTION WITH THE SERVER ON WELL KNOWN POR
2. SERVER SENDS CODE 220(SERVICE READY ELSE 421(SERVICE NOT AVAILABLE)
3. CLIENT SENDS HELLO MESSAGE TO IDENTIFY ITSELF USING ITS DOMAIN NAME
4. SERVER RESPONDS WITH CODE 250(REQUEST COMAND COMPLETED) OR AN ERROR

**PHASE 2**

THIS PHASE IS THE MOST IMPORTANT ONE AS IT ACTUALLY INVOLVES THE TRANSFER OF EMAIL CONTENTS FROM THE SENDER TO THE RECEIVER. FOLLOWING ARE THE STEPS:

1.CLIENT SENDS MAIL MESSAGE ,IDENTIFYING THE SENDER.

2. SERVER RESPONDS WITH 250(OK)

3. CLIENT SENDS RCPT MESSAGE TO IDENTIFY THE RECEIVER

4.SERVER RESPONDS WITH 250(OK)

5.CLIENT SENDS DATA TO INDICATE START OF MESSAGE TRANSFER.

6.SERVER RESPONDS WITH 354(START MAIL INPUT)

7.CLIENT SENDS EMAIL HEADER AND BODY IN CONSECUTIVE LINES

8.THE MESSAGE IS TERMINATED WITH A LINE CONTAINING JUST A PERIOD.

9. THE SERVER RESPONDS WITH 250 (OK)

**PHASE 3**

* 1. CLIENT SENDS QUIT MESSAGE
* SERVER RESPONDS WITH 221(SERVICE CLOSED)
* TCP CONNECTION IS CLOSED

**EMAIL ACCESS AND RETREIVAL**

* THERE ARE THREE PRIMARY EMAIL ACCESS MODELS
* 1. ONLINE ACCESS MODEL: THIS IS THE MOST IDEAL BUT NOT PRACTICAL APPROACH. EVERY USER NEEDS TO BE CONNECTED TO THE INTERNET AND HENCE TO THE MAILBOX MANAGED BY THE SMTP SERVER AT ALL TIMES. CLEARLY THIS IS NOT POSSIBLE
* 2. OFFLINE ACCESS MODEL: HERE THE USER CONNECTS TO THE MAILBOX FROM A REMOTE CLIENT COMPUTER,DOWNLOADS EMAILS TO THE CLIENT COMPUTER AND DISCONNECTS FROM THE MAILBOX. ONCE THIS HAPPENS EMAILS ARE DELETED FROM THE SERVER MAILBOX.
* 3.DISCONNECTED ACCESS MODEL: THIS IS A MIXED APPROACH. HERE THE USER CAN DOWNLOAD EMAILS TO THE CLIENT COMPUTER BUT THEY ARE RETAINED ON THE SERVER. SYNCHRONIZATION BETWEEN CLIENT AND SERVER EMAIL STATES IS POSSIBLE(i.e MARKS EMAILS AS READ/UNREAD ETC)
* THE TWO MAIN EMAIL ACCESS AND RETRIEVAL PROTOCOLS ARE
* POST OFFICE PROTOCOLS (POP) AND INTERNET MAIL ACCESS PROTOCOL(IMAP)4

**POST OFFICE PROTOCOL POP**

The Post Office Protocol (POP) allows a user to retrieve the incoming

mails from HIS/HER email server. POP (like IMAP) works only at the receiver’s end, and has no role to play at the sender’s side.

POP has two parts, a client POP (i.e., the receiver’s POP) and a server POP (which uses the receiver’s email server). The client (i.e., the receiver) opens a TCP connection with the receiver’s POP server on wellknown port 110. The client user name and password to access the mailbox are sent along with it. Provided these are correct, the receiver user can list and receive emails from the mailbox. POP supports delete mode (i.e., delete emails from the mailbox on the email server once they are downloaded to the receiver’s computer) and keep mode (i.e., keep emails in the mailbox on the email server even after they are downloaded to the receiver’s computer). The default option is delete.

POP uses TCP. The server listens to well-known port 110. Client sends commands

to server, and server responds with replies and/or email contents and deletes emails from server. POP commands are 3-4 letters long and are case-insensitive. They are actually plain ASCII text, terminated with a CR-LF pair. Server replies are simple: either +OK or –ERR.

A POP session between a client and a server has three states, as given below.

Authorization state Here, the server does a passive open and the client authenticates itself.

Transaction state Here, the client is allowed to perform mailbox operations (view/retrieve/delete/...

mails).

Update state Here, the server deletes messages marked for deletion, session is closed, and TCP

connection is terminated.

 " POP is very popular but is offline (mail is retrieved from the server and deleted from there). POP was made disconnected to achieve this functionality (i.e., retrieve mail on to the client computer, but do not delete from the server; synchronize changes, if any). This is not always desired. Hence, a different email access and retrieval protocol is necessary. That protocol is Internet Mail Access Protocol (IMAP).

