UNIT-IV UPPER LAYERS: -

Session Layer Protocols: Dialog Management, Synchronization.
Presentation layer functions: translation, encryption, compression.
Cryptography : substitution and Transposition Ciphers,
Data Encryption standards (DES) , DES Chaining, Breaking DES, Public Key cryptography, Authentication protocols, Different compression coding techniques.
Application layer protocols & services : Email, World Wide Web, file transfer protocol, remote file server, internet telephony & chatting.

Session Layer Protocols:

The **session layer** is **layer 5** of the seven-layer OSI model of computer networking.

The session layer provides the mechanism for opening, closing and managing a session between end-user application processes, i.e., a semi-permanent dialogue. Communication sessions consist of requests and responses that occur between applications. Session-layer services are commonly used in application environments that make use of remote procedure calls (RPCs).

An example of a session-layer protocol is the OSI protocol suite session-layer protocol, also known as X.235 or ISO 8327. In case of a connection loss this protocol may try to recover the connection. If a connection is not used for a long period, the session-layer protocol may close it and re-open it. It provides for either full duplex or half-duplex operation and provides synchronization points in the stream of exchanged messages.

Other examples of session layer implementations include Zone Information Protocol (ZIP) – the AppleTalk protocol that coordinates the name binding process, and Session Control Protocol (SCP) – the DECnet Phase IV session-layer protocol.

Within the service layering semantics of the OSI network architecture, the session layer responds to service requests from the presentation layer and issues service requests to the transport layer.

Dialog Management

There are many different points of view and techniques for achieving application check pointing. Depending on the specific implementation, a tool can be classified as having several properties:

Amount of state saved: This property refers to the abstraction level used by the technique to analyze an application. It can range from seeing each application as a black box, hence storing all application data, to selecting specific relevant cores of data in order to achieve a more efficient and portable operation.

Automatization level: Depending on the effort needed to achieve fault tolerance through the use of a specific checkpointing solution.

Portability: Whether or not the saved state can be used on different machines to restart the application.

System architecture: How is the check pointing technique implemented: inside a library, by the compiler or at operating system level.

Each design decision made affects the properties and efficiency of the final product. For instance, deciding to store the entire application state will allow for a more straightforward implementation, since no analysis of the application will be needed, but it will deny the portability of the generated state files, due to a number of non-portable structures (such as application stack or heap) being stored along with application data.

Synchronization

synchronization refers to one of two distinct but related concepts: synchronization of processes, and synchronization of data. **Process synchronization** refers to the idea that multiple processes are to join up or handshake at a certain point, so as to reach an agreement or commit to a certain sequence of action. **Data synchronization** refers to the idea of keeping multiple copies of a dataset in coherence with one another, or to maintain data integrity. Process synchronization primitives are commonly used to implement data synchronization.

Authentication is the act of confirming the truth of an attribute of a datum or entity. This might involve confirming the identity of a person or software program, tracing the origins of an artifact, ensuring that a product is what its packaging and labeling claims to be.

Presentation layer functions:

Translation

Data conversion is the conversion of computer data from one format to another. Throughout a computer environment, data is encoded in a variety of ways. For example, computer hardware is built on the basis of certain standards, which requires that data contains, for example, parity bit checks. Similarly, the operating system is predicated on certain standards for data and file handling. Furthermore, each computer program handles data in a different manner. Whenever any one of these variable is changed, data must be converted in some way before it can be used by a different computer, operating system or program. Even different versions of these elements usually involve different data structures. For example, the changing of bits from one format to another, usually for the purpose of application interoperability or of capability of using new features, is merely a data conversion. Data conversions may as simple as the conversion of a text file from one character encoding system to another; or more complex, such as the conversion of office file formats, or the conversion of image and audio file formats.

Encryption

In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The result of the process is encrypted information (in cryptography, referred to as ciphertext). The reverse process, i.e., to make the encrypted information readable again, is referred to as decryption (i.e., to make it unencrypted).

Compression

In computer science and information theory, **data compression**, **source coding** or **bit-rate reduction** involves encoding information using fewer bits than the original representation. Compression can be either lossy or lossless. Lossless compression reduces bits by identifying and eliminating statistical redundancy. No information is lost in lossless compression. Lossy compression reduces bits by identifying marginally important information and removing it.

