SATHYABAMA
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Accredited "A" Grade by NAAC | 12B Status by UGC | Approved by AICTE
www.sathyabama.ac.in

SCHOOL OF COMPUTING
DEPARTMENT OF INFORMATION TECHNOLOGY

UNIT – V – Data communication and Computer networks – SCS1314

APPLICATION LAYER

Networking Devices - Repeaters - Switches - Bridges - Routers - Gateways- Domain Name System - FTP - WWW and HTTP - SNMP - SMTP - POP3 - IMAP - MIME.

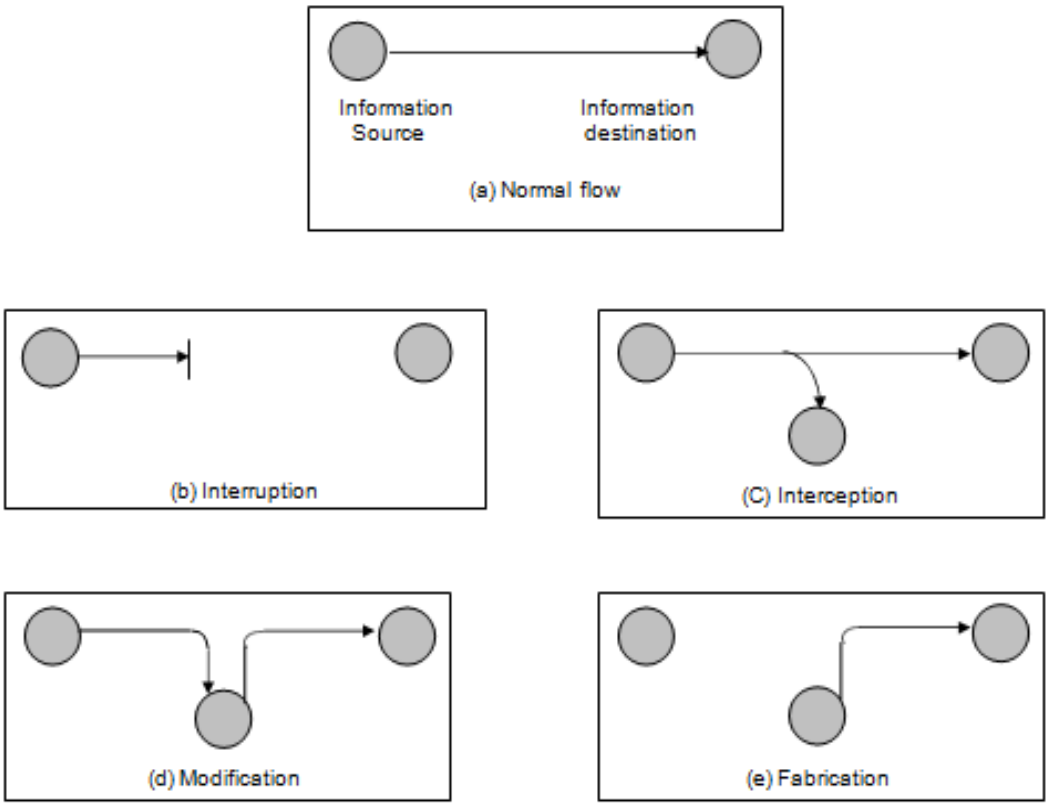
Network Security

Security Attacks

Attacks on the security of a computer system or network are best characterized by viewing the function of the computer system as providing information.

There are four general categories of attack:

- **Interruption:** An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability. Examples include destruction of a piece of hardware, such as a hard disk, the cutting of a communication line, or the disabling of the file management system.
- **Interception:** An unauthorized party gains access to an asset. This is an attack on confidentiality. The unauthorized party could be a person, a program, or a computer. Examples include wiretapping to capture data in a network, and the illicit copying of files or programs.
- **Modification:** An unauthorized party not only gains access to but tampers with an asset. This is an attack or integrity. Examples include changing values in a data file, altering a program so that it performs differently, and modifying the content of messages being transmitted in a network.
- **Fabrication:** An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. Examples include the insertion of spurious messages in a network or the addition of records to a file.



CONVENTIONAL ENCRYPTION MODEL

The original intelligible message, referred to as plaintext, is converted into apparently random nonsense, referred to as ciphertext. The encryption process consists of an algorithm and a key. The key is a value independent of the plaintext. The algorithm will produce a different output depending on the specific key being used at he time. Changing the key changes the output of the algorithm.

Once the ciphertext is produced, it may be transmitted. Upon reception, the ciphertext can be transformed back to the original plaintext by using a decryption algorithm and the same key that was used for encryption.

The security of conventional encryption depends on the secrecy of the key, not the secrecy of the algorithm. We do not need to keep the algorithm secret; we need to keep only the key secret. A source produces a message in plaintext, $X = [X_1, X_2, \ldots\ldots, X_M]$. For encryption, a key of the form $K = [K_1, K_2, , K_J]$ is generated. If the key is generated at the message source,

then it must also be provided to the destination by means of some secure channel. Alternatively, a third party could generate the key and securely deliver it to both source and destination.

With the message X and the encryption key K as input, the encryption algorithm forms the ciphertext Y = [$Y_1, Y_2, \ldots\ldots, Y_N$]. We can write this as

$$Y = E_K(X)$$

This notation indicates that Y is produced by using encryption algorithm E as a function of the plaintext X, with the specific function determined by the value of the key K.

The intended receiver, in possession of the key, is able to invert the transformation:

$$X = D_K(Y)$$

Substitution Techniques

A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns.

Caesar Cipher

The earliest known use of a substitution cipher, and the simplest, was by Julius Caesar. The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places further down the alphabet. For example,

plain : meet me after the toga party

cipher : PHHW PH DIWHU WKH WRJD SDUWB

Note that the alphabet is wrapped around, so that the letter following Z is A. We can define the transformation by listing all possibilities, as follows:

plain: a b c d e f g I j k l m n o p q r s t u v w x y z

cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

If we assign a numerical equivalent to each letter (a =1, b = 2, etc.), then the algorithm can be expressed as follows. For each plaintext letter p, substitute the ciphertext letter C:

$$C = E(p) = (p + 3) \bmod (26)$$

A shift may be of any amount, so that the general Caesar algorithm is C =

$$E(p) = (p + k) \bmod (26)$$

Where k takes on a value in the range 1 to 25. The decryption algorithm is simply P =

$$D(c) = (C - k) \bmod (26)$$

Playfair Cipher

The bet-known multiple-letter encryption cipher is the Playfair, which treats digrams in the plaintext as single units and translates these units into ciphertext digrams.

The Playfair algorithm is based on the use of a 5 X 5 matrix of letters constructed using a keyword. Here is an example, solved by Lord Peter Wimsey in Dorothy Sayers's Have His carcase.

