1. Explain in detail about Electronic Mail.

Electronic Mail:

Electronic mail, or e-mail, as it is known to its many fans, has been around for over two decades. Before 1990, it was mostly used in academia. During the 1990s, it became known to the public at large and grew exponentially to the point where the number of e-mails sent per day now is vastly more than the number of snail mail (i.e., paper) letters.

E-mail, like most other forms of communication, has its own conventions and styles. In particular, it is very informal and has a low threshold of use. People who would never dream of calling up or even writing a letter to a Very Important Person do not hesitate for a second to send a sloppily-written e-mail.

E-mail is full of jargon such as BTW (By The Way), ROTFL (Rolling On The Floor Laughing), anIMHO (In My Humble Opinion). Many people also use little ASCII symbols called smiley's or emoticons in their e-mail.

The first e-mail systems simply consisted of file transfer protocols, with the convention that the first line of each message (i.e., file) contained the recipient's address. As time went on, the limitations of this approach became more obvious.

Some of the complaints were as follows:

1. Sending a message to a group of people was inconvenient. Managers often need this facility to send memos to all their subordinates.

2. Messages had no internal structure, making computer processing difficult. For example, if a forwarded message was included in the body of another message, extracting the forwarded part from the received message was difficult.

3. The originator (sender) never knew if a message arrived or not.

4. If someone was planning to be away on business for several weeks and wanted all incoming e-mail to be handled by his secretary, this was not easy to arrange.

5. The user interface was poorly integrated with the transmission system requiring users first to edit a file, then leave the editor and invoke the file transfer program.

6. It was not possible to create and send messages containing a mixture of text, drawings, facsimile, and voice.

As experience was gained, more elaborate e-mail systems were proposed. In 1982, the ARPANET e-mail proposals were published as RFC 821 (transmission protocol) and RFC 822 (message format). Minor revisions, RFC 2821 and RFC 2822, have become Internet standards, but everyone still refers to Internet e-mail as RFC 822.

In 1984, CCITT drafted its X.400 recommendation. After two decades of competition, e-mail systems based on RFC 822 are widely used, whereas those based on X.400 have disappeared. How a system hacked together by a handful of computer science graduate students beat an official international standard strongly backed by all the PTTs in the world, many governments, and a substantial part of the computer industry brings to mind the Biblical story of David and Goliath.

The reason for RFC 822's success is not that it is so good, but that X.400 was so poorly designed and so complex that nobody could implement it well. Given a choice between a simple-minded, but working, RFC 822-based e-mail system and a supposedly truly wonderful, but nonworking, X.400 e-mail system, most organizations chose the former.

2. Explain the basic functions of e-mail system.

Basic functions of e-mail system:

Composition: It refers to the process of creating messages and answers. Although any text editor can be used for the body of the message, the system itself can provide assistance with addressing and the numerous header fields attached to each message. For example, 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 proper place in the reply.

Transfer: It refers to moving messages from the originator to the recipient. In large part, this requires establishing a connection to the destination or some intermediate machine, outputting the message, and releasing the connection. The e-mail system should do this automatically, without bothering the user.

Reporting: It has to do with telling the originator what happened to the message. Was it delivered? Was it rejected? Was it lost? Numerous applications exist in which confirmation of delivery is important and may even have legal significance ("Well, Your Honor, my e-mail system is not very reliable, so I guess the electronic subpoena just got lost somewhere").

Displaying incoming messages is needed so people can read their e-mail. Sometimes conversion is required or a special viewer must be invoked, for example, if the message is a PostScript file or digitized voice. Simple conversions and formatting are sometimes attempted as well.

Disposition: It is the final step and concerns what the recipient does with the message after receiving it. Possibilities include throwing it away before reading, throwing it away after reading, saving it, and so on. It should also be possible to retrieve and reread saved messages, forward them, or process them in other ways.

In addition to these basic services, some e-mail systems, especially internal corporate ones, provide a variety of advanced features. Move or when they are away for some period of time, they may want their e-mail forwarded, so the system should be able to do this automatically.

Most systems allow users to create mailboxes to store incoming e-mail. Commands are needed to create and destroy mailboxes, inspect the contents of mailboxes, insert and delete messages from mailboxes, and so on.

Corporate managers often need to send a message to each of their subordinates, customers, or suppliers. This gives rise to the idea of a mailing list, which is a list of e-mail addresses. When a message is sent to the mailing list, identical copies are delivered to everyone on the list.

Other advanced features are carbon copies, blind carbon copies, high-priority e-mail, secret (i.e., encrypted) e-mail, alternative recipients if the primary one is not currently available, and the ability for secretaries to read and answer their bosses' e-mail.

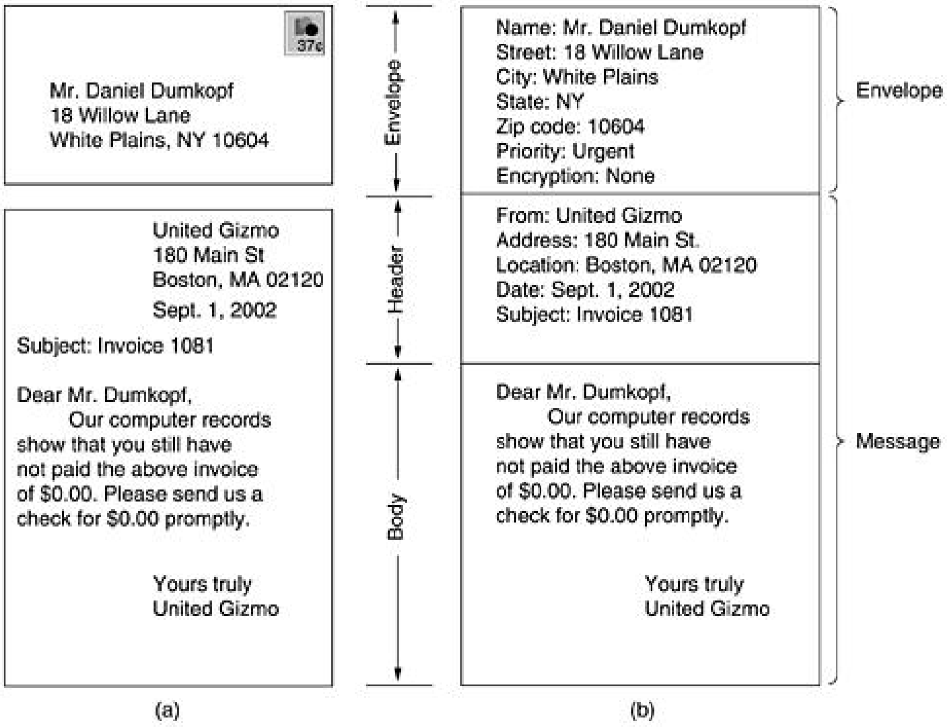


Figure: Envelopes and messages. (a) Paper mail. (b) Electronic mail.

3. What is Authentication? How it is different from Authorization? Explain in brief different authentication protocols with their relative merits and demerits.

Authentication:

Authentication is the process of verifying the genuineness of someone (or) something which claims to be genuine.

In the internet applications, authentication can be performed by means of login-ID and passwords, i.e., an individual who knows the correct ID and a respective password is considered to be a genuine user and is provided access to the internal applications. Whereas, authorization is a process of assigning different access permissions to different users.

The authorization is the first task carried-out by a system administrator after authentication is performed.

In other words, a system administrator assigns access permissions and privileges to the users once they get authenticated.

Authentication Protocols:

Authentication protocols are mainly used for addressing the security issues associated with the untrusted networks (internet). Many different protocols and methods are available for authentication.

Diffie-Heliman Key Exchange Protocol:

When two strangers like to establish a shared secret key, they can make use of a 'Diffie-Heliman Key Exchange Protocol'.

Working of Diffie-Heliman key exchange protocol is as follows.

The senders and receivers will exchange the calculated values between each other, using which they will compute an encryption. This calculation also includes two more numbers which are not kept secret.

Consider a situation when Alice and Bob would like to communicate they need to have a shared secret key. To establish this key any one among Alice and Bob can decide to use two large prime numbers p and n such that the result of (p-1)/2 is also a prime number, and then tell the other about these numbers openly. Then both of them will select their large secret numbers as a and b respectively.

To start this key exchange protocol, suppose Alice sends a message consisting of (p, n n^a mod p) to Bob. Then Bob replies with a message containing Alice will now compute the secret key by raising the received message to the power a, i.e.,(n^b mod p)^a = n^{ab} mod p. On the other hand, Bob will compute the secret key by raising the received message to the power b i.e., (n^a mod p)^b = (n^{ab} mod p). Eventually, both Alice and Bob will now share a secret key i.e., (n^{ab} mod p).