Compression is useful because it helps reduce the consumption of resources such as data space or transmission capacity. Because compressed data must be decompressed to be used, this extra processing imposes computational or other costs through decompression. For instance, a compression scheme for video may require expensive hardware for the video to be decompressed fast enough to be viewed as it is being decompressed, and the option to decompress the video in full before watching it may be inconvenient or require additional storage. The design of data compression schemes involve trade-offs among various factors, including the degree of compression, the amount of distortion introduced (*e.g.*, when using lossy data compression), and the computational resources required to compress and uncompress the data.

Cryptography :

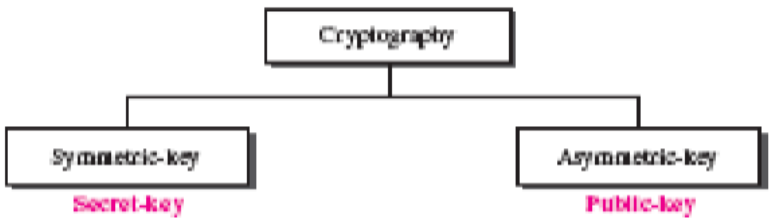
- Components of Cryptography
- Plain text
- Cipher text
- Encryption
- Decryption

Cipher
An algorithm for transforming an intelligible message into unintelligible by transposition and/or substitution
Key
Some critical information used by the cipher, known only to the sender & receiver
Encipher (encode)
The process of converting plaintext to ciphertext
Decipher (decode)
The process of converting ciphertext back into plaintext
Cryptanalysis
The study of principles and methods of transforming an unintelligible message back into an intelligible message *without* knowledge of the key. Also called **codebreaking**
Cryptology
Both cryptography and cryptanalysis
Code
An algorithm for transforming an intelligible message into an unintelligible one using a code-book

Two basic components of classical ciphers:
Substitution: letters are replaced by other letters
Transposition: letters are arranged in a different order
These ciphers may be:
Monoalphabetic: only one substitution/ transposition is
used, or
Polyalphabetic:where several substitutions/transpositions are used
Product cipher:
several ciphers concatenated together

Keys

- To encrypt a message, we need an encryption algorithm, an encryption key & the plain text. These creates the cipher text.
- To decrypt a message, we need an decryption algorithm, an decryption key & the cipher text. These creates the plain text.
- In cryptography, the encryption/decryption algorithms are public but the keys are secret.
- We can divide all the cryptography algorithms into two categories:



Cryptography (or "hidden, secret"; and *graphein*, "writing", or "study") respectively is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about

constructing and analyzing protocols that overcome the influence of adversarie and which are related to various aspects in information security such as data confidentiality, data integrity, and authentication.Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

Substitution Ciphers:- In cryptography, a **substitution cipher** is a method of encryption by which units of plaintext are replaced with ciphertext, according to a regular system; the "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing an inverse substitution.

Substitution ciphers can be compared with transposition ciphers. In a transposition cipher, the units of the plaintext are rearranged in a different and usually quite complex order, but the units themselves are left unchanged. By contrast, in a substitution cipher, the units of the plaintext are retained in the same sequence in the ciphertext, but the units themselves are altered.

There are a number of different types of substitution cipher. If the cipher operates on single letters, it is termed a **simple substitution cipher**; a cipher that operates on larger groups of letters is termed **polygraphic**. A **monoalphabetic cipher** uses fixed substitution over the entire message, whereas a **polyalphabetic cipher** uses a number of substitutions at different positions in the message, where a unit from the plaintext is mapped to one of several possibilities in the ciphertext and vice versa.