M	**O**	**N**	**A**	**R**
C	**H**	**Y**	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

In this case, the keyword is monarchy. The matrix is constructed by filling in the letters of the keyword from left to right and from top to bottom, and then filling in the remainder of the matrix with the remaining letters in alphabetic order. The letters I and J count as one letter. Plaintext is encrypted two letters at a time, according to the following rules:

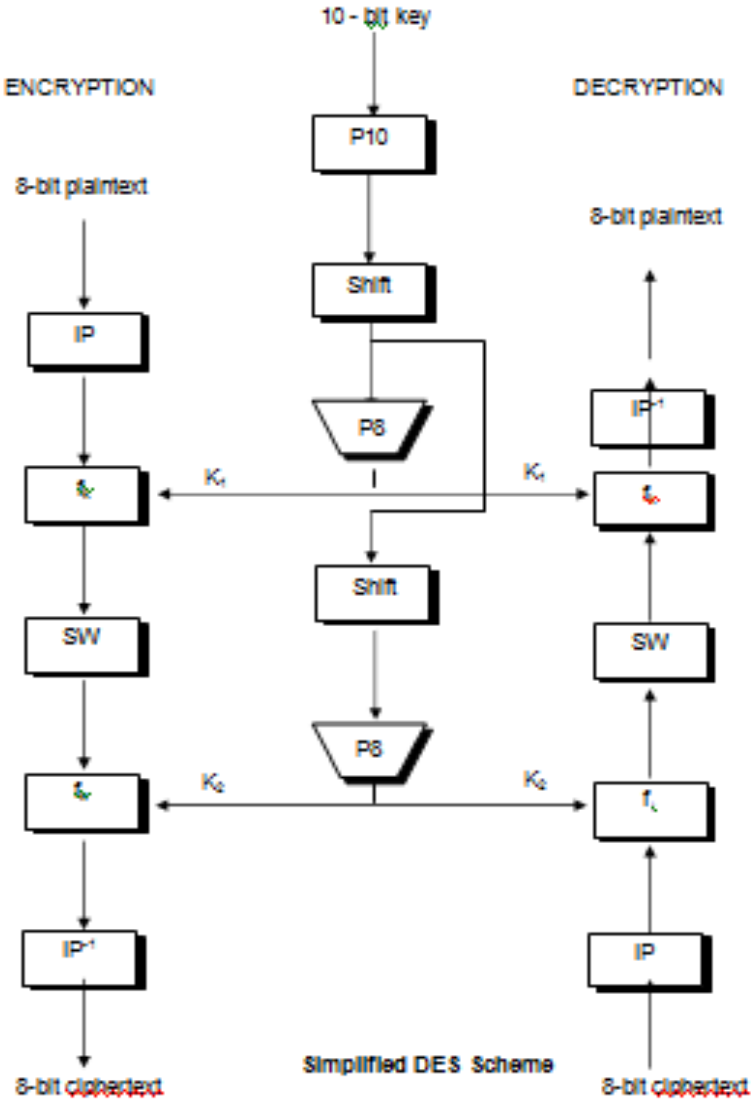
1. Repeating plaintext letters that would fall in the same pair are separated with a filler letter, such as x, so that balloon would be enciphered as ba lx lo on.
2. Plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the row circularly following the last. For example, mu is encrypted as CM.
3. Otherwise, each plaintext letter is replaced by the letter that lies in its own row and the column occupied by the other plaintext letter. Thus, hs becomes BP and ea becomes IM (or JM, as the encipherer wishes).

Simplified DES

The S-DES decryption algorithm takes an 8-bit block of plaintext (example: 10111101) and a 10- bit key as input and produces an 8-bit block of ciphertext as output. The S-DES decryption algorithm takes an 8-bit block of ciphertext and the same 10-bit key used to produce that ciphertext as input and produces the original 8-bit block of plaintext.

The encryption algorithm involves five functions: an initial permutation (IP); a complex function labeled f_k, which involves both permutation substitution operations and depends on a key input; a simple permutation function that switches (SW) the two halves of the data; the function f_k again, and finally a permutation function that is the inverse of the initial permutation (IP^{-1}).

The function f_k takes as input not only the data passing through the encryption algorithm, but also an 8-bit key. The algorithm could have been designed work with a 16-bit key, consisting of two 8-bit subkeys, one used for each occurrence of f_k. Alternatively, a single 8-bit key could have been used, with the same key used twice in the algorithm. A compromise is to use a 10-bit key from which two 8-bit subkeys are generated, as depicted in fig. In this case, the key is first subjected to a permutation (P10). Then a shift operation is performed. The output of the shift operation then passes through a permutation function that produces an 8-bit output (P8) for the first subkey (K_1). The output of the shift operation also feeds into another shift and another instance of P8 to produce the second subkey (K_2).



Simplified DES Scheme

We can concisely express the encryption algorithm as a composition of functions:

$IP^{-1} \circ f_{k2} \circ SW \circ f_{k1} \circ IP$

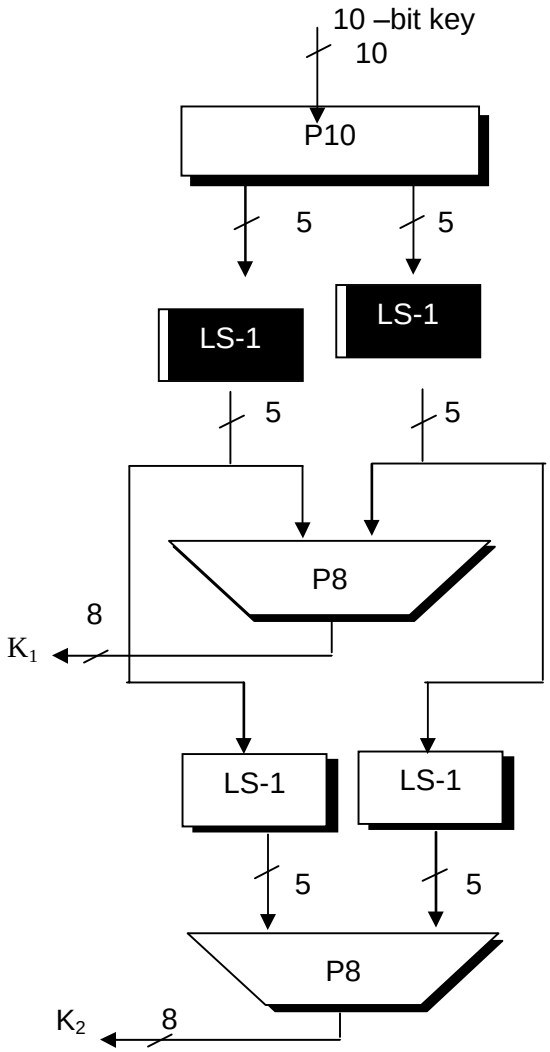
Which can also be written as

$ciphertext = IP^{-1}(f_k (SW (f_k (IP (plaintext)))))$

Where

$K_1 = P8 (Shift (P10 (key)))$

$K_2 = P8 (Shift (Shift (P10 (key))))$



Key Generation for Simplified DES

Decryption is also shown in fig. and is essentially the reverse encryption:

$plaintext = IP^{-1} (f_{k1} (SW (f_{k2} (IP (ciphertext)))))$ We now examine the elements of S-DES in more detail.

S-DES Key Generation

S-DES depends on the use of a 10-bit key shared between sender and receiver. From this key, two 8-bit subkeys are produced for use in particular stages of the encryption and decryption algorithm. Figure depicts the stages followed to produce the subkeys.

First, permute the key in the following fashion. Let the 10-bit key be designated as (k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10}). Then the permutation P10 is defined as P10 (k_1, k_2, k_3, k_4, k_5, k_6, k_7, k_8, k_9, k_{10}) = (k_3, k_5, k_2, k_7, k_4, k_{10}, k_1, k_9, k_8, k_6)

P10 can be concisely defined by the display:

P10									
3	5	2	7	4	10	1	9	8	6

This table is read from left to right; each position in the table gives the identity of the input bit that produces the output bit in that position. So the first output bit is bit 3 of the input; the second output bit is bit 5 of the input, and so on. For example, the key (1010000010) is permuted to (1000001100). Next, perform a circular left shift (LS-1), or rotation, separately on the first five bits and the second five bits. In our example, the result is (00001 11000).

Next we apply P8, which picks out and permutes 8 of the 10 bits according to the following rule:

P8							
6	3	7	4	8	5	10	9

The result is subkey 1 (K_1). In our example, this yields (10100100).

We then go back to the pair of 5-bit strings produced by the two LS-1 functions and perform a circular left shift of 2 bit positions on each string. In our example, the value (00001 11000) becomes (00100 00011). Finally, P8 is applied again to produce K_2. In our example, the result is (01000011).