Disadvantage:

If an attacker comes to know the p and n numbers from the messages and if he also computes the a and b values then he will be easily able to compute the secret key that is shared by the sender and receiver.

Merits:

- **(i)** This key exchange algorithm enables the users to establish a shared session even with strangers.
- **(ii)** Even if the intruder intercepts the message he/she cannot understand it unless he knows the shared session key.

Demerits:

- **(i)** The problem with the Diffie-heilman key exchange algorithm is that, it cannot deal with bucket brigade attack in which intruder directly intercepts the session establishment messages.
- **(ii)** For interacting with 'n' number of people, we need 'n' keys to be stored and managed.

4. How POP works? What are the advantages of IMAP over POP?

Post Office Protocol, version 3 (POP3) is one of the simplest message access protocol available which requires installation of POP3 software on both the client machine as well as the server machine.

The following figure 4.1 shows the architectural view of communication that takes place betweenaPOP3clientand a POP3 mail server.

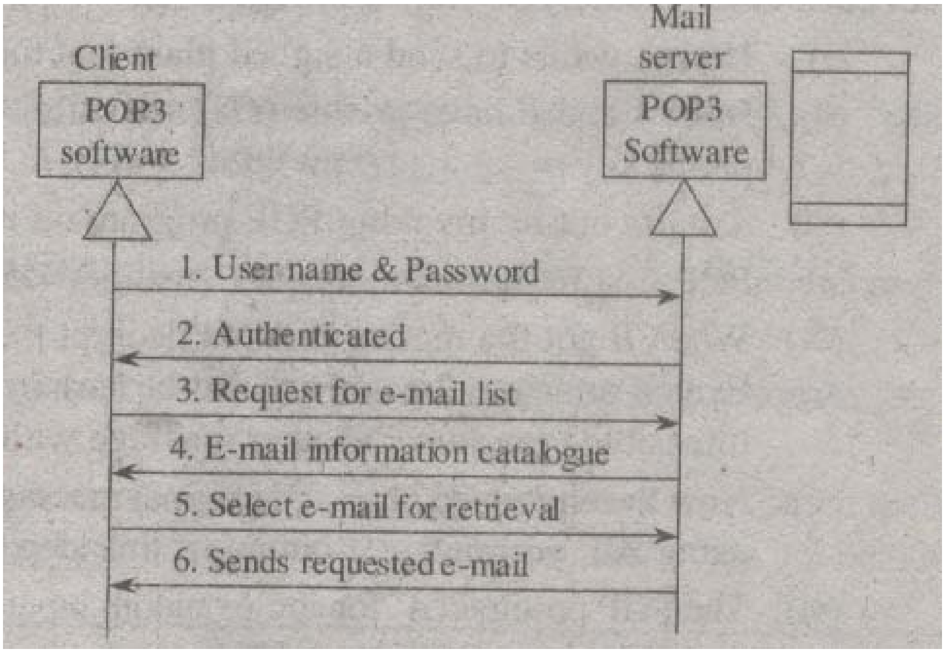

Client
POP3 software
Mail server
POP3 Software
1. User name & Password
2. Authenticated
3. Request for e-mail list
4. E-mail information catalogue
5. Select e-mail for retrieval
6. Sends requested e-mail

Figure 4.1: PUP3 Communication

In POP3 communication, the client needs to bring out the e-mails from the mailbox which resides on the mail server. Initially, client sends username and password for authorization. The mail server verifies the username and password and then provides privileges and permissions o that client. The client requests a list of e-mails to which mail server provides e-mail information catalogue (including e-mail numbers, sizes etc.). Finally, client retrieves e-mail from the mailbox based on its requirement.

POP3 consists of two message access modes such as keep mode and delete mode. In keep mode context, the mail stays in the mailbox once it is retrieved for future reviewing. This mode is commonly used when user is remotely accessing the mails.

In delete mode context, the mail gets deleted from the mailbox as soon as it is retrieved. This mode is commonly used when user is accessing the mails from its personal computer, where it can save the mails for future use.

Internet Mail Access Protocol version 4 (IMAP4) provides certain advantages to the user over POP3 which are as follows,

(i) E-mail header can be viewed before retrieval.

(ii) E-mail contents can be identified with a given string of characters before retrieval.

(iii) E-mail can be partially retrieved when the bandwidth is low and the multimedia contained in e-mail needs high bandwidth.

(iv) A user can have accessing privileges such as creating, deleting and renaming the mailboxes on the mail server.

(v) A collection of mailboxes can be created in a folder for storing the e-mails.

5. Explain how privacy is achieved in e-mail system.

Privacy Enhanced Mail (PEM):

PEM is the internet Privacy Enhanced Mail standard adopted by the Internet Architecture Board (JAB) to private secure electronic mail over the Internet. It was initially designed by the Internet Research Task Force, Privacy and Security Research Group (PSRG). The PEM protocols provide for encryption, authentication message integrity and key management.

PEM Documents:

The specification for PEM comes from four documents,

- ❖ Messages encryption and authentication procedures.
- ❖ Certificate-based key management.
- ❖ Algorithms modes and identifiers.
- ❖ Key certification and related services.

Procedure for PEM Messages:

PEM's heart is its message format. The following format is necessary for PEM messages.

- ❖ Identifying the type of processing performed on the message i.e., the PEM messages should be in human readable form.
- ❖ This can be done by using PEM software. A PEM message is always signed, it is optionally encrypted.

- Compute the message hash using either MDI (denoted by “RSA-MD I “) or MD 5 (Which would be denoted by“RSA-MD5”).
- With the help of DES, encrypt the concatenated message (i.e., hash and message) and encode this message with base 64 coding and then transmit this message.
- There are various key certifications available like IPRA (Internet Policy Registration Authority), PCA (Policy Certificate Authority). Each certificate has a unique number that includes an MD5 hash signed by the certificate authority’s private key.

6. Describe the significant features of application layer.

The following are the features of application layer.

1. Efficient User Interface Design:

Application layer, the top layer of the OSI model serves as the Interface between user and application and also between user and the network. It provides the user, a way of accessing information present on the network through an application. Since the application layer is closest to the end user, both the user and the application layer can interact directly with the application.

2. Identification of Communicating Parties:

Application layer defines the way ‘how’ an application running on one system communicates with an application on another system. In addition to this, the layer also determines ‘who’ the communicating partners are and whether they are ready for communication or not (i.e., their identity and availability) whenever there is an application which has data to transmit.

3. Determination of Resource Availability:

For a communication to be successful a variety of resources are required. So, whenever a communication request is made, the application layer verifies whether the existing network resources are sufficient for handling the communication request. Thus, it determines the availability of resources.

4. Synchronization of communication:

The application layer is responsible for verifying either the two communicating parties are synchronized. It does this by ensuring that both the parties employ similar network protocols and that the communication is done in a cooperative manner.

5. Implementation of Protocols:

The application layer implements various protocols like Telnet, HTTP (Hyper Text Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol) etc. Among which the most widely used one is HTTP. This protocol is the basis for the World Wide Web. When the users need to access some web pages of a website, then they specify the name of the page in the URL and send it to the servers using the browser. This request is sent as HTTP request and response is also sent to the user using HTTP protocol.

Then communication protocols of application layer are used by, many applications that are responsible for providing network functionality. The other protocols are used for purposes like file transfer, emails and network news.

7. What is meant by encryption? Describe the public key cryptography.

Encryption:

Encryption is a method of converting plain text into cipher text. Using this method, security of data can be achieved effectively. An encrypted file can be decrypted if the user has the capability of accessing a secret key or password. In this context, unencrypted data is referred to as plain text where as encrypted data is referred to as cipher text.

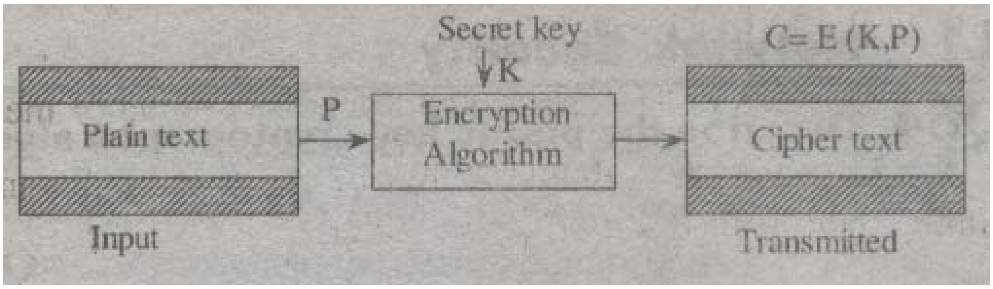


Figure 7.1: Encryption process

The following are the two major types of encryption,

1. Symmetric encryption

2. Asymmetric encryption.

1. Symmetric Encryption:

Symmetric encryption is also known as private key or secret key encryption. In this, only one secret key is required for encryption and decryption of the message. This key shared by both sender and recipient. It is a simple process when compared to the asymmetric encryption.