Transposition Ciphers:-

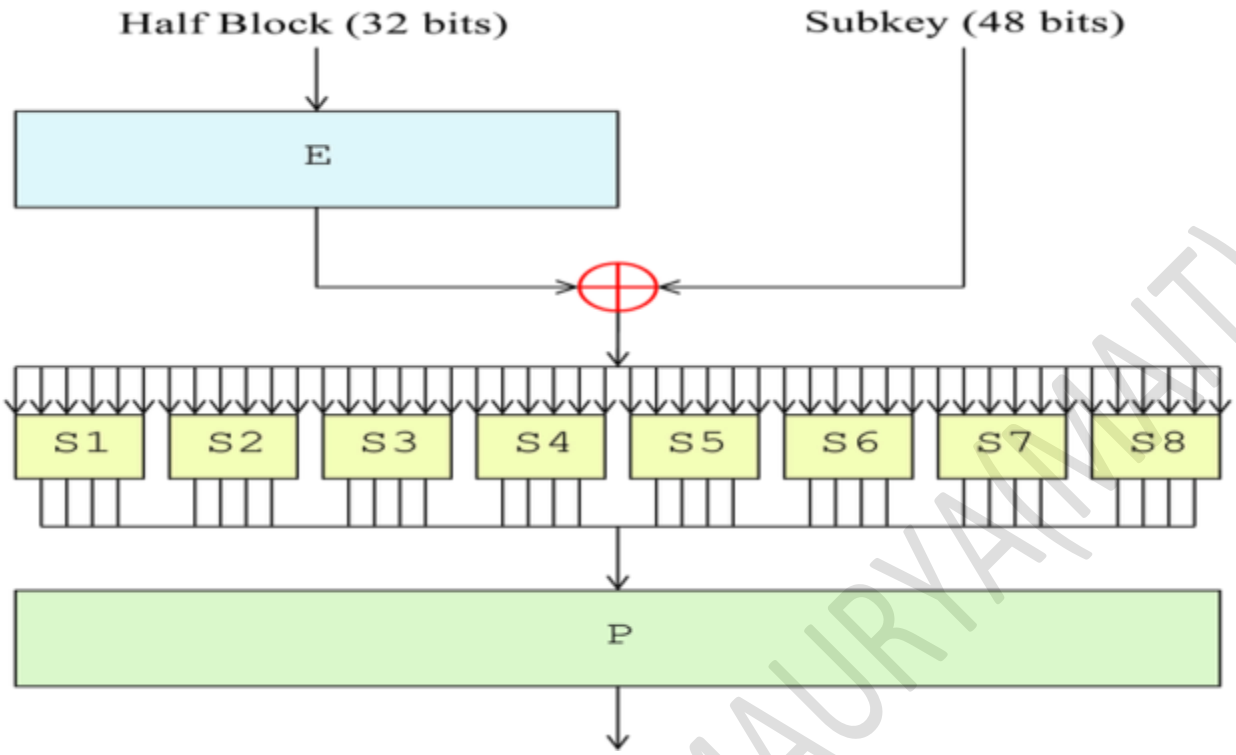
In cryptography, a **transposition cipher** is a method of encryption by which the positions held by units of plaintext (which are commonly characters or groups of characters) are shifted according to a regular system, so that the ciphertext constitutes a permutation of the plaintext. That is, the order of the units is changed. Mathematically a bijective function is used on the characters' positions to encrypt and an inverse function to decrypt.

Data Encryption standards (DES)

The **Data Encryption Standard** is a previously predominant algorithm for the encryption of electronic data. It was highly influential in the advancement of modern cryptography in the academic world. Developed in the early 1970s at IBM and based on an earlier design by Horst Feistel, the algorithm was submitted to the National Bureau of Standards (NBS) following the agency's invitation to propose a candidate for the protection of sensitive, unclassified electronic government data. In 1976, after consultation with the National Security Agency (NSA), the NBS eventually selected a slightly modified version, which was published as an official Federal Information Processing Standard (FIPS) for the United States in 1977. The publication of an NSA-approved encryption standard simultaneously resulted in its quick international adoption and widespread academic scrutiny. Controversies arose out of classified design elements, a relatively short key length of the symmetric-key block cipher design, and the involvement of the NSA, nourishing suspicions about a backdoor. While these suspicions eventually have turned out to be unfounded, the intense academic scrutiny the algorithm received over time led to the modern understanding of block ciphers and their cryptanalysis.

DES is now considered to be insecure for many applications. This is chiefly due to the 56-bit key size being too small; in January, 1999, distributed.net and the Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes. There are also some analytical results which demonstrate theoretical weaknesses in the cipher, although they are infeasible to mount in practice. The algorithm is believed to be practically secure in the form of Triple DES, although there are theoretical attacks. In recent years, the cipher has been superseded by the Advanced Encryption Standard (AES). Furthermore, DES has been withdrawn as a standard by the National Institute of Standards and Technology (formerly the National Bureau of Standards).