The RSA Algorithm

Description of the Algorithm

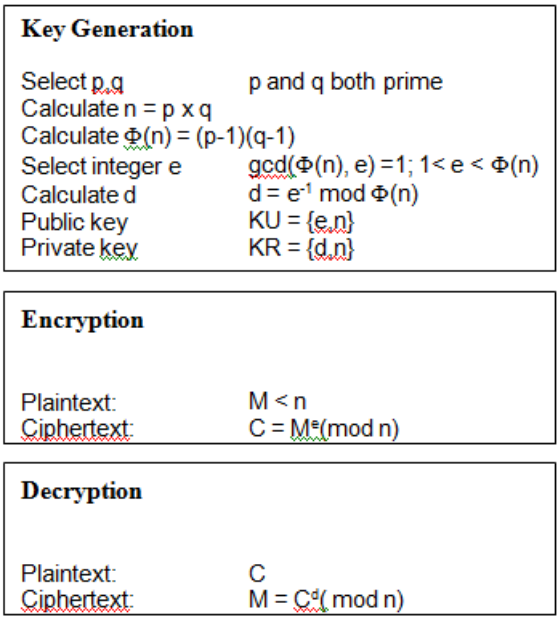
The scheme developed by Rivest, Shamir, and Adleman makes use of an expression with exponentials. Plaintext is encrypted in blocks, with each block having a binary value less than some number n. That is, the block size must be less than or equal to $\log_2(n)$; in practice, the block size is 2^k bits, where $2^k < n \leq 2^{k+1}$. Encryption and decryption are of the following form, for some plaintext block M and ciphertext block C:

$C = M^e \bmod n$

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Both sender and receiver must know the value of n. The sender knows the value of e, and only the receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of KU = {e, n} and a private key of KR = {d, n}. For this algorithm to be satisfactory for public – key encryption, the following requirements must be met:

1. It is possible to find values of e, d, n such that $M^{ed} = M \bmod n$ for all $M < n$.
2. It is relatively easy to calculate M^e and C^d for all values of $M < n$.
3. It is infeasible to determine d given e and n. 4.



The RSA Algorithm (a)

Fig (a) summarizes the RSA algorithm.

Example 1:

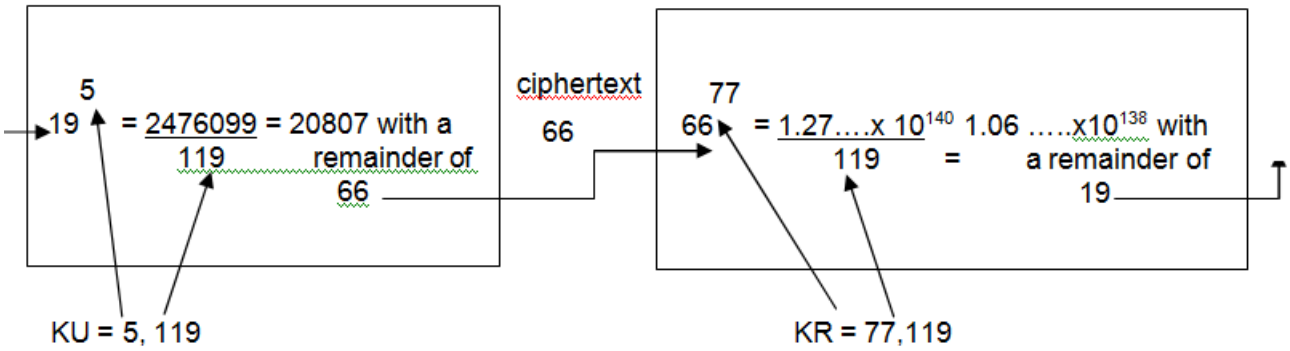
Select two prime numbers, p=7 and q = 17.

1. Calculate n = pq = 7 X 17 = 119 2.

   Calculate □(n) = (p-1) (q-1) = 96

3. Select e such that e is relatively prime to □(n) = 96 and less than □(n); in this case, e =5.
4. Determine d such that de = 1 mod 96 and d < 96. The correct value is d = 77, because 77 X 5 = 385 = 4 X 96 +1.

The resulting keys are public key KU = {5,119} and private key KR = { 77,119}. The example shows the use of these keys for a plaintext input of M = 19. For



Example of RSA algorithm (b)

Encryption, 19 is raised to the fifth power, yielding 2476099. Upon division by 119, the remainder is determined to be 66. Hence $19^5 \equiv 66 \bmod 119$, and the ciphertext is 66. For decryption, it is determined that $66^{77} \equiv 19 \bmod 119$.

Example 2 :

p = 3, q = 11, d = 17

assume plaintext symbol M = 5

n = p*q = 33, z = = (3-1) (11 – 1) = 20

Find e such that e * d = 1 mod z (z+1)
[$d = e^{-1} \bmod z$] k * z+1 (k =1 here)

e = 3 3 X 7 = 1 mod 20

public key = { e,n} = { 3, 33}

private key = { d, n} = { 7, 33}

Encryption M =5

$C = M^e \bmod n$

$= 5^e \bmod 33 = 125 /33 = 3$

with reminder 26

ciphertext = 26

decryption c = 26

$p = M = C^d \bmod n = 26^7 \bmod 33$

= 8031810176/33 = 243388187

with reminder 5

plain text = 5

Example 3:

P = 17, q = 31, e = 7, m = 2

N = 17 X 31 = 527

z = (17-1) (31 – 1) = 16 x 30 = 480

e =7

Finding d such that e * d = 1 mod 480

and d < 480 = k * z + i

e = 7

the value obtained is 343 1/7 x (480 x k +1)