2. Asymmetric Encryption:

Asymmetric encryption is also known as pubic key encryption. In this, two keys are required for encryption and decryption of a message i.e., a public key and a private key. Private key must be kept secret for security purposes while the other key must be shared by both sender and recipient. It is a complex and time consuming process when compared to symmetric encryption.

Public key Cryptography:

Public key cryptography was invented by Diffie and 1-lehman in the year 1976. For this reason, it is sometimes known as Diffie-Heliman encryption. Public key cryptography is also known as asymmetric cryptography. It is a form of cryptography in which an user has a pair of cryptographic keys i.e., public key and private key. The private-key is kept secret, whereas the public key is distributed widely. A message or text data which is encrypted with the public-key can be decrypted only with the corresponding private key. For instance, when Johny wants to send a secure message to Sunny, he uses Sunny's public key to encrypt the message. Sunny then uses his private key to decrypt it.

A public key cryptography/encryption consists of the following five elements. They are,

(i) Text data/Message

(ii) Encryption algorithm

(iii) Public key and private key

(iv) Cipher text/Unreadable text

(v) Decryption algorithm.

(i) Text data/Message:

This can be any input data, such as text data or message. For example, Johny is a user of computer and wants o send his message, M="Hello" securely to his friend Sunny, who is also a user of computer.

(ii) Encryption Algorithm:

To encrypt the message, an encryption algorithm performs certain transformation on it. There are various encryption algorithms but the RSA public key encryption algorithm is mostly used to perform certain transformations or calculations on the text data or message.

For example, Johny uses the public key of Sunny and encrypted his message by using RSA algorithm.

(iii) Public Key and Private Key:

These pair of keys is used to encrypt and decrypt the message respectively. The private key is always kept secret, whereas public key is widely distributed.

For example, Johny uses a public key of Sunny to encrypt his message, whereas Sunny uses his private key to decrypt the Johny's message as shown in the figure7.2.

(iv) Cipher text/Unreadable Text:

Once the encryption is done on the text data it is in unreadable format means it cannot be read by human beings.

For example, Johny's message has converted into unreadable from so that nobody except Sunny can read his message, as he has a corresponding private key for that message.

(v) Decryption Algorithm

A decryption algorithm takes the unreadable text and its corresponding key to original text. Hence, we can say that the decryption algorithm is the reverse of encryption algorithm.

For example, decryption algorithm takes the unreadable text of Johny and also takes the Sunny's private key to decrypt that message and convert the unreadable text into readable form i.e., original text sent by Johny. As shown in the below figure7.2

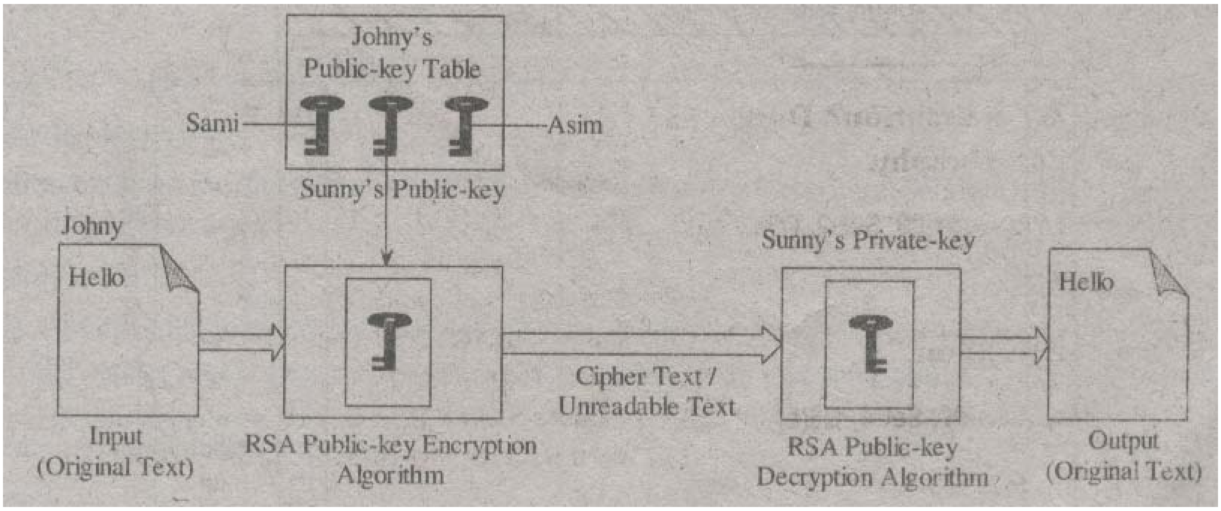


Figure 7.2: Public key Encryption

8. Write short notes on VTR.

Communication between different types of equipment and software is made possible through networks. Full-screen text editor iš a software using which communication is made possible between the screen and the user. Using the editor, text is displayed on screen, cursor can be moved by the user and changes can be made in the text. But, the number of rows and columns on the screen are dependent on the terminal that is being used i.e., the commands to change cursor position, perform insert and delete operations on text that varies as per the type of terminal. This problem can be avoided by the use of Virtual Terminal Protocol (VTP).

A VTP is a data structure whose information is maintained by a local terminal or an application software. This protocol is used to define the state of the terminal like the current position of cursor, its shape, number of rows and columns, reverse video indicator and color. By referencing to this protocol, user and application perform their operations irrespective of the terminal-specific issues. For instance, the data is displayed on the screen independent of the terminal type. VTP protocol performs a reverse process when data is entered by the user. This process involves the following three steps,

(i) The format of the data structure is defined by VTP.

(ii) The user input is converted into a standard form by the software.

(iii) The standard screen is read by the application.

In case of scrolling, virtual terminals store more data than the data that can be the displayed on screen, as shown figure 8.1 below.

Information stored in VTI specifies the first and last lines of the data displayed (window). The displayed data is defined within window delimiters. Whenever the user scrolls, delimiters are changed by the virtual terminal software, thereby retrieving different text lines on window.