Some documentation makes a distinction between DES as a standard and DES as an algorithm, referring to the algorithm as the **DEA** (**Data Encryption Algorithm**).



DES Encryption Operation Modes

DES encryption algorithm defines how a single 64-bit plaintext block can be encrypted. It does not define how a real plaintext message with an arbitrary number of bytes should be padded and arranged into 64-bit input blocks for the encryption process. It does not define how one input block should be coupled with other blocks from the same original plaintext message to improve the encryption strength.

(FIPS) Federal Information Processing Standards Publication 81 published in 1980 provided the following block encryption operation modes to address how blocks of the same plaintext message should be coupled:

- ECB - Electronic Code Book operation mode.
- CBC - Cipher Block Chaining operation mode.
- CFB - Cipher Feedback operation mode
- OFB - Output Feedback operation mode

Public Key cryptography

Public-key cryptography refers to a cryptographic system requiring two separate keys, one to lock or encrypt the plaintext, and one to unlock or decrypt the cyphertext. Neither key will do both functions. One of these keys

is published or public and the other is kept private. If the lock/encryption key is the one published then the system enables private communication from the public to the unlocking key's owner. If the unlock/decryption key is the one published then the system serves as a signature verifier of documents locked by the owner of the private key. Although in this latter case, since encrypting the entire message is relatively expensive computationally, in practice just a hash of the message is encrypted for signature verification purposes.

Because this cryptographic approach uses asymmetric key algorithms such as RSA its more general name is "asymmetric key cryptography". Some of these algorithms have the public key/private key property---that is, neither key is derivable from knowledge of the other---but not all asymmetric key algorithms have this property. Those with this property are particularly useful and have been widely deployed, and are the source of the commonly used name.
Although unrelated, **the two parts of the key pair are mathematically linked**. The public key is used to transform a message into an unreadable form, decryptable only by using the (different but matching) private key. By publishing the public key, the key producer empowers anyone who gets a copy of the public key to produce messages only s/he can read—because only the key producer has a copy of the private key (required for decryption). When someone wants to send a secure message to the creator of those keys, the sender encrypts it (i.e., transforms it into an unreadable form) using the intended recipient's public key; to decrypt the message, the recipient uses the private key. No one else, including the sender, can do so.

Thus, unlike symmetric key algorithms, a public key algorithm does not require a secure initial exchange of one, or more, secret keys between the sender and receiver. These algorithms work in such a way that, while it is easy for the intended recipient to generate the public and private keys and to decrypt the message using the private key, and while it is easy for the sender to encrypt the message using the public key, it is extremely difficult for anyone to figure out the private key based on their knowledge of the public key. They are based on mathematical relationships (the most notable ones being the integer factorization and discrete logarithm problems) that have no efficient solution.

The use of these algorithms also allows authenticity of a message to be checked by creating a digital signature of a message using the private key, which can be verified using the public key.

Public key cryptography is a fundamental and widely used technology. It is an approach used by many cryptographic algorithms and cryptosystems. It underpins such Internet standards as Transport Layer Security (TLS) (successor to SSL), PGP, and GPG.

The distinguishing technique used in public key cryptography is the use of asymmetric key algorithms, where the key used to encrypt a message is not the same as the key used to decrypt it. Each user has a pair of cryptographic keys — a **public encryption key** and a **private decryption key**. The publicly available encrypting-key is widely distributed, while the private decrypting-key is known only to the recipient. Messages are encrypted with the recipient's public key and can be decrypted *only* with the corresponding private key. The keys are related mathematically, but parameters are chosen so that determining the private key from the public key is prohibitively expensive.

The two main branches of public key cryptography are:

- Public key encryption: a message encrypted with a recipient's public key cannot be decrypted by anyone except a possessor of the matching private key — it is presumed that this will be the owner of that key and the person associated with the public key used. This is used for confidentiality.

- Digital signatures: a message signed with a sender's private key can be verified by anyone who has access to the sender's public key, thereby proving that the sender had access to the private key (and therefore is likely to be the person associated with the public key used), and the part of the message that has not been tampered with.

Authentication protocols

An **authentication protocol** is a type of cryptographic protocol with the purpose of authenticating entities wishing to communicate securely.