publickey = { 7, 527} private key = { 343, 527 }

ciphertext = $2^7 \bmod 527$

= 128 mod 527 = 0

∴ with reminder = 128

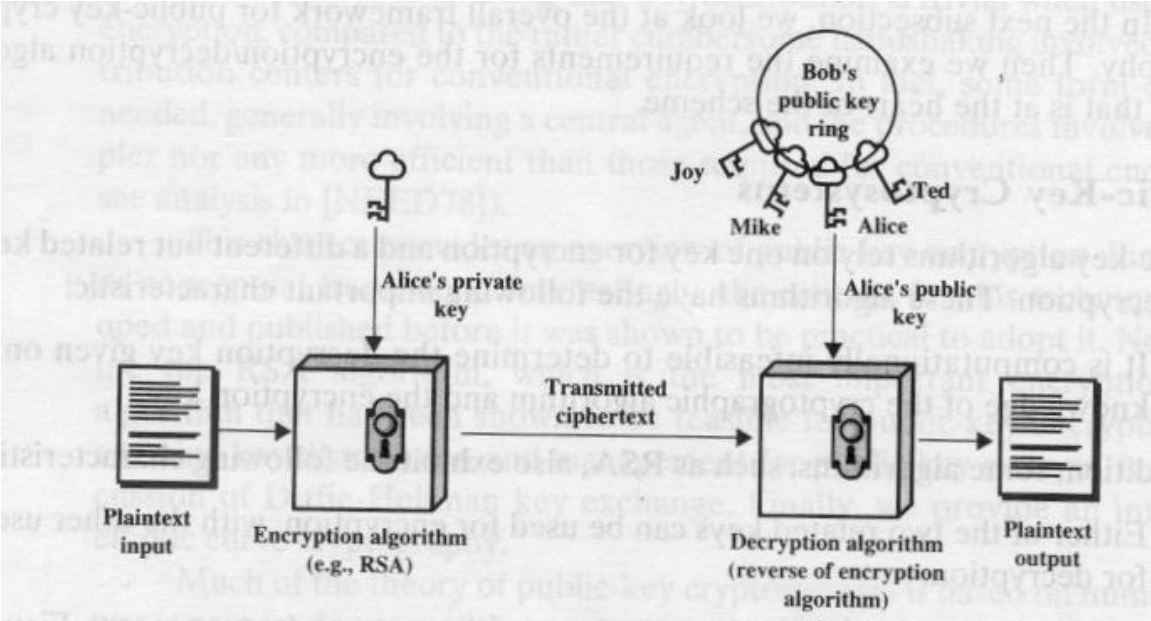
ciphertext = 128

Decryption

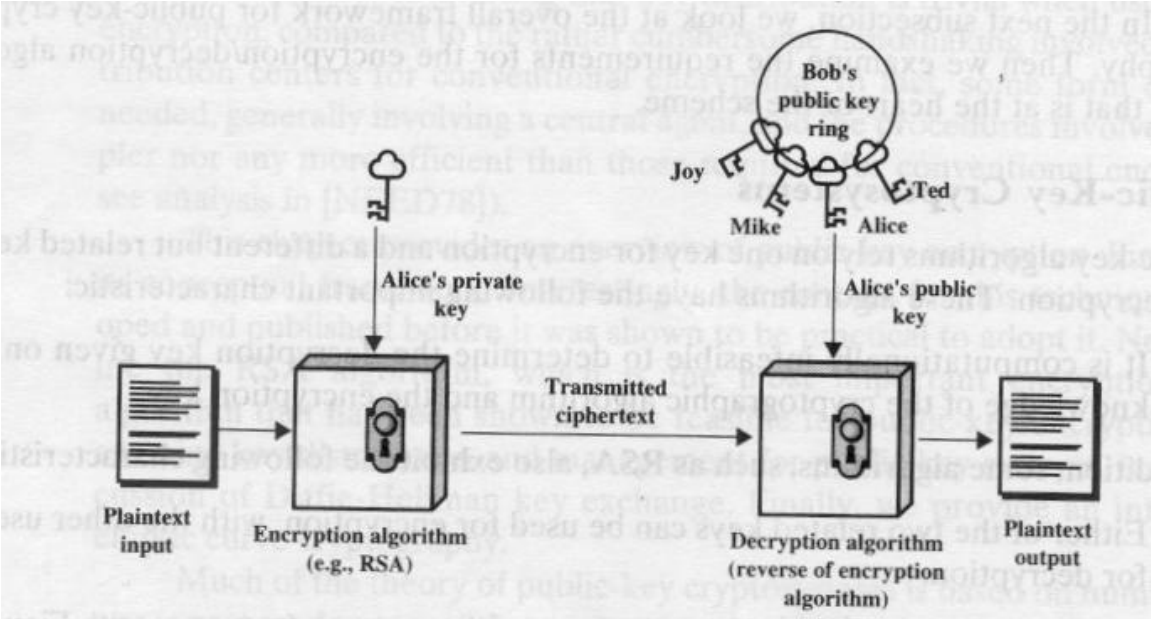
128^{343} mod 527

2 is reminder

∴ plaintext =2



(a) Encryption



(b) Authentication

Public – Key Encryption

Conventional Encryption

Needed to work:

1. The same algorithm with the same key is used for encryption and decryption.

2. The sender and receiver must share the algorithm and the key.

Need for Security:

1. The key must be kept secret.

2. It must be impossible or at least impractical to decipher a message if no other information is available.

3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.

Public-Key Encryption

Needed to work:

1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption.

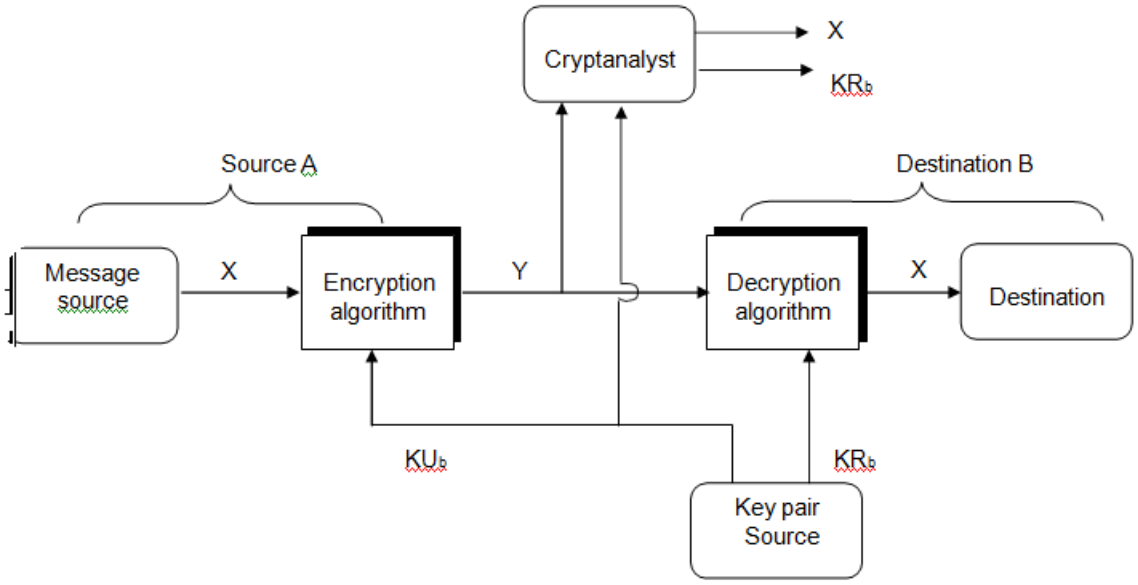
2. The sender and receiver must each have one of the matched pair of keys (not the same one).

Need for Security:

1. One of the two keys must be kept secret.

2. It must be impossible or at least impractical to decipher a message if no other information is available.

3. Knowledge of the algorithm plus one of the keys plus samples of ciphertext must be insufficient to determine the other key.



E-mail :

E-mail system consists of two subsystems

- the user agent, and
- the message transfer agents
- **User Agents :**

  They allow people to read and send e-mail they are local programs that provide a command based, menu based, or graphical method for interacting with e-mail system.

- **Message transfer agents :**

  They are responsible for moving the messages from the source to the destination. They are typically system daemons that run in the background and move e-mail through the system.

Typically, e-mail system support five basic functions given below.

(i) Composition :

It refers to the process of creating messages and answers.

(ii) Transfers :

it refers to moving messages from the originator to the recipient. This requires, establishing a connection to the destination (or) some intermediate machine, outputting the message and releasing the connection.

(iii) Reporting :

It informs the originator about the status of the message, whether it is delivered, rejected(or) lost.

(iv) Displaying :

These provides the incoming messages to be read by the people. Simple conversions and formatting is performed.

(v) Disposition :

It is the final step and concerns what the recipient does with the message after receiving it.

Other Services of E-mail include:

Mailboxes :

Used for storing incoming E-mail.

Mailing List = List of e-mail addresses to whom, identical copies of messages need to be sent.

Registered E-mail = It allows the originator to know that his mail has arrived. High

priority E-mail = Secret E-mail etc.

User Agent :

A user agent is normally a program that accepts a variety of commands for composing, receiving and replying to messages as well as manipulating mail boxes.

Sending E-mail :

To send an e-mail a user must provide the message, the destination address and some other parameters. The message can be produced in any text editor (or) the one built in user agent. The destination address must be in the format that the user agent can deal with i.e., either DNS address (or) X.400 address. Most e-mail systems support mailing list, so that a user can send the same message to a list of people with a single command.

Reading E-mail :

When a user agent is started up, it will look at the user's mailbox for incoming e-mail before displaying anything on the screen. It then announces the number of messages in the mail box(or) a one line summary of each one.

In a sophisticated system the user can specify the fields to be displayed by providing the display format.

Eg:

1. Message numbers
2. Flag etc.

Message format:

Message consist of a primitive envelope, some number of header field, blank line followed by message body. In normal usage, the user agent builds a message and passes it. To the message transfer agent which then uses some of the header fields to construct the actual envelope.

Principal header include:

To :

DNS address of primary recipient.

CC :

DNS address of secondary recipient.

In terms of delivery there is no distinction between primary and secondary (carbon copies).

BCC :

Similar to CC, allows people to send copies to third parties without primary and secondary knowing it.

From :

Who wrote the message.

Sender :

The one who sent the message.

Received :

Added by each message transfers agent along the way used for finding bugs in routing system.

Return path :

Added by final message transfer agent intended to tell how to get back to the sender etc.

Explain how e-mail works?