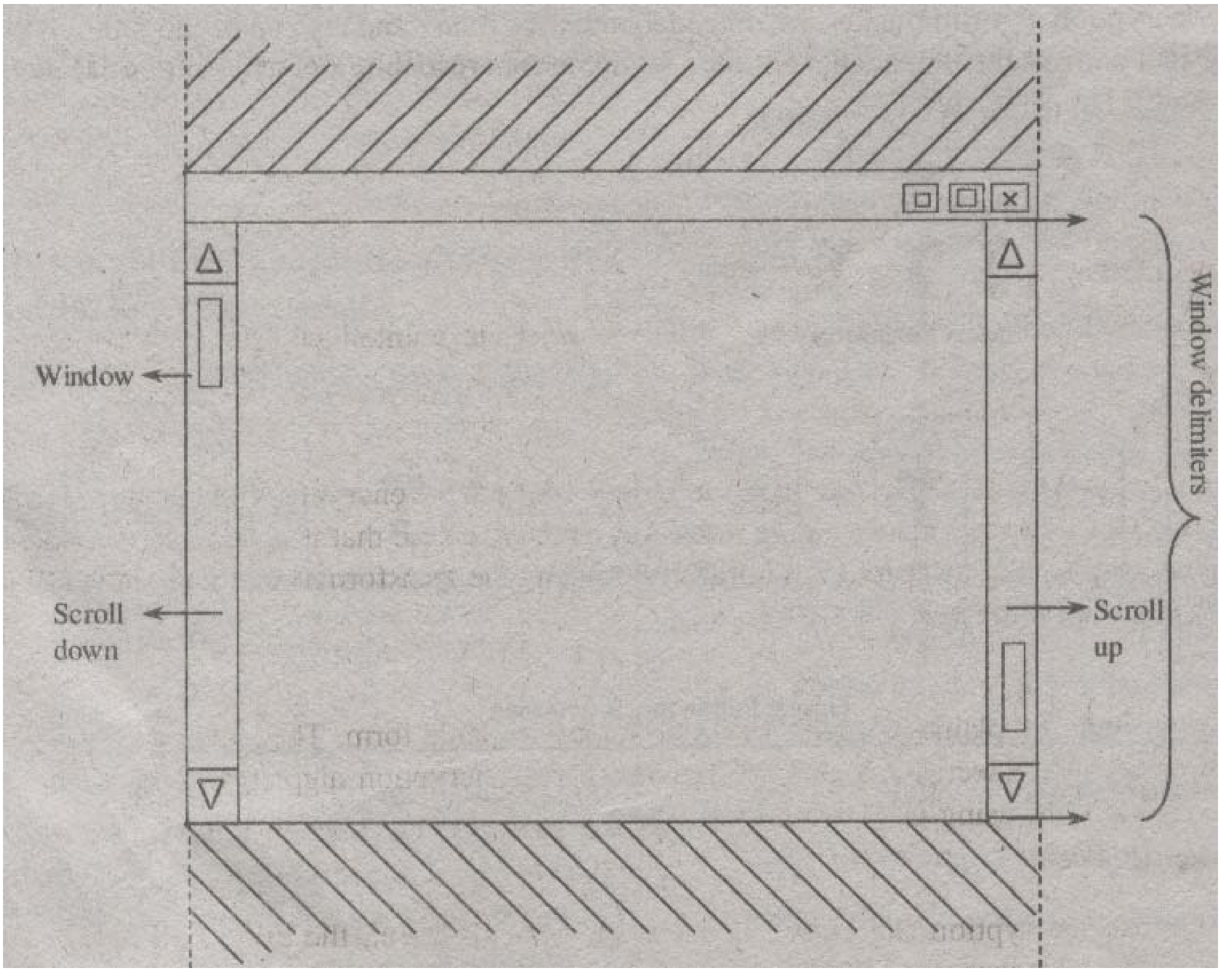


Figure 8.1: Virtual terminal

An example of VTP is Telnet, which is a network protocol used over LANs or Internet. This protocol generates a bidirectional interactive communication between a remote user and application.

9. Write short notes on architecture of WWW.

World Wide Web:

The World Wide Web (WWW), or the web, is a repository of information spread all over the world and linked together. The WWW has a unique combination of flexibility, portability and user-friendly features that distinguish it from other services provided by the Internet.

The WWW project was initiated by CERN (European Laboratory for Particle Physics) to create a system to handle distributed resources necessary for scientific research. The WWW today is a distributed client-server service, in which a client using a browser can access a service using a server. However, the service provided is distributed over many locations called websites.

The web consists of many web pages that incorporate text, graphics, sound, animation and other multimedia components. These web pages are connected to one another by hypertext. In a hypertext environment the information is stored using the concept of pointers. WWW uses a concept of HTTP which allows communicating between a web browser and web server. The web pages can be created by using a HTML (Hyper Text Markup Language). This language has some commands which are used to inform the browser about the way of displaying the text, graphics and multimedia files. HTML also has some commands through which we can give links to the web pages.

If we want to get a page from the web, we have to type URL (Uniform Resource Locator) ‘for our desired page, or otherwise we have to click on a link that provides the URL. The URL specifies the internet address of the web server, the directory and name of our desired page. If there is no directory or web page specified, then the web server will provide a default home page.

The WWW today is a distributed client-server service, in which a client using a browser can access a service using a server. Figure 9.1 illustrates how the different web site can communicate with each other.

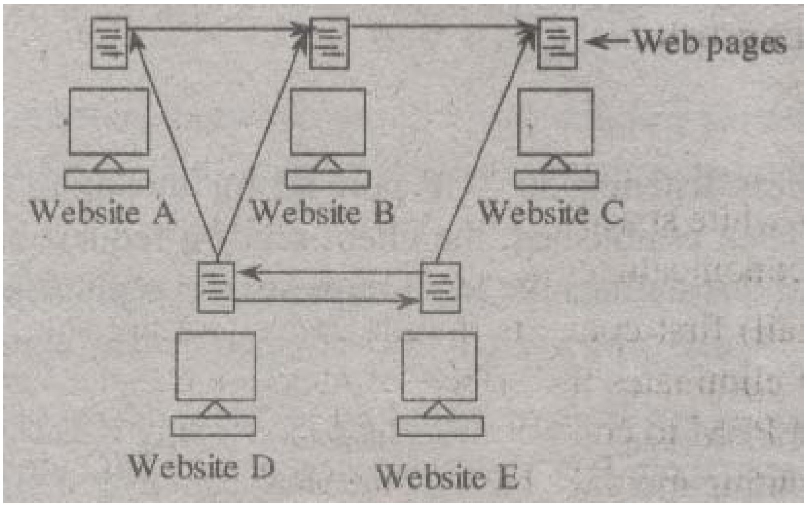


Figure 9.1: Distributed Services (Different Websites can communicate with Each Other)

Working of a Web:

The Web operates on a client/server model. A web browser acts as the client in the WWW interaction. Using this program, a user sends a request for a web page stored on a web server. The web server locates this web page and sends it back, to the client computer. The web browser then interprets the web page written in the HTML language and then displays it on the client computer’s screen.

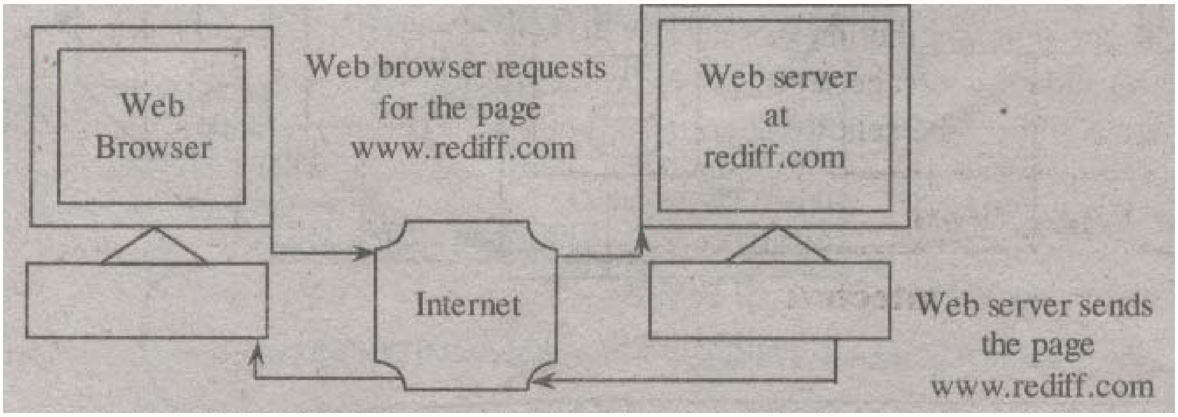


Figure 9.2: Interaction between a Web Browser and a Web server

10. With the help of diagram explain the encryption model.

Symmetric cipher model uses a secret-key or a single-key for encryption or decryption purposes. It employs a symmetric encryption, also known as conventional encryption single-key or secret-key encryption.

A few symmetric key algorithms are,

1. Data Encryption Standard (DES)

2. Triple DES (3DES)

3. International Data Encryption Algorithm (IDEA)

Symmetric cipher model as shown in the figure 10.1 consists of five components,

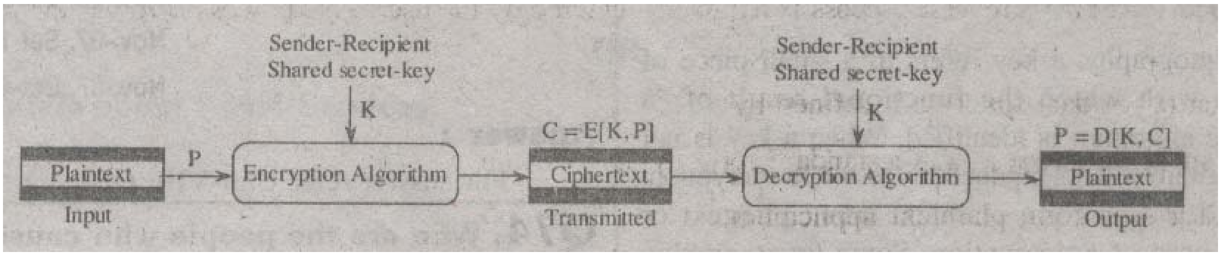


Figure 10.1: Symmetric Cipher Model

1. Plaintext:

It refers to the original message that is not encrypted and is human readable. It forms an input to an encryption algorithm and output of or decryption algorithm.

Example:

A text document is an executable file or an image.

2. Encryption Algorithm:

Application of this algorithm will transform plaintext to an unreadable, unintelligible form by performing various transformations and substitutions.

3. Secret-key:

It is a piece of data that is randomly selected. It acts as an input to both the encryption and decryption algorithms. Therefore, both the sender and receiver must share the same key and make sure that it is secured, in order to restrict intruders from reading messages. The encryption algorithm performs the transformations and substitutions on the plaintext accordingly, depending on the key.

4. Cipher text:

It is a scrambled version of a plaintext and is not in a human-readable form. The cipher text produced by the encryption algorithm depends on the secret-key and the plain text. The encryption algorithm can produce different cipher text for the same plain text by using different secret-keys.