**INTERNET MAIL ACCESS PROTOCOL IMAP**

* IMAP is more powerful and also more complex than POP.
* It allows folder creation on the server, reading the mail before retrieval, search for email contents on the server, etc. Here, work is focused on email server, rather than downloading emails on the client before doing anything else (unlike what happens in the case of POP).
* In this protocol, the server does a passive open on well-known port number 143. TCP three-way handshake happens and client and server can use IMAP over a new session that gets created. There are four possible IMAP session states.
* 1. Not Authenticated State 3. Selected State
* 2. Authenticated State 4. Logout State
* 1. Not authenticated state Session normally begins in this state after a TCP connection is established.
* 2. Authenticated state Client completes authentication. Client is now allowed to perform mailbox operations. Client selects a mailbox to work with.
* 3. Selected state Client can access/manipulate individual messages in the mailbox. Thereafter, client can close the mailbox and return to the Authenticated State to work with another mailbox, or log out of the IMAP session.
* 4. Logout state Client can explicitly log out by sending a Logout command, or session can also expire because of timeout. Server sends a response and connection is terminated.
* AFTER PROCESSING A CLIENT COMMAND THE SERVER CAN SEND BACK EITHER A RESULT OR A RESPONSE

**MULTIPURPOSE INTERNET MAIL EXTENSIONS MIME**

IN CLIENT SERVER COMMUNICATION, THE DATA IS SENT IN THE FORM OF BYTES

THE WEB BROWSER RECEIVES BYTES FROM THE SERVER AND ARRANGES THIS DATA IN THE PROPER ORDER. HOW DOES A WEB BROWSER UNDERESTAND IF THE DATA IS NORMAL TXT,IMAGE OR VIDEO?

MIME HELPS IN THIS.

MIME IS A SPECIFICATION FOR NON ASCII MESSAGES SO THAT THEY CAN BE SENT OVER THE INTERNET.MANY EMAIL CLIENTS NOW SUPPORT MIME WHICH ENABLE THEM TO SEND AND RECEIVE GRAPHICS ,AUDIO AND VIDEO FILES OVER THE INETRNET MAIL SYSTEM.MIME ALSO SUPPORTS MESSAGES IN CHARACTER SETS OTHER THAN ASCII.

IN ADDITION TO EMAIL APPLICATIONS ,WEB BROWSERS ALSO SUPPORT VARIOUS MIME TYPES.THIS ENABLES THE BROWSER TO DISPLAY FILES THAT ARE NOT IN HTML FORMAT.

DURING A TRANSACTION BETWEEN A WEB SERVER AND A BROWSER THE FIRST THING THE WEB SERVER DOES IS SEND THE MIME TYPE OF THE FILE TO THE BROWSER SO THAT THE BROWSER KNOWS HOW TO DISPLAY THE DOCUMENT.

A NEW VERSION CALLED S/MIME SUPPORTS ENCRYPTED MESSAGES.

**MIME SPECIFICATIONS**

* A MIME SPECIFICATION HAS THE FOLLOWING FORM
* type/subtype
* For example the MIME TYPE FOR MICROSOFT WORD FILE IS application AND SUB TYPE IS msword. TOGETHER THE COMPLETE MIME TYPE is application/msword
* A GIF IMAGE WILL HAVE MIME TYPE AS image/gif
* A list of MIME specifications is stored in the configuration file of every web server.

**EMAIL PRIVACY**

When one person sends an email to another, the email message can

potentially travel through a number of intermediate routers and

networks before it reaches the recipient. Consequently, there is a concern among email users about its privacy. What if the email message gets trapped on its way and is read by an unintended recipient? To resolve this issue, the **Pretty Good Privacy (PGP)** is widely used. A slightly older protocol called as **Privacy Enhanced Mail (PEM)** also exists.

* Phil Zimmerman is the creator of the **Pretty Good Privacy (PGP)** protocol.

He is credited with the creation of PGP. The most significant aspects of PGP are that it supports the basic requirements of cryptography, is quite simple to use, and is completely free, including its source code and documentation. Moreover, for those organizations that require support, a low-cost commercial version of PGP is available from an organization called as Viacrypt (now Network Associates). PGP has become extremely popular and is far more widely used, as compared to PEM.

**PGP**

* THE SECURITY FEATURES OFFERED BY PGP INCLUDE:
* 1.ENCRYPTION 2.NON REPUDIATION 3.MESSAGE INTEGRITY.
* THE 5 STEPS FOLLOWED IN PGP OPERATIONS ARE:
* 1.DIGITAL SIGNATURE 2.COMPRESSION 3.ENCRYPTION
* 4.ENVELOPING 5.BASE 64 ENCODING.
* PGP ALLOWS FOR 3 SECURITY OPTIONS WHEN SENDING A EMAIL MESSAGE
* 1.SIGNATURE ONLY(STEPS 1 AND 2)
* 2. SIGNATURE AND BASE 64 ENCODING(STEPS 1,2 & 5)
* 3. STEPS 1 TO 5
* PGP ALSO INTRODUCES THE CONCEPT OF KEY RINGS WHEN A MESSAGE HAS TO BE SENT TO MULTIPLE RECEPIENTS. i.e PGP SPECIFIES A SET OF PUBLIC AND PRIVATE KEYS.