SMTP :

E-mail is delivered by having the source machine establish a TCP connection to destination. Listening to this port is an E-mail daemon that speaks SMTP. This daemon accepts incoming connections and copies messages from them to appropriate mail boxes. If the message cannot be delivered, an error message is given.

After establishing a TCP connection, the sending machine operates as a client and waits for receiving entity to talk first. The server starts by giving its identity and informing whether (or) not it is prepared to receive mail. If it is not, the client releases the connection.

If the server is ready, the client announces whom the E-mail is coming from and whom it is going to. If the recipient exists, the server gives a go-ahead to send the message. Then the client sends the message and the server acknowledges it. When the E-mail has been exchanged then the connection is released.

E-mail Gateways :

SMTP does not work, when both sender and receiver are not on internet. In order to overcome this difficulty E-mail gateways are used.

Here the sender establishes a TCP connection to the gateway and then uses SMTP to transfer the message. The daemon on the gateway then puts the message in a buffer of messages destined for host2. Late TPU (similar to TCP) is established with host2 and the message is transmitted.

Final Delivery :

Post Office Protocol (POP)

Used to fetch e-mail from a remote mail box, has commands for user to logon, logout, fetch and delete messages. If fetches the mail and stores it in local system.

Interactive mail access protocol (IMAP)

This protocol is used by a person having multiple systems (office, residence, car, etc). Here the E- mail server maintains a central repository that can be accessed from any machine. IMAP does not copy E-mail as POP.

DOMAIN NAME SYSTEM

Generally host names, mailboxes and other resources are represented by using ASCII sting such as rgm@vsnl.net.in.But the network itself only understands binary address i.e., the address written in the binary form. So we need some mechanism to convert the ASCII strings to network addresses in binary. It is easy to maintain the host names and their IP addresses in file for a network of few hundred hosts. For a network of thousand hosts it is very difficult.

The Domain Name System, DNS is a distributes data that is used by TCP/IP application to map between host names and IP addresses, and to provide electronic mail routing information. We use the term

distributed because no single site on the Internet knows all the information. Each site maintains its own data base information and runs a server program that other systems (clients) across the Internet can query. It is a good example of a TCP/IP client-server application.

The DNS provides the protocol that allows client and server to communicate with each other. DNS is defined in RFC's 1034 and 1035.

The DNS identifies each host on the internet with a unique name that identifies it as unambiguously as its IP address as follows. To map a name onto an IP address, an application program calls a library procedure called the resolver, passing it the name as a parameter. The 'resolver' sends a UDP packet to a local DNS server, which then looks up the name and returns the IP address to the resolver, which then returns it to the caller. To create names that are unique and at the same time decentralized and easy to change, the TCP/IP designers have chosen a hierarchical system made up of a number of labels separated by dots.

THE DNS NAME SPACE

Internet is divided it several hundred top level domains, where each domain covers many hosts. Each domain is partitioned into sub domains, these are further partitioned and so on. Thus DNS is implemented using a tree in which each node represents one possible label of up to 63 characters.

The root of the tree is a special node with new label as shown in fig. Any comparison of label considers uppercase and lower-case characters the same i.e., Domain names are case insensitive.

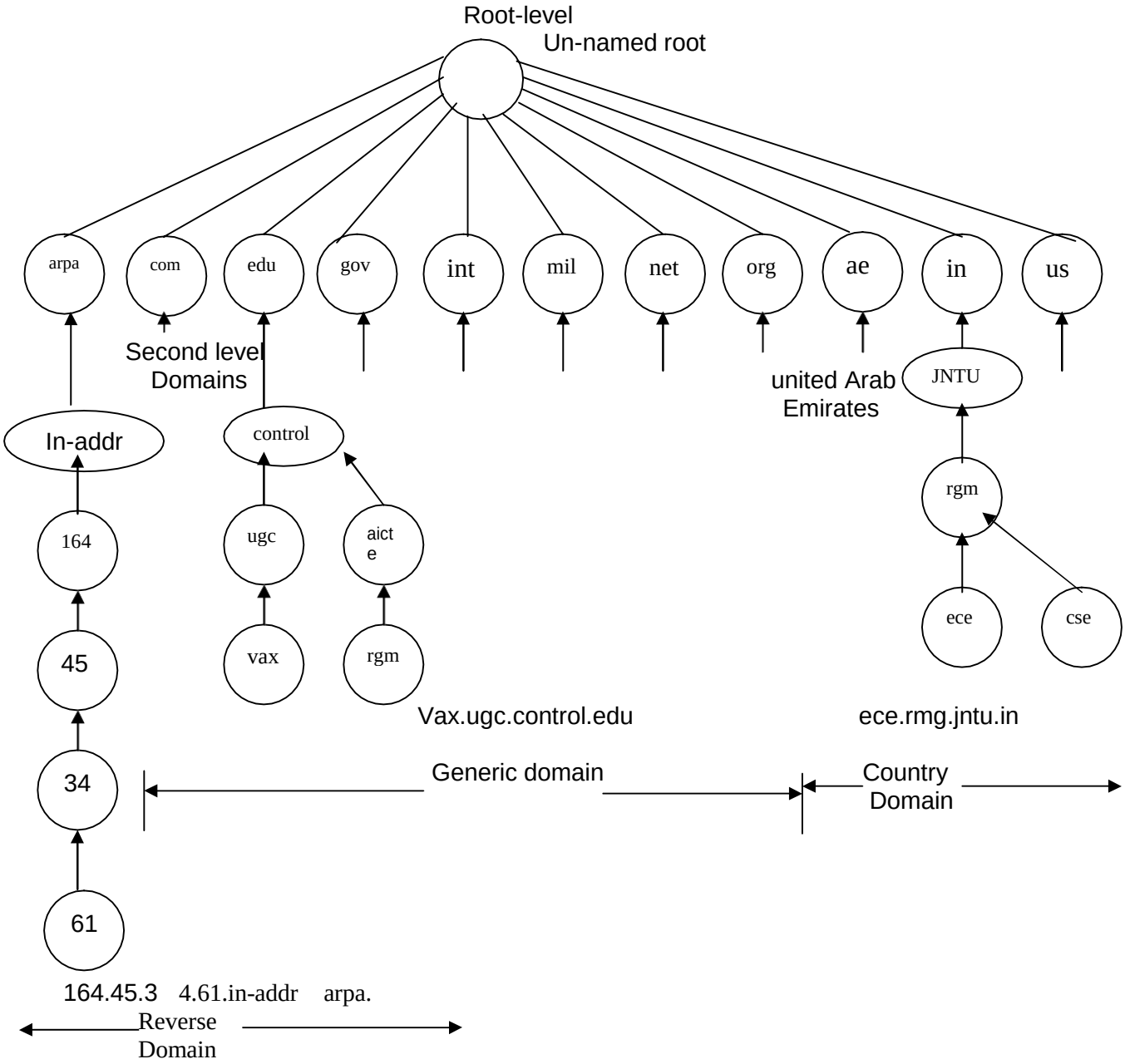
The leaves of the tree represent a company/organization and contain thousands of hosts.

Each domain is named by the path from it to the unnamed root. The components in the name are separated by periods (dots), that is domain name of any node in the tree is the list of labels starting at the node, working up to the root using the period (dot) separate the labels.

The domain names that ends with a period is called an absolute domain name or fully qualified domain name(FQDN).An example is vax.ugc,central.edu.

If domain does not end with a period, it is assumed that the name needs to be completed. How the name is completed on the DNS software being used. If the incomplete names consist of two or more labels, it might be considered to be complete. Otherwise, local addition might be added to the right of the name. The name vax might be completed by adding the local suffix.ugc.central.edu.

The right most label in the name corresponds to the level of the tree closest to the root (lowest), and left-most to the level farthest from the root(highest).The tree is divided into three domains: generic, country and reverse as shown in fig.



DOMAIN NAME SYSTEM

Generic Domain: The generic domain is also called the organization domain, divides registered hosts according to their generic behaviour. Generic domain names, read left to the right , start with the most specific information about the host(e.g. the name of the workstation) and become more and more general with each label until they reach the rightmost label, which describes the broadcast affiliation of the normal host i.e., the nature of the organization.