5. Decryption Algorithm:

It is a reversed form of encryption algorithm. It takes the cipher text (i.e., the encrypted data) as input and decrypts it, using the same key that was used by the encryption algorithm in order to produce the plaintext (i.e., the original message or data).

11. What is the role of key secrecy and algorithm secrecy in security?

Algorithm Secrecy:

'Algorithm secrecy' is a way of keeping an algorithm secret from the unauthorized users. A concept that is based on the secrecy of an algorithm is often referred to as secrecy through obscurity, which provides security by hiding the data in an obscure location. But, the system using this concept may suffer from many security vulnerabilities. The disadvantage of using algorithm secrecy is that it is difficult to maintain the secrecy of the system because when algorithms are known to the unauthorized users, an entirely new secret algorithm is to be developed for performing encryption and decryption of cipher text. In addition to algorithms, it would be necessary to change keys as well.

Key Secrecy:

In cryptography, a key refers to a small piece of information with which the functional result of a cryptographic algorithm is identified. When a key is not used, the algorithm will not produce any result. In encryption, a key is used to transform plaintext into cipher text or vice versa in case of a decryption. Some cryptographic algorithms like message authentication codes and digital signature schemes use key for the purpose of security. "Key" protection can be easily managed when compared to "encryption algorithm" protection. However, the length of the key must be as long as possible so as to provide a strong security.

When a key is known by the unauthorized users, it can be easily changed. Hence, the security of an encryption system mostly depends on a certain key, which is being kept secret.

`Practically, it is difficult to provide key secrecy in cryptography. For instance, when an attacker obtains the key, the original message can be retrieved from the encrypted data.

Encryption algorithms that use a similar key for performing both encryption and decryption are referred to as symmetric key algorithms. The other public key cryptographic algorithms that use two different keys for encryption and decryption are known as asymmetric key algorithms. In asymmetric key algorithms, one key is made public, while the other is kept private. Hence, it is extremely difficult for the unauthorized users to determine the private key even if the corresponding public key is known to them.A user of public key technology keeps the private key secret and discloses the public key so that anyone can send them an encrypted message.

12. What is cryptanalysis? Briefly discuss about substitution cipher, transposition ciphers and, onetime pads.

The messages which are intended to transmit secretly and securely are subjected to the process of encryption and decryption in order to provide required security. The original message which is to be encrypted i called plain text. This plain text is transformed by a function with encryption key (K) as the parameter. The plain text after the transformation i.e., the output of the encryption process is known as cipher text. And this cipher text (encrypted message with key) is actually transmitted.

Though an intruder listens to this message (cipher text) by catching the communication channel yet he cannot decrypt the cipher text because he doesn’t know the key. Even though he doesn’t know the key yet he is able to break that cipher text sometimes and that art of breaking ciphers is called as cryptanalysis.

The art of devising as well as breaking ciphers is collectively called as cryptology.

The encryption methods are, divided into two categories,

1. Substitution Ciphers

2. Transposition Ciphers.

1. Substitution Ciphers:

In this cipher, each letter (or) group of letters is replaced by another (or) group of letters. Good example of substitution cipher is Caesar cipher. In this cipher, a becomes D, and b becomes E and so on and Z becomes C.

Example:

Attack becomes DWWDFN

This general system is called mono alphabetic substitution.

In substitution ciphers, order of letters is same as that of plain text but just disguises them.

2. Transposition Ciphers

In contrast to substitution ciphers, transposition ciphers read the letters but do not disguise them. The key of this cipher is a word, containing no repeated letters. An example of a transposition cipher text is as follows.

M	E	G	A	B	U	C	K	Plain Text
7	4	5	1	2	8	3	6	
p	l	e	a	s	e	t	r	Please transfer one million dollars to my swiss bank account six two two.
a	n	s	f	e	r	o	n	
e	m	i	l	l	i	o	n	**Cipher text** **AFLLSKSOSELAWAIATOOSSC** **TCLNMOMANTES1LYNRNNTSO** **WDPAEDOBUOERICXB**
d	o	l	l	a	r	s	t	
o	m	y	s	w	i	s	s	
b	a	n	k	a	c	c	o	
u	n	t	s	I	x	t	w	
o	t	w	o	a	b	c	d	

The purpose of the key is to number the columns. The plain text is in rows and cipher text is prepared by gathering letters in columns.

Onetime Pads:

There is an easy way of constructing an unbreakable cipher. The procedure is initiated with the choice of a random bit string as the key. Converting plaintext into a bit string and computhexc1usjve OR operation for these two strings i.e., (key string and bit string of plain text), and resulting output stri4gi the cipher text. This method is known as Onetime Pad.

13. What is security? What is network security? What is information security? How network security and information security are related?

Security:

Security is a protective measure that results a condition to ensure a state of data integrity is maintained against unauthorized access. In simple terms, security is a measure or mechanism which ensures safety from intruders. The intent of using security measure is to make sure that intruders cannot interfere in any confidential matters. Security can be provided to information as well as network.

Network Security:

Network security s mainly concerned with protection of networks and their services from unauthorized access, alteration and destruction. In simple terms, network security protects remote services from intruders who are not authorized to use them. An efficient network security strategy involves identification of all the threats, before selection of tools that tackle them.

Information Security:

The process of preventing the sensitive information from the intruders is simply termed as information security. It protects information availability, confidentiality and integrity against unauthorized access. The intent of information security is to make sure that intruders cannot read, write or modify any content of the information.

The network security and information security are mostly related to each other i.e., network security provides security to the information which is being traversed across the network. Hence, it also performs the functionality of information security in addition to securing the network peripherals.

14. What are the pros and cons of providing security?

There are various benefits associated with providing security. They are,

(i) Confidentiality/ Privacy

(ii) Integrity

(iii) Availability

(iv) Authentication.

(i) Privacy:

Security ensures that the information available in a system is kept confidential, by allowing access only to authorized users.

(ii) Integrity:

(a) Hardware Integrity

The physical and administrative security measures ensure that the hardware is safe from incidental (or) intentional damages and is readily available round the clock.

(b) Software Integrity:

Security ensures that the system software I free from any illegitimate alterations, damages etc.

(c) Data Integrity

Security also ensures that data files are secured from unauthorized access thereby privacy, availability and integrity is maintained.

(d) Network Integrity

Security mechanisms also prevent the network from active and passive attacks.

(iii). Resource Availability:

Security also ensures that computer resources are available only to the legitimate (or) authorized users.

(iv). Authentication:

Security also ensures that the authentication of users (or) resources is done before initiating any transaction.

Disadvantages (or) Cons of Providing Security:

Apart from the various advantages, the security also has certain drawbacks. They are,

(i) Expensive

(ii) Time consuming

(iii) Additional resource utilization

(iv) Increased employee count.

(i) Expensive:

Though security mechanisms protect the hardware, software, data and network from intruders' interference, they are quite expensive to implement and maintain.

(ii) Time Consuming:

Providing confidentiality, integrity, availability, authenticity etc., involve lot of steps to be taken. Thus, they require an additional time.

(iii) Additional Resource Utilization:

The implementation of the security mechanisms involves utilization of additional memory space, bandwidth, hardware and software for storing, exchanging, downloading and implementing the encryption/decryption procedures.

(iv) Increased Employee (or) Staff Count:

Providing security to the various applications need the involvement of more number of high-end professionals, thus, more staff must be employed.

15. Who are the people who cause security problems?

Many unauthorized people cause network security problems for gaining information about the other users or causing harm to them. The following is the list of intruders,

(i) Student:

A student can cause network security problems for his/her fun by interrupting with the e-mails of other users.

(**ii) Sales Representative**:

A sales representative can harm the network security by pretending that he/she is representing the entire country but not a specific state or city.

(iii) Businessman:

By identifying the strategic marketing plan of his competitor, a businessman can damage network security.

(iv) Hacker:

A hacker can intrude the network security by stealing someone's data or by testing the security of some others system.

(v) Accountant:

By fraudulently obtaining the company's money, an accountant can destroy network security.

(vi) Ex-employee:

For taking a revenge of being fired by the company, an ex-employee can interrupt the security of the network.

(vii) Spy:

It damages the network security by learning the military strength of an enemy.

(viii) Con Man:

By stealing and selling the credit card numbers, the network security gets damaged.

(ix) Terrorist:

The network security is affected by stealing the warfare secrets by a terrorist.

(x) Stockbroker:

A stockbroker can cause damage to network security by denying to the commitment made by him with the customer through an e-mail.

16. Explain in detail DES.

DES (Data Encryption Standard):

DES is now the most widely used key cryptographic systems. DES can be implemented much more efficiently in hardware rather than in software.