A cryptographic protocol usually incorporates at least some of these aspects:

- Key agreement or establishment
- Entity authentication
- Symmetric encryption and message authentication material construction
- Secured application-level data transport
- Non-repudiation methods

There are many different authentication protocols such as:

- AKA
- CAVE-based_authentication
- Challenge-handshake authentication protocol (CHAP)
- CRAM-MD5
- Diameter
- Extensible Authentication Protocol (EAP)
- Host Identity Protocol (HIP)
- Kerberos
- MS-CHAP and MS-CHAPv2 variants of CHAP
- LAN Manager
- NTLM, also known as NT LAN Manager
- Password-authenticated key agreement protocols
- Password Authentication Protocol (PAP)
- Protected Extensible Authentication Protocol (PEAP)
- RADIUS
- Secure Remote Password protocol (SRP)
- TACACS and TACACS+
- RFID-Authentication Protocols
- Woo Lam 92 (protocol)

Cryptanalysis

Cryptanalysis is the art of defeating cryptographic security systems, and gaining access to the contents of encrypted messages, without being given the cryptographic key.

In addition to mathematical analysis of cryptographic algorithms, cryptanalysis also includes the study of side-channel attacks that do not target weaknesses in the cryptographic algorithms themselves, but instead exploit weaknesses in their physical implementation or software implementation.

Application layer protocols & services :

The Internet protocol suite (TCP/IP) and the Open Systems Interconnection model (OSI model) of computer networking each specify a group of protocols and methods identified by the name **application layer**.

In TCP/IP, the application layer contains all protocols and methods that fall into the realm of process-to-process communications across an Internet Protocol (IP) network. Application layer methods use the underlying transport layer protocols to establish host-to-host connections.

In the OSI model, the definition of its application layer is narrower in scope, explicitly distinguishing additional functionality above the transport layer at two additional levels, the session layer and the presentation layer. OSI specifies strict modular separation of functionality at these layers and provides protocol implementations for each layer.

TCP/IP protocols

The following protocols are explicitly mentioned in RFC 1123 (1989), describing the application layer of the Internet protocol suite

- Remote login category
  - Telnet
- File transfer category
  - FTP
  - TFTP
- Electronic mail category
  - SMTP
  - IMAP
  - POP
- Support services category
  - DNS
  - RARP
  - BOOTP
  - SNMP
  - CMOT

Email

Electronic mail, commonly known as email or e-mail, is a method of exchanging digital messages from an author to one or more recipients. Modern email operates across the Internet or other computer networks. Some early email systems required that the author and the recipient both be online at the same time, in common with instant messaging. Today's email systems are based on a store-and-forward model. Email servers accept, forward, deliver and store messages. Neither the

users nor their computers are required to be online simultaneously; they need connect only briefly, typically to an email server, for as long as it takes to send or receive messages.

An email message consists of three components, the message envelope, the message header, and the message body. The message header contains control information, including, minimally, an originator's email address and one or more recipient addresses. Usually descriptive information is also added, such as a subject header field and a message submission date/time stamp.

World Wide Web

The World Wide Web (abbreviated as WWW or W3, commonly known as the Web, and nickname: "information superhighway") is a system of interlinked hypertext documents accessed via the Internet. With a web browser, one can view web pages that may contain text, images, videos, and other multimedia, and navigate between them via hyperlinks.

Using concepts from his earlier hypertext systems like ENQUIRE, British engineer and computer scientist Sir Tim Berners-Lee, now Director of the World Wide Web Consortium (W3C), wrote a proposal in March 1989 for what would eventually become the World Wide Web.At CERN, a European research organization near Geneva situated on Swiss and French soil,Berners-Lee and Belgian computer scientist Robert Cailliau proposed in 1990 to use hypertext "... to link and access information of various kinds as a web of nodes in which the user can browse at will",and they publicly introduced the project in December.
Berners-Lee's breakthrough was to marry hypertext to the Internet. In his book Weaving The Web, he explains that he had repeatedly suggested that a marriage between the two technologies was possible to members of both technical communities, but when no one took up his invitation, he finally tackled the project himself. In the process, he developed three essential technologies:
. a system of globally unique identifiers for resources on the Web and elsewhere, the Universal Document Identifier (UDI), later known as Uniform Resource Locator (URL) and Uniform Resource Identifier (URI);
. the publishing language HyperText Markup Language (HTML);
. the Hypertext Transfer Protocol (HTTP)