The first level of the generic domain convention allows seven possible three character labels describing organization type.

1. Com. commercial organization.
2. edu.: educational institution .
3. gov.: government institution.
4. int.: international organization.
5. mil.: military group.
6. net.: Network support center.
7. org. organizations other than listed above.

Each domain name corresponds to a particular IP address. To find the address, the resolution application begins searching with the first level. As a much is found, a pointer leads to the next level and finally to the associated IP address.

Country Domain: The country domain convention follows the same format as generic domain, but uses two character country abbreviation in place of three character organizational abbreviations at the first level shown in table. Second level labels can be organizational or they can be more specific national designations.

Table: SOME DOMAIN NAME SYSTEM COUNTRY CODE

Country Code	Country Name	Country Code	Country Name
AE	Arubeme rates	IN	India
AU	Australia	IT	Italy
BE	Belgium	JP	Japan
CA	Canada	KW	Kuwait
CH	Switzerland	NL	Netherlands
DE	Germany	NO	Norway
DK	Denmark Spain	NZ	Newzeland
ES	Finland	SE	Sweden
FI		US	United States of America
GR	Greece		

Reverse Domain: If we have the IP address and need the domain name, you can reverse domain the functions of DNS.

The domain can be inserted onto the tree in two ways. For example ugc.control.edu could equally be listed under the country domain as cs.yale.ct.us.

To create a new domain, permission is required of the domain in which it will be included. For example, rgm group was started under aicte and is known as rgm.aicte.control.edu. It needs permission from which use manages aicte.control.edu. Naming follows organizational boundaries, not physical networks.

RESOURCE RECORDS

Every domain in the DNS tree maintains a set of Resource Records, which are connected to it. For a leaf node i.e., single host, the most common resource record is its IP address. When a resolver gives a name to DNS, it gets back called as resource records associated with that name.

The original function of a DNS is to map domain names on to the resource records.

A resource record is a five tuple, in ASCII text they are represented as

Domain-name Time-to live type class value.

- The domain-name tells the domain to which this record belongs. This is the primary search key used to satisfy queries.
- The time-to live field gives information regarding the stability of the record. A large value such as 86-400(number of seconds in one day) indicates that the information is highly stable. The small value such as 60(1 minute) indicates that the information is highly volatile.
- The type of field tells what kind of record it is, some of the type records are listed in table 5.3.

S.No	Type	Meaning	Value
1.	SoA	Start of Authority	Parameter for this zone
2.	A	IP address of a host	32 bit integer
3.	Mx	Mail Exchange Name	Priority
4.	NS	Server Canonical	Name of the server for this domain
5.	CNAME	name Pointer	Domain Name
6.	PTR	Text	Alias for an IP address
7.	TXT		Uninterpreted ASCII text

1. The SOA record provides name of the primary source of information about (a) name servers zone (b) e-mail address of its administration (c) various flags and (d) various time outs.
2. The record A, holds a 32 bit IP address of the host. If a host connects two or more networks, each case it has one type of a resource record per network connection.
3. The MX record specifies the name of domain prepared to accept e-mail for the specified domain. It allows the host that is not on the internet to receive e-mail from internet sites.
4. NS record specifies Name server.

5. CNAME record specifies allows the aliases to be created.
6. PTR is a regular DNS data type whose interpretation depends on the context on which it is found.
7. The TXT record allows domains to identify themselves in arbitrary way i.e., it is for user convenience.

- The fourth field in the general structure of resource record is the class. It may be Internet information, used IN and for non-internet information, other codes are used.
- The value field can be number, domain name or an ASCII string.

NAME SERVERS

The Inter network Information center (Inter NIC) manages the top level domain names. The Inter NIC delegates responsibility for assigning names to different organizations. Each organization is responsible for a specific portion of the DNS tree structure. Internet professionals refer to these areas of responsibilities as zones.

Alternatively, the Inter NIC delegates responsibility for assigning names with in a specific zone to specific organizations. Each zone contains some part of the tree and also contains name servers holding the authoritative information about the zone. Each zone contains one primary name server and one or more secondary name servers. Primary name server and one or more secondary name servers. Primary name server gets its information from a file on its disk, the secondary name server and get their information from the primary name server. One or more servers are located outside the zone, for each zone, for reliability. The number of name servers needed in a zone depends on the zone boundaries.

Let us consider an example shown in fig connected with another domain. here a resolver on "ece.rgm.jntu.in" wants to know the IP address of the host "rgm.aicte.control.edu" can be explained in 8 steps.

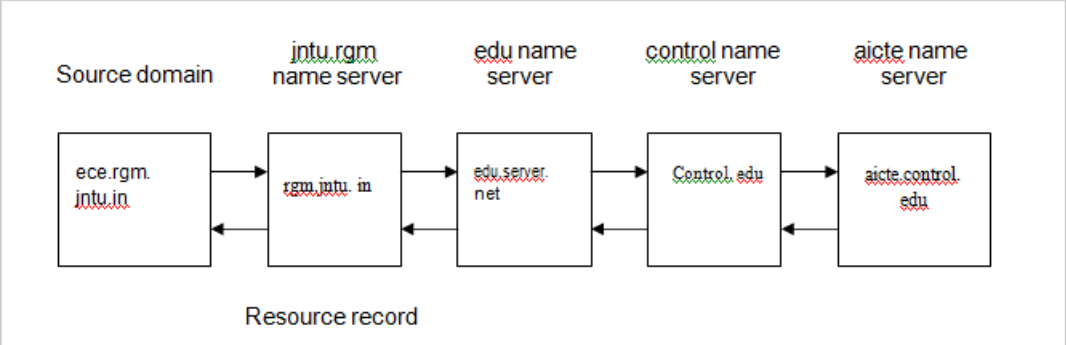
Step 1: It sends a query to the local name server rgm.jntu.in.This query asks a record of type A and the class IN.

Step 2: If the local name server had no such domain and knows nothing about it, it may ask a few other near by name servers if none of them know, it sends a UDP packet to the server for "edu" given in its database (see fig) edu.server.net.

Step 3: It forwards the request to the name server control.edu.

Step 4: And in turn this forwards the request aicte.control.edu, which has authoritative resource records.

This is the request from client to a server, the resource record requested will work its way back in step 5 to step 8.Once these records get back to rgm.jntu.in name server, they will be entered into a cache/memory. However this information is not authoritative, since changes made at aicte.control.edu will not be propagated to all the memories in the world. For this reason cache should not live too long, so time-to-live field is used in each resource record. It tells the name server how long to cache records.



WORKING OF A RESOLVER FOR A DOMAIN IN 8 STEPS

ELECTRONIC MAIL

Electronic mail or E-mail as it is popularly called, is a system that allows a person or a group to electronically communicate with each other through a netork. Presently people can now receive and send e-mail to:

- nearly any country in the world.
- one of millions of computer users.
- many users at once.
- computer programs.

The first e-map systems consisted of file transfer protocols, with the convention that the first line of each message contained the recipient address. Some of the complaints at that time were

1. Sending a message to a group of people was inconvenient.
2. Messages had no internal structure, making computer processing difficult.
3. The sender never knew if a message arrived or not.

4. It is difficult to forward the mails.
5. It is not possible to create and send messages containing a mixer of text, drawing facsimile and voice.

After a decade of competition, email systems based on RFC822 are widely used, where all the above problems are solved.

BASIC FUNCTIONS

Email systems support five basic functions, which are: Composition, Transfer, Reporting, Displaying and Disposition.