In this method, DES first divides the original message into blocks of 64 bits. Each block of 6 bit plaintext is separately encrypted into a block of 64 bit cipher. DES uses a 56 bit secret key. There are about 19 stages in this algorithm out of which 16 stages are for iteration of the message. This is shown in figure 16.1. The encryption process is reverse of the encryption. Each step in DES takes 64 bit input from preceding step and produces a 64 bit output for next step.

The first step performs the initial transformation (permutation) of 64 bit plaintext. The last step performs the transformation just in the reverse of initial transformation.

The stage before the last stage performs the 32 bits swap of the message encrypted in the 16 iterations. The working of each iteration is shown in figure 16.2.

Each iteration divides the 64 bit text into 32 bit inputs and produces two 32 bit outputs. The left output is simply a copy of right input. The right output is the bitwise of EXCLUSIVE OR of the left input and a function of right input and key for this stage K_i.

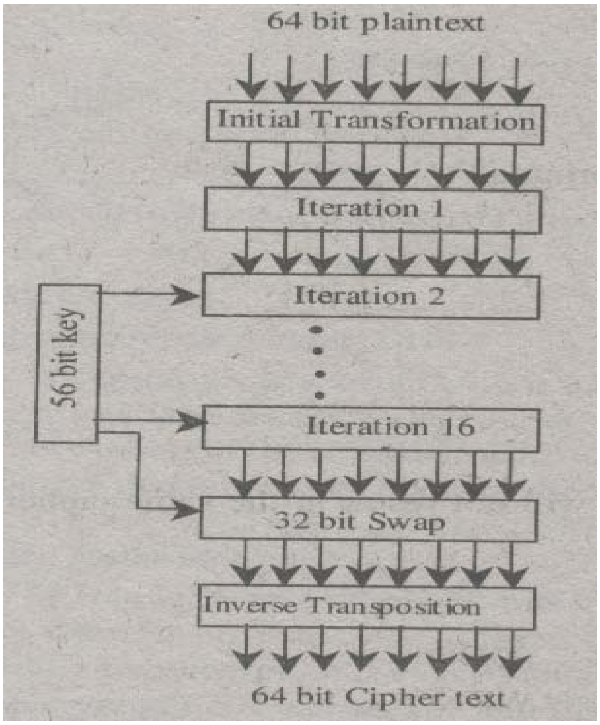


Figure 16.1: General Outline of DES

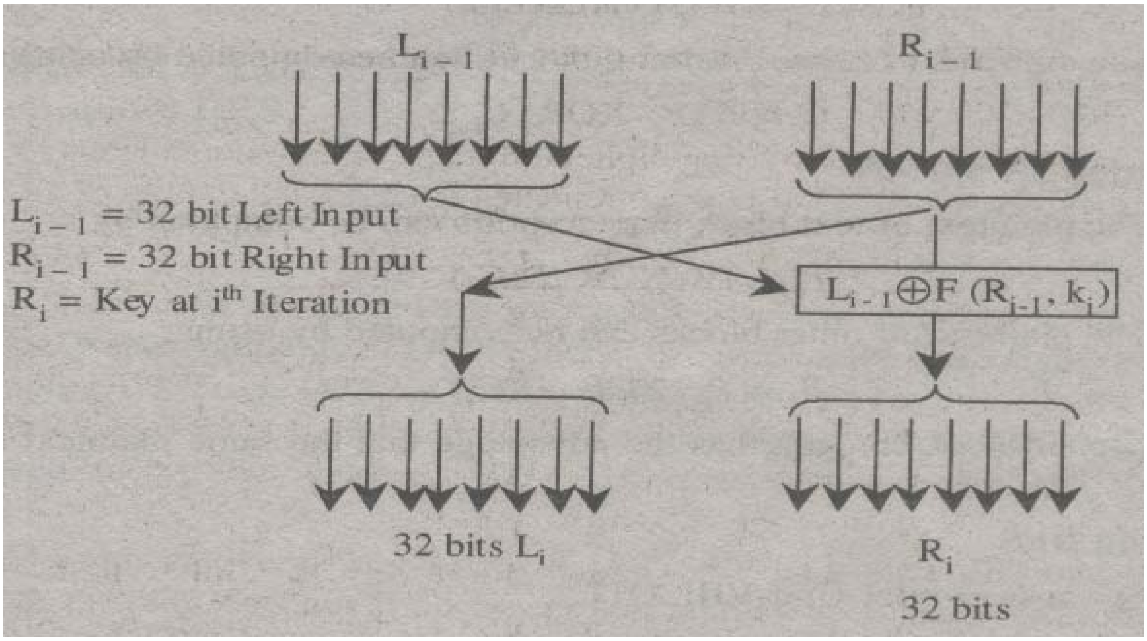

L_{i-1}
R_{i-1}
L_{i-1} = 32 bit Left Input
R_{i-1} = 32 bit Right Input
R_i = Key at i^{th} Iteration
$L_{i-1} \oplus F(R_{i-1}, k_i)$
32 bits L_i
R_i
32 bits

Figure 16.2: Working of One Iteration

Before algorithm starts, a 56 bit transposition is applied to the key. The key is partitioned into two 28 bit units before each iteration. These 28 bit units are rotated left by a number of bits depending on iteration number. K_i is derived from this rotated key by applying yet another 56 bit transposition to it. A different 48 bit subset of 56 bit is extracted and permuted on each round.

DES Chaining:

The DES works in Electronic code book mode, this mode may give a chance to break the DES, if the structure of message is known to the intruder. This can be stopped by chaining all the block ciphers. One way of chaining is called as "Cipher block chaining".

In this method, each plaintext block is EXCLUSIVE OR ed with previous cipher text block before applying encryption. The first block is EXCLUSIVE OR ed with a randomly chosen Initialization Vector (IV) that is transmitted along the cipher text. The chaining of blocks is shown in figure 16.3, EXCLUSIVE OR is denoted by #.

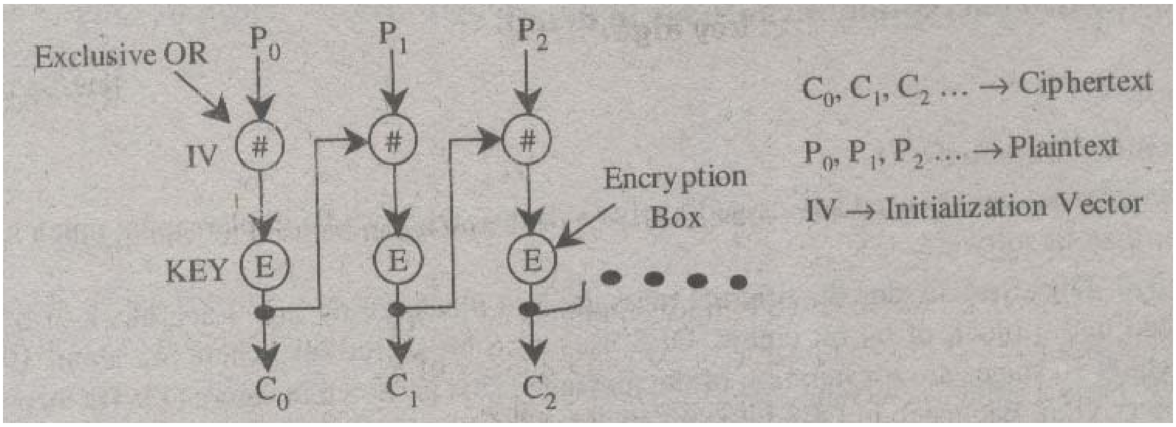

Exclusive OR
P0
P1
P2
IV
#
KEY
E
Encryption Box
C0
C1
C2
C0, C1, C2 ... → Ciphertext
P0, P1, P2 ... → Plaintext
IV → Initialization Vector

Figure 16.3(a): Cipher Block Chaining(Encryption)

