Unit-4

Security :⇒ Computer Security means to Protect information, it deals with Prevention and detection of Unauthorized actions by User of a Computer.

⇒ in Simple Words Security is defined as "Protecting information System from Unintended access"

⇒ Security of information system refers to Protecting all Components of information system, specifically data, software, hardware and Networks.

⇒ Network Security Measures are Needed to Protect data during their transmission and to guarantee that data transmission are authentic

Network Security Threats :⇒ Any Action that Compromises the Security of information.

1. Passive threats
2. Active threats

① Passive threats :⇒ Sometimes referred to as eavesdropping dropping, involve attempts by an attacker to obtain information relating to Communication.

② Realcase of Message Contents :⇒

⇒ A telephone Conversion, an E-mail Message and a transferred file may Contain sensitive or Confidential information.

⇒ We would like to Prevent the opponent from learning the Content of these transmission

Teacher's Signature.....

Date / /
Page No.

(b) Traffic Analysis :-)

⇒ It is a kind of attack done on encrypted Message.
⇒ the opponent might be able to observe the pattern of such encrypted Message.
⇒ the opponent could determine the location and identity of communicating hosts and could observe the frequency and length of Messages being exchanged.

(2) Active threats :⇒ involve some Modification of the data stream or the creation of a false stream.

(a) masquerade :-)

⇒ It takes place when one entity pretends to be a different entity.
⇒ A masquerade attack usually includes one of the other forms of active attack.
⇒ for e.g. authentication sequences can be captured and replayed after a valid authentication sequences has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by impersonating an entity that has those privileges.

(b) Replay :⇒

⇒ It involves the passive capture of a data unit and its subsequent retransmision to produce an unauthorized effect.

Teacher's Signature.....

Date / /
Page No.

(c) Modification of Message :⇒ it means that some position of a message is altered, or that Message are delayed or rendered, to produce an unauthorized effect.

(d) Denial of services (DoS) :⇒

⇒ A denial of service attack takes Place when the Availability to a resource is intentionally blocked or degrade by an attacker

⇒ In this way the Normal use of Management of Communication facilities is inhibited

⇒ this attack may have a specific target

eg. an entity may suppress all messages directed to a Particular destination.

Security Services :⇒ it is a services that is provided by a Protocol layer of Communicating Open System and that ensures adequate security of the System or of data transfer. it enhances the security of data Processing and transferring

OR

A service that enhances the security of data Processing system and information transfers, A security services makes use of one or more security Mechanism

(1) Confidentiality :⇒

⇒ it Means that the Content of a Message when transmitted across a Network must remain Confidential i.e. Only the intended receiver and no one else should be able to read the Message.

Teacher's Signature.....

⇒ the user; therefore, want to encrypt the message they send so that an eavesdropper on the network will not be able to read the contents of the message.

② Integrity :⇒

⇒ it means the data must reach the destination with any adulteration i.e. exactly as it was sent,
⇒ there must be no changes during transmission, neither accidentally nor maliciously.
⇒ integrity of a message is ensured by attaching a checksum to the message.
⇒ the algorithm for generating the checksum ensures that an intruder cannot alter the checksum or the message.

③ NoN - repudiation :⇒

⇒ it means that a sender must not be able to deny sending a message that it actually sent.
⇒ the burden of proof falls on the receiver.
⇒ it is not only in respect of the ownership of the message; the receiver must prove that the contents of the message are also the same as the sender sent.
⇒ It is achieved by authentication and integrity mechanisms.

④ Authenticity :⇒ Provide Authentication to all the node and base station for utilizing the avilable limited resources. it also ensures that only the authorized node can participant for the communication.

Teacher's Signature.....

Date / /
Page No.

(5) Access Control :⇒ Access Control is the ability to limit and control the access to host systems and application via Communication links. To achieve this, each entity trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual

Security Mechanism :⇒ the various security mechanisms to provide security

(1) Encipherment :⇒ this is hiding or covering of data which provides confidentiality. It is also used to complement other mechanisms to provide other services, cryptography and steganography are used for enciphering

(2) Digital Integrity :⇒ the Data integrity mechanism appends to the data a short check value that has been created by a specific process from the data itself. Data integrity is preserved by comparing check value received to the check value generated.

(3) Digital Signature :⇒ A digital signature is a means by which the sender can electronically sign the data and the receiver can electronically verify the signature.

(4) Authentication Exchange :⇒ in this two entities exchange some message to prove their identity to each other.

Date / /
Page No.

(5) Traffic padding :⇒ Traffic padding means inserting some bogus data into the data traffic to thwart the adversary's attempt to use the traffic analysis

(6) Routing control :⇒ Routing control means selecting and continuously changing different avilable routes between sender and receiver to prevent the opponent from eavesdropping on a particular route.

(7) Notarization :⇒ Notarization means selecting a third trusted party to control the communication between two entities. the receiver can involve ~~the~~ a trusted third party to store the sender request in order to prevent the sender from later denying that she has made a request

(8) Access control :⇒ Access control used methods to prove that a user has access right to the data or resources owned by a system.
Examples of proofs are Password and PIN's

Security Mechanism at Network layer :⇒ Several security machanism has been developed in such a way that they can be developed at a specific layer of the OSI network layer Model

⇒ Security at application layer → Security measures used at this layer are application

Teacher's Signature.....

Date / /
Page No.

specific. Different types of application would need seperate security measures. in order to ensure application layer security, the application Need to be modified

it is considered that designing a cryptographically sound application protocol is very difficult and implementing it properly is ~~very difficult and implementing it pro~~ is even more challenging. Hence, application layer security mechanisms for Protecting Network Communications are preferred to be only standards-based solutions that have been in use for some time.

→ Security at transport layer :⇒ Security measures at this layer can be used to protect the data in a single Communication session between two hosts. the most Common use for transport layer Security protocols is Protecting the HTTP and FTP session traffic. HTTP and FTP are the most Common Protocols used for