1. **Composition** is a process for creating the messages and answers. This can be done by text editor, outside the mailer, the system will provide assistance in addressing and numerous header fields attached to each message. For eample:when answering a message, the e mail system can extract the originator's address from the incoming e-mail and automatically insert it into the address space in reply.
2. **Transfer** refers to moving of messages from the source to the recipent. In some cases, connection establishment is needed with the destination, outputting the message and releasing the connection. The e-mail system should do automatically this.
3. **Reporting** is used to indicate the originator what happened to the message i.e., confirmation of the message delivery. Was it delivers successfully? Was it rejected? Was it lost? Did errors occur?
4. **Displaying** It refers to read the incoming e-mail by the person. Sometimes conversion is required or a special viewer must be invoked.
5. **Disposition** It concerns what the recipient does with the message after receiving it. The possibilities are
    (a) Throwing it away before reading
    (b) Throwing it away after reading.
    (c) Saving it and so on. It is also possible to forward them or process them in other ways.

In addition to these basic services, most of e-mail systems provide a large variety of advanced features such as

(a) It allows to create a mailbox to store incoming e-mail.
(b) It allows to have a mailing list, to which the e-mail messages have to send.
(c) Carbon copies, high priority email, secret email, registered email etc.

THE USER AGENT

The user agent is a program that allows users to read reply to, forward, save and compose messages. User agents for electronic mail are sometimes called mail readers. Some user agents have menu or icon driven interface that requires a mouse, some other requires only 1 character command from keyboard.

Sending e-mail: To send an email message the user must provide

(a) message
(b) destination address and
(c) priority or security levels (options).

- Message can be produced with a free standing text editor, a word processing program or by using a text editor built into the user agents. The format of an e-mail message is similar to that of a conventional letter.

There are two main parts: Header and body.

The header contains out name and address, the name and address of the person it's being sent to, the name and address of the person who is being sent a copy, the date of the message and the subject when we receive an e-mail from someone, the header tells us where it came from, what it is about, how it was sent and when.

The body is the place where we write the contents of what we want to communicate. The message sent should be simple and direct. Body is entirely for human recipient.

- The designation address must be in a format that the user agent can deal with. The basic form of e-mail address is

  User name @host name.subdomain.domain.

The text before the sign @(pronounced "at") specifies the user name of the individual, the text after the @ sign indicates how the computer system can locate that individual's mailboxes.

For example

mvs@cs.colorado.edu

Here cs is a sub domain of Colorado is a sub domain of edu.the edu specifies the top-level domain name.
The number of periods (pronounced as dots) varies from e-mail address.
Reading e-mail: On connecting to the net, the first thing a user usually does is check his mail, it's like checking the mailbox when we go home. The display like fig 5.28 appears on the screen.

Each line refers to one message. In the fig, the mailbox contains 4 (four) messages. The display line contains several fields, which provides user profile.

S.No	Flag	Bytes	Sender	Subject
1.	K	1000	n / p	Got the job
2.	KA	2000	Smer	Request for MP
3.	KF	4000	Vimicro	Repair of controller
4.		1536	hiq	Enquiry of the book

- The first field is the message number.
- The second field is flags, can contain,

  K-means that, message was read previously and kept in mail box. A-means the message has already answered and

  F-message has been forwarded to someone else.
- The third field indicates the length of the message in bytes.
- Fourth field tells who sent the message, this field is simple extracted from the message, so this field contains initials, log in name, first name etc.
- The last field is a 'subject field' gives brief summary of the message.

MESSAGE FORMATS

The e-mail message format was defined in RFC 822.There are two types: ASCII e-mail and multimedia extensions.

ASCII e-mails using RFC 822: The e-mail message consists of a primitive envelope, some number of header fields, a blank like and then message body.

Each header field consists of a single line of ASCII text containing the field name, a colon, and a value of RFC.

The list of header fields related to message transport are

- A recipient's address or "To"
- A sender's address or "From"
- A subject.

The email header may additionally contain.

- **A List of "C_d":** This is a list of e-mail or 'carbon copies' addresses to whom a copy of the message is to be delivered. Multiple e-mail addresses in the "C_c" field are separated by a comma.

- **A List of "B_c":** This is same as "C_c" except that this is a carbon copy. The list of recipients is not visible to the person who receives this message.
- **Attached:** This is a convenient method to share both data and programs. These files may be attached or enclosed with an e-mail message.
- **Signature:** It contains sender's full name and address or whatever information the sender wishes to send.

Instead of creating a message from the scratch, we may choose to reply or forward the messages.

- **Replying:** When we reply a message, the sender's address is automatically put in the "To" header and subject of the original message is reduced proceeded by Re, for the reply.
- **Forwarding:** When we forward a message, the subject of the original message is reused, with prefix "FW".We must specify the e-mail address of the recipient of the forward message.
- **Redirecting:** Some e-mail programs allow to redirect messages. It is similar to forwarding a message, except that the message retains the original sender in the form header and adds a notation that the message comes through you.

Multipurpose Internet Mail Extensions(MIME):

This is the solution defined in 1341 and updated in 1521 for the following problems.

1. Messages in languages with accents.
2. Messages in non Latin alphabets.
3. Messages in languages with out alphabets.
4. Messages not containing text at all.

The basic idea of MIME is to continue the use of RFC 822 format, but to add structure to the message body defined encoding rules for non ASCII formats. The MIME messages can be sent using the existing mail programs, and protocols.

The MIME defines five new message header

- **MIME-Version:** It tells the use agent receiving the message that it is dealing with a MIME message, and which version of MIME it uses.
- **Content-Description:** It tells what is there in the message, this header helps the recipient whether it is worth decoding and reading the message.

- **Content-Transfer Encoding:** It tells how the body is wrapped for transmission through a network that may object to most characters other than letters, numbers and punctuation marks.
- **Content-Type:** It specifies the nature of the message body. Seven types are defined in RFC 1521, each of which has one or more sub types. The type and sub type are separated by a slash. The sub type must be given explicitly in the header, no defaults are provided. Table 5.4 shows the list of types and sub types.

TYPE AND SUB TYPE FIELDS DEFINED IN RFC 1521

S.No	Type	Sub Type	Meaning
1.	Text	Plain HTML Rich text	Unformated text Hyper text mark up language Allows a simple mark up language to included in the text (standardized general ma up language (SGML)
2.	Image	GIF JPEG PNG	To transmit still pictures in GIF format To transmit still pictures in JPEG format To transmit still pictures in portable network graphics
3.	Audio	au Basic aiff	Sun micro systems sound Audiable sound Apple sound
4.	Video	sgi.movie MPEG avi	Silicon graphics movie Visual information, the video format is moving picture experts group MPEG Microsoft audio video interleaved
5.	Application	Octet stream Post Script tex	It is a sequence of uninterrupted bytes Which refers the postscript language produced by Adobe systems and widely used for describing printed pages. TEX document.
6.	Message	RFC822 Partial External	A MIME RFC-822 message (ASCII characters message) Break and encapsulated message up into pieces and send them separately. Used for very long message (i.e., video films)
7.	Multiport	Mixed Alternative Parallel Digest	Each part to be different with no additional structure imposed Each part must contain the same message but expressed in a different medium or encoding. All parts must be viewed simultaneously Many messages are packed together into composite message.

MESSAGE TRANSFER

The message Transfer system, MTS is concerned with relaying messages from originator to the recipent.The simplest way to do this is to establish a transport connection from source machine to the destination machine and just transfer the message.

Mail servers are from the core of the e-mail infrastructure.Each recipient has a mail box, located in one of the mail servers.A typical message starts its journey in the sender's user agent, travels to the sender's main server, and then travels to the recipient mail server where it is deposited in the recipient mail box.