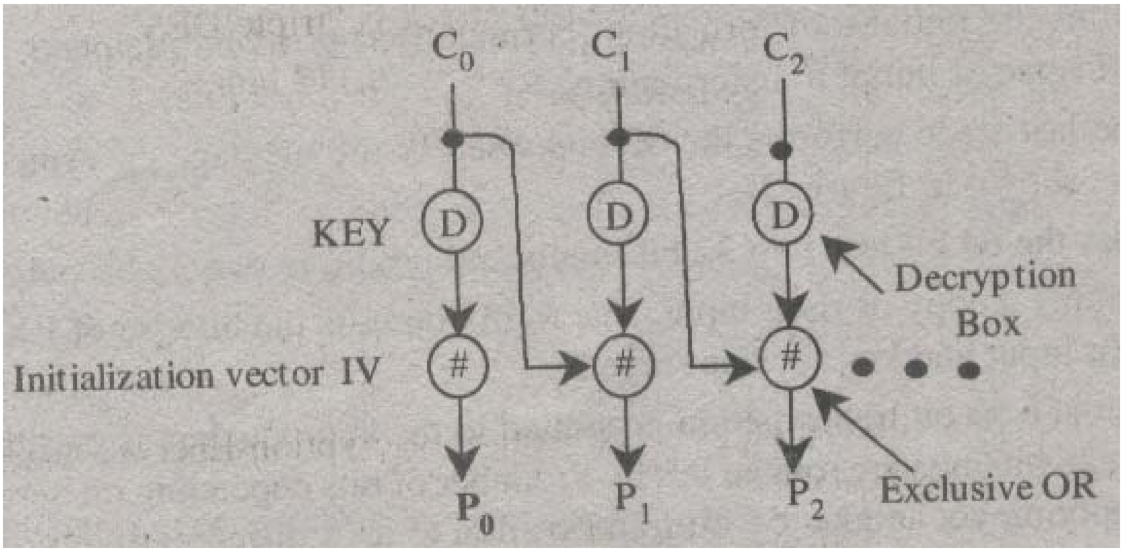


Figure 16.3(b): Cipher Block Chaining(Decryption)

Encryption:

The ciphertext of first block can be computed by using, C_0=E(P_0 XOR IV) The ciphertext of the remaining blocks can be computed by using the formula,
C = E (P_i XOR C_{i-1})

Decryption:

The plaintext of text block in decryption can be computed by

$$P_0=IV \text{ XOR } D(C_0)$$

The plaintext of other blocks can be computed by using

$$P_1= P_0 \text{ XOR } D(C_1)$$

Cipher block chaining has the advantage that the same plaintext block will not result in the same ciphertext block.

17. What is DNS? Explain usage of resource records.

Domain Name System:

The Domain Name Service (DNS) is a hierarchical distributed method of organizing the name space of the Internet. The DNS administratively groups hosts into hierarchy of authority that allows addressing and other information to be widely distributed and maintained. A key advantage to the DNS is that it eliminates dependence on' a centrally maintained file that maps host names addresses. DNS is supported via asset of network-resident servers, also called domain name servers.

The IP address is a numeric address that serves role analogous to a telephone number. In representation, addresses always consist of four numbers; four decimal values separated by periods. Figure 17.1 illustrates the addresses. The computer named mugwump.cl.msu.edu for instance, is assigned a number of 35.8:1.212. The reason a computer would have two names is that IP addresses numeric; they can be easily understood and manipulated b the hardware and software that must move information over the Internet. So IP addresses are better-suited t computers, and domain addresses are better-suited t humans. DNS allows a translation between the domain na and the IP address. Domain names do not necessarily hay four parts. They might have only two parts-a top-level domain such as “edu” or “corn,” preceded by a sub domain or three, four, or many. The limitations are,

(i) A domain- Mime cannot exceed 255 characters and

(ii) Each part of the name cannot exceed 63 characters.

The DNS translates the plain english address, www.metahouse.com, for example, into numbers that Internet computers can understand, such as 123.23.43. 121. In order to do this efficiently, the Internet has been organized into a number of major domains. Major domains refer to the letters at the end of a plain english address, such as .com. A number of common domains are used in the United States: .com (commercial); .edu (education); .gov government); .mil (military), .net (Internet service providers and networks-companies and groups concerned with the organization of the Internet); and .org (organization). Because the number of Internet sites has been growing exponentially, the domain name system is being expanded and may also include at least seven additional domains, such as .web for Web. Only two letters are used outside the United States to identify the domains; for example, .au for Australia; .ca for Canada; .uk for United Kingdom; and .for for France.

IP address read from general to specific
35.8.1.212

Network address Host address

Figure 17.1

Domains are organized in a hierarchical manner, so that beneath major domains are many minor domains. As an example of how the DNS and domains work, looks at NASA's SPACE link Internet address: spacelink.msfc.nasa.gov.

The .top domain is .gov, which stands for government. The domain just below that is .nasa, which is the NASA domain. Then below that, .msfc (Marshall Space Flight Center) is one of NASA's many computer networks. SPACE link identifies the NASA computer that runs the SPACE link program. SPACE link's numeric IP address has changed through the years, but its Internet address has stayed the same.

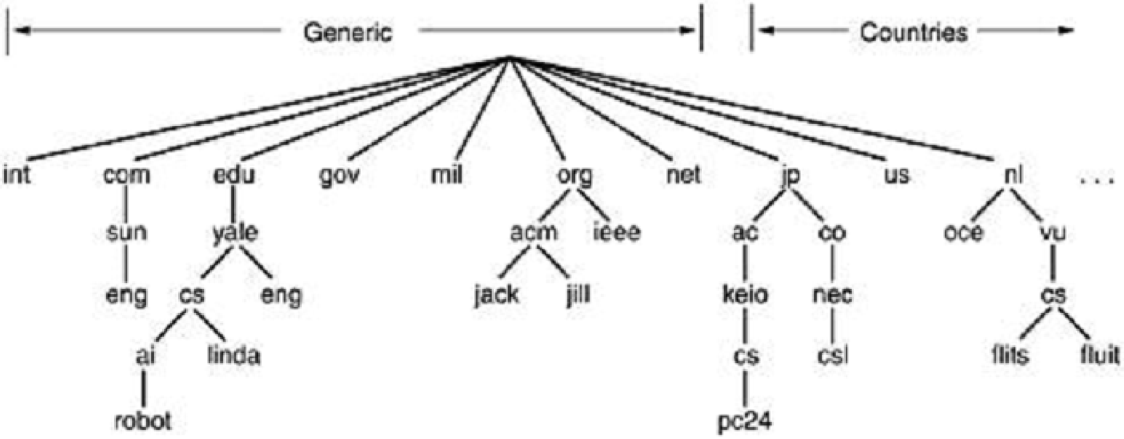


Figure 17.2: A Portion of the Internet Domain Name Spice

The top-level domains come in two flavors: generic and countries. The generic domains are corn (commercial), edu (educational institutions), goy (the U.S. federal government), mil (certain international organizations) mil (the U.S. armed forces), net (network providers), and org (non-profit organizations). The country domains include one entry for every country, as defined in ISO 3166.

Each domain is named by the path upward from it to the (unnamed) root. The components are separated by periods (pronounced “dot”). Thus, Sun Microsystems engineering department might be eng.sun.com rather than a UNIX-style name such as /com/sun/eng.

Absolute and Relative Domain Names:

Domain names can be either absolute or relative. An absolute domain name ends with a period (e.g., eng.sun.com) whereas a relative one does not. Relative names have to be interpreted in some context to uniquely determine their true meaning. In both cases, a named domain refers to a specific node in the tree and all the nodes under it.

Domain names are case insensitive, so edu and EDU mean the same thing. Component names can be up to 63characters long, and full path names mu not exceed 255 characters.

In principle, domains can be inserted into the tree in two different ways. For example, cs.yale.edu could equally well be listed under the country domain asçs.yale.ct.us.

Resource Records:

The ‘name servers’ that together implement the DNS distributed database, store resource records (RR)’ for the hostname to IP address mapping. Each DNS reply message carries one or more resource records.

For a single host, the most common resource record is just its IP address, but many other kinds of resource records also exist. When a resolver gives a domain name to DNS, it gets back the resource records associated with that name. Thus the real function of DNS is to map domain names onto resource records.

A resource record is a five-tuple. Its format is as follows.

Domain_name Time_to_live Type Class Value

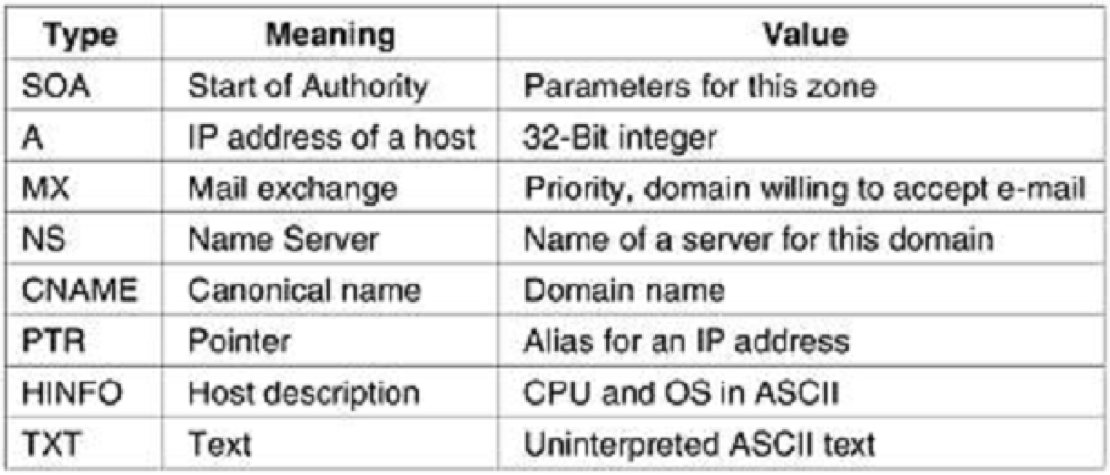
(i) The Domain_name tells the domain to which this record applies. Normally, many records exist for each domain and each copy of the database holds information about multiple domains. The field is thus the primary search key used to satisfy queries.