The terms Internet and World Wide Web are often used in everyday speech without much distinction. However, the Internet and the World Wide Web are not one and the same. The Internet is a global system of interconnected computer networks. In contrast, the Web is one of the services that runs on the Internet. It is a collection of text documents and other resources, linked by hyperlinks and URLs, usually accessed by web browsers from web servers. In short, the Web can be thought of as an application "running" on the Internet.

file transfer protocol

File Transfer Protocol (FTP) is a standard network protocol used to transfer files from one host to another host over a TCP-based network, such as the Internet. It is often used to upload web pages and other documents from a private development machine to a public web-hosting server. FTP is built on a client-server architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves using a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that hides (encrypts) your username and password, as well as encrypts the content, you can try using a client that uses SSH File Transfer Protocol.

The first FTP client applications were interactive command-line tools, implementing standard commands and syntax. Graphical user interfaces have since been developed for many of the popular desktop operating systems in use today, including general web design programs like Microsoft Expression Web, and specialist FTP clients such as CuteFTP.

remote file server

Remote File Sharing (RFS) was a distributed file system developed by AT&T in the 1980s. It was first delivered with UNIX System V Release 3 (SVR3).

Compared to NFS it made quite different design decisions. Instead of focusing on reliable operation in the presence of failures, it focused on preserving UNIX file system semantics across the network. Unlike NFS (before version 4), the RFS server maintains state to keep track of how many times a file has been opened, if any process has locked the file, etc. RFS was a product from Bell Laboratories. Features:

Provides complete UNIX/POSIX file semantics. (File locking, etc.)
Allows mounting of devices across the network (e.g. /dev/cdrom can be accessed remotely)
Transparent access to files. Users needn't know where a file is located.

internet telephony

Voice over IP (VoIP) commonly refers to the communication protocols, technologies, methodologies, and transmission techniques involved in the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. Other terms commonly associated with VoIP are *IP telephony*, *Internet telephony*, *voice over broadband* (VoBB), *broadband telephony*, and *broadband phone*.

Internet telephony refers to communications services —voice, fax, SMS, and/or voice-messaging applications— that are transported via the Internet, rather than the public switched telephone network (PSTN). The steps involved in originating a VoIP telephone call are signaling and media channel setup, digitization of the analog voice signal, encoding, packetization, and transmission as Internet Protocol (IP) packets over a packet-switched network. On the receiving side, similar steps (usually in the reverse order) such as reception of the IP packets, decoding of the packets and digital-to-analog conversion reproduce the original voice stream. Even though IP Telephony and VoIP are terms that are used interchangeably, they are actually different; IP telephony has to do with digital telephony systems that use IP protocols for voice communication, while VoIP is actually a subset of IP Telephony. VoIP is a technology used by IP telephony as a means of transporting phone calls.

chatting.

Online chat may refer to any kind of communication over the Internet, that offers an real-time direct transmission of text-based messages from sender to receiver, hence the delay for visual access to the sent message shall not hamper the flow of communications in any of the directions. Online chat may address point-to-point communications as well as multicast communications from one sender to many receivers and voice and video chat or may be a feature of a Web conferencing service.

Sven Birkerts says

"as new electronic modes of communication provoke similar anxieties amongst critics who express concern that young people are at risk, endangered by a rising tide of information over which the traditional controls of print media and the guardians of knowledge have no control on it".

This person is arguing that the youth of the world may have too much freedom with what they can do or say with the almost endless possibilities that the Internet gives them, and without proper controlling it could very easily get out of hand and change the norm of literacy of the world. In Guy Merchant's journal article Teenagers in Cyberspace: An Investigation of Language Use and Language Change in Internet Chatrooms; he says

"that teenagers and young people are in the leading the movement of change as they take advantage of the possibilities of digital technology, drastically changing the face of literacy in a variety of media through their uses of mobile phone text messages, e-mails, web-pages and on-line chatrooms. This new literacy develops skills that may well be important to the labor market but are currently viewed with suspicion in the media and by educationalists.

If any thing is wrong in this then heartly sorry no responsibility of 100% accuracy

COMPILED BY- AMIT MAURYA C.S.E.6TH SEM 3RD YEAR DR. C. V. RAMAN INSTITUTE OF SCIENCE AND TECHNOLOGY