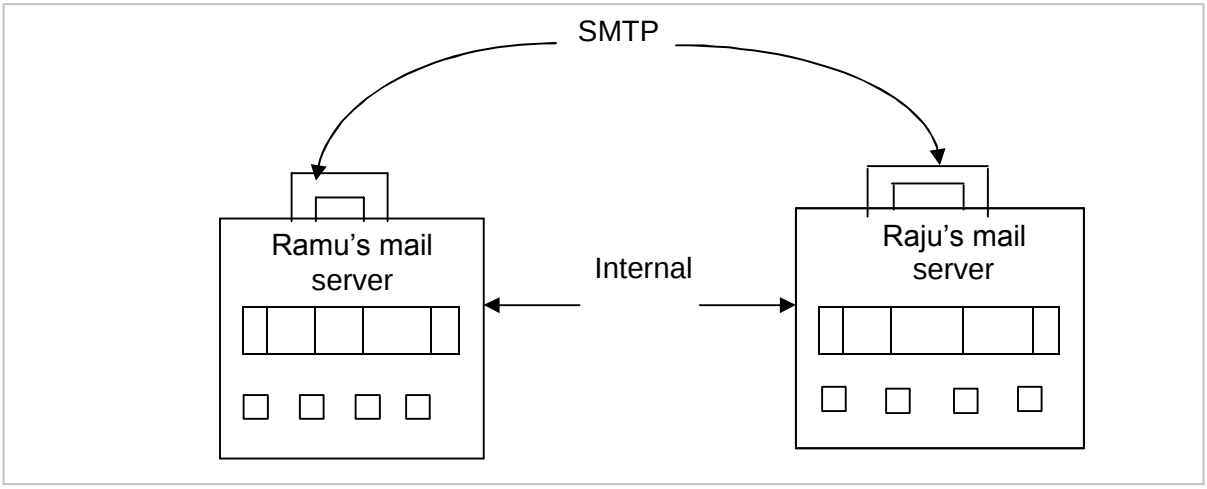
A mail server needs to be running all the time, waiting for e-mail messages and routing them approximately.If a mail server crashes or down for an extended period(3-4 days), e-mail can be lost.There may be a limitation on the size of mail box.Generally once this limit is reached, new incoming messages are refused until you free up space by deleting some messages.

SIMPLE MAIL TRANSFER PROTOCOL-SMTP

The simple mail transfer protocol (SMTP) is the principal application layer protocol for internet e- mail. It is simple ASCII protocol. It uses the reliable data transfer service of TCP to transfer mail from the sender's mail server to the recipient's mail server. In most application protocols SMTP has two sides: a client side, which executes on the sender's mail server and a server side-which executes on the recipient mail server. When a mail server sends a mail (to other mail server), it acts as a client SMTP.When a mail server receives a mail (from other mail server), it acts as an SMTP server.

The SMTP defined in RF821, is at the heart of Internet e-mail.SMTP is much older than HTTP.To illustrate the basic operation of SMTP, let's walkthrough a common scenario. Suppose Ramu wants to send Raju a simple ASCII message.

- Ramu invokes his user agent for e-mail, provides Raju's e-mail address(example Raju@some school.edu) composes a message, and instructs the user agent to send the message.
- Ramu's user agent sends the message to his mail server, where it is placed in a message queue.
- The client side of SMTP, running on Ramu's mail server, sees the message in the message queue.It opens a TCP connection to a SMTP running Raju's mail server.
- After some initial SMTP hand shaking, the SMTP client sends Ramu's message into the TCP connection.
- At Raju's mail server host, the server side of SMTP recives the message.Raju's mail server then places the message in Raju's mail box.
- Raju invokes his user agent to read the message at his convenience. The scenario is summarized in fig.5.29



RAMU'S MAIL SERVER TRANSFERS RAMU'S MESSAGE TO RAJU'S MAIL SERVER

Let us now take closer look at how SMTP transfers a message from a sending mail server to a receiving mail server.

We will see that the SMTP protocol has many similarities with protocols that are used for face-to- face human interaction.

- The client SMTP has TCP to establish a connection on port 25 to server SMTP.If server is down, the clients tries again later. Once the connection is established, the server and client perform some application layer handshaking. During this SMTP handshaking phase, the SMTP client indicates the e-mail address of the sender and the e-mail address of the recipient. Once the SMTP client and server have introduced themselves to each other, the client sends the message, SMTP can count on the reliable data transfer service of TCP to get the message to the server without errors. The client then repeats this process over the same TCP connection if it has other message to send to the server; otherwise it instructs TCP to close the connection.

Even though the SMTP protocol is well defined, a few problems can still arise. These are.

1. **Related to the Message Length :** Some older implementations cannot handle messages exceeding 64kB.
2. **Related to Time Outs :** If the client and server have different time-outs, one of them may give up while the other is still busy, unexpectedly terminating the connection.
3. Infinite mail storms can be triggered .

To get around some of these problems, extended SMTP (ESMTP) has been defined in RFC1425.

E-mail Gateways: E-mail using SMTP works best when both the sender and receiver on the internet and can support TCP connections between sender and receiver.However many

machines that are not on the internet)because of security problem) still want to send and recive e- mail from internet sites.

Another problem occurs when the sender speaks only RFC822 and the receiver speaks only X.400 or some proprietary vendor specific mail protocol.

- Here Host1 speaks only TCP/IP and RFC822, where as host 2 speaks only OSITP_4 ans X.400. They can exchange e-mail using an e-mail gateway.

Procedure:

1. Host 1 establishes a TCP connection to gateway and then use SMTP to transfer message there.
2. The gateway then puts the message in a buffer of messages destined to host 2.
3. A TP_4 connection is established between host 2 an the gateway.
4. The message is transferred using OSI equivalent of SMTA.

The problems here are

(a) The Internet address and X.400 address are totally different. Need of elaborating mapping mechanism between them.

(b) Envelope and header fields are present in one system and are not present in the other.

MAIL ACCESS PROTOCOL

Till now we have assumed that an users work on machines that are capable of sending and receiving e-mail. Sometimes this situation is false. For example in an organization, users work on desktop PCs that are no in the internet and are capable of sending and receiving e-mail from outside. Instead the organization has one or more e-mail servers that can send and receive e-mail. To sned and receive e-mails, a PC must talk to an e-mail server using some kind of delivery protocol.

There are currently two popular mail access protocols:POP_3(Post office Protocol version3) and 1 MAP (internet mail access protocl)

POP_3 : POP_3 defined in RFC 1939, it is an extremely simple amil access protocol.POP_3 begins when the user agents (clients) opens a TCP connection to the mail server (the server) on port 100.With the TCP with TCP connection established, POP_3 progress through three phases.

1. **Authorization:** The user agent sends a user name and a password to authenticate the user downloading the mail.
2. **Transaction:** The user agent receives messages. In this phase the user agent can also mark messages for deletion, remove deletion marks, and obtain mail statistics.
3. **Update:** During the third phase, update occurs after the client has issued the quit command, ending the POP_3 session. This time the mail server deletes the messages that were marked for deletion.

IMAP: The Internet Mail Access Protocol (IMAP), is defined in RFC 2060.It has many features than POP_3 , but it is also significantly maore complex. It was designed to help the user whi uses multiple computers, perhaps a workstation in the office, a PC at a home and laptop on the road.The basic idea behind IMAP is

for the e-mail server to maintain a central reposition that can be accessed from any machine.Thus unlike POP_3 , IMAP does not copy email to the user's personal machine because the user may have several.

The IMAP has many features.

a) It has commands that permit a user agents to obtain components of messages. This feature is useful when there is a low bandwidth connection between the user agent and mail server.

b) An IMAP session consists of a client command, server data and a server completion result response.

The IMAP server has four states.

1. **Non Authenticated State:** Initial state whenthe connection begins, the user must supply a user name and password before most commands will be permitted.
2. **Authenticated State:** The user must select a folder before sending commands that affect messages.
3. **Selected State:** The user can issue commands that affect messages.
4. **Log Out State:** Here the session is terminated.

TEXT / REFERENCE BOOKS

1. Behrouz A. Fourouzan, "Data Communication and Networking", McGraw-Hill Education India Pvt. Ltd - New Delhi.
2. William Stallings, Data and Computer Communications (8th ed.), Pearson Education, 2007.
3. P.C. Gupta, Data Communications and Computer Networks, Prentice-Hall of India, 2006.
4. Andrew S. Tanenbaum, "Computer Networks", Fourth Edition, Pearson.
5. L. L. Peterson and B. S. Davie, Computer Networks: A Systems Approach (3rd ed.), Morgan Kaufmann, 2003.