(ii) The Time_to_live field gives an indication of the stability of record. Information that is highly stable is assigned a large value. Such as864OO (the number of seconds in I day). Information that is highly volatile is assigned a small value, such as 60 (1 minute).

(iii) The type field tells the record type, as listed in the table below.

(iv) The fourth field of every resource record is the Class. For Internet information, it is always in. For non Internet information, other codes can be used.

(v) Value field, can be a number, a domain name, or an ASCII string. The semantics depend on the records type.



Type	Meaning	Value
SOA	Start of Authority	Parameters for this zone
A	IP address of a host	32-Bit integer
MX	Mail exchange	Priority, domain willing to accept e-mail
NS	Name Server	Name of a server for this domain
CNAME	Canonical name	Domain name
PTR	Pointer	Alias for an IP address
HINFO	Host description	CPU and OS in ASCII
TXT	Text	Uninterpreted ASCII text

The principal DNS resource record types for IPv4.

18. In e-mail system, where the e-mail messages are stored and why?

E-mail messages are stored in the user's private electronic mailbox. A mailbox refers to a local hard drive component, a special file associated with permission restrictions so that only the owner i.e., the authorized user may have the capability of accessing it. The messages are stored until the recipient checks their electronic mailboxes (i.e. opens and reads them). Thus, the user should check the electronic mailbox regularly. However, most of the systems provide an alert whenever a mail is received. After thee-mail message has been read. The user can store it (in the form of a text file), reply to it, forward it (to the other users), delete it copy it or take a print of it. Since, mailboxes are not very stable, the e-mail message can be saved by copying it to a file or a document.

Q19. Describe about FTAM services.

FTAM (File Transfer Access and Management):

FTAM is an ISO application protocol which performs the following operations on files.

1. File transfer

2. File access

3. File modification

4. File management

Different systems have differential storage mechanisms.

For example:

In Unix, a file is stored as a sequence of characters whereas in IBM VMS environment, a file is stored as a collection of records. Thus, file organization is dependent on host operating system.

FTAM helps the users in accessing files on diverse systems provided that they have compatible implementations

FTAM:

In FTAM system, the server maintains the user’s connection oriented information, session information. The FTAM client requests the server for a session. Then the file transfer takes place after establishment of the session.

FTAM uses the concept of virtual file store that provides a common view of files.

Virtual Files and File stores:

These are used to make interaction possible among different file systems. A virtual file store is a model which is n-implementation-specific. It is used as an intermediary for transferring, accessing and managing files and databases.

A virtual file is asymmetrically accessed in FTAM i.e., every transaction ispossb1e only in The presence of an initiator and a responder. Initiator is the one who requests for the services (like file transfer, access and management) from the responder which allows the initiator to use the virtual file model it instead of the real file. This model is a software designed by the responder irrespective of hardware and operating system used. This model is also helpful in creating a separation between the file (stored in same storage system), which is accessed both by the initiator and other users.

Attribute and Content:

Virtual file store is created based on attributes and content. Attributes are nothing but a set of properties or security measures. They are used to control the information as well as access to the information. The two types of attributes are per-content, related to the contents of files and per-access, related to security measure that control file access.

The following are the service classes that FTAM provides.

1. Transfer Service Class:

This service class involves the concept of file exchange. It supports exchange of complete files as well as parts of files. The file transfers are very simple with single operations and a very less number of interactions among different files.

2. Access Service Class:

This service class provide the initiator with rights to performs various operations on either the whole file or the individual data units called FADUs i.e., File Access Data Units.

3. Management Service Class:

This service class deals wt the control mechanism over virtual file store. Such mechanism allows the user toper form various operations like rating or deleting files, reading, modifying attributes of a file.

4 The Transfer and Management Service Class:

This class provides the combined functionalities of both the transfer class and the management service class, so that it can provide support for navigation of directories and implement simple functions.

Q20. Write the significance of syntax conversion.

Syntax Conversion:

Syntax conversion is an important function carried out in the presentation layer. It is basically a process of converting the syntax of data received from higher layer (i.e., application layer) into a standar4 format that can be easily understood by all the receiving layers. The advantage of performing syntax conversion is that it enables a smooth data communication between different OSI layers. (Which have their own syntax). While the conversion of syntax is being performed, presentation layer ensures that the semantics of messages remain unaltered.
Let us consider an example wherein two systems (that follow two different syntax) are communicating with each other, one system stores data in big-endian representation and the other stores data in little endian representation.

In order to manage the communication between these two systems the best way is to convert data into a “universal” format that is understood by both the systems. The advantage of using such data conversion approach is that it is very extensible i.e., whenever a new system with different data format is added then instead of understanding the different format used by the other systems the newly added system need to understand the way of converting data to and from the universal format.

Q21. Describe the salient features of multimedia. Also explain the applications of multimedia.

Multimedia:

Multimedia is basically a media that makes use of combination of various content forms such as video, images, animation etc. Usually computerized and electronic devices utilize multimedia for the purpose of recording and playing games, displaying at accessing data. Multimedia is different from fixed media, because the form or even include the audio content. Multimedia can be classified into two categories based on navigational control.

(i) Linear Multi media:

The content of this media does not require any navigation control for example: cinema presentation.

(ii) Non-linear Multimedia:

The content of non-linear multimedia enables user interactivity due to which the user is sole responsible for controlling the progress of the content, for example: computer games, hypermedia. Salient features of Multimedia

a) Multimedia Presentation:

A presentation that makes use of multimedia is called multimedia presentation, this presentation is considered as me of the significant feature of multimedia. These presentation can be delivered by a person live on the stage or by laying a recorded content in a media player or by projecting the content on a screen.

b) Digital on-line Multimedia:

The content of this media either be downloaded or streamed (streaming multimedia can either be live or on demand). However this form of on-line multimedia is transforming as object oriented and data driver. This transformation facilitates applications to support end user innovation and even enables personalization on different content forms.

c) Broadcast Multimedia:

This form of multimedia presentation can be live or recorded. These broadcasts and recordings is done by employing electronic media technology which can either be in digital or analog format multimedia games and simulations can be used globally in a network, locally on a desktop, game system or simulator and on physical environment quipped with special effects.

Applications of Multimedia:

There are many areas where multimedia is applicable. Some of these areas include,

Entertainment Industry:

In recent years, the massive use of multimedia in the entertainment industry is witnessed. Multimedia is utilized in this industry for playing interactive games and for developing affirmation and special effects in a movie.

Commercial Purpose:

Multimedia can be used innovative presentations for advertisements and by creating advanced multimedia presentations for selling ideas and liven up training.

Industrial Sector:

In the industrial sector, use of multimedia is very much useful in providing information to workers, stakeholders and co-workers and also in providing training to employees.

Education Purpose:

In the field of education the use of multimedia can be seen in development of computer based training courses encyclopedia and Almanaus.

Medicine Field:

Multimedia is used to develop a virtual surgery that helps the doctors o gédié insight view of human body and also to develop a presentation that shows the effects of viral and bacterial infections on human body.

Mathematical Scientific Research:

The most important use of multimedia in this field is modeling and simulation.

Document Imaging:

The multimedia is used in conversion of hard copy image to digital image.

In addition to the above fields, the most emerging application of multimedia is virtual reality. Virtual reality is also known as artificial intelligence where in artificial environment (that appears real to the users) is created with the help of specialized software and hardware.

Q22. Write short notes on data compression and transport services.

Transport Services:

The main objective of transport layer is to provide services that are reliable, efficient and cost-effective. These services are processed in the application layer. In order to achieve the objective, the transport layer uses the services that are provided by its lower layer i.e., network layer. The services are accessed by the software or hardware known as transport entity, which is stored in a library package bound, an operating system kernel, a different user process or on the network interface card.

Similar to the network service, the transport service is also divided into two types i.e., connection-oriented transport service and connectionless transport service. Though, the functionalities of these layers are similar, both of them use separate services because the code of transport layer is executed on the user's machine and the code of network layer is executed on routers operated by the carrier.

Due to the presence of transport layer, the transport services are considered as highly-reliable services when compared to the underlying network service. The transport layer even detects and compensates the loss of packets during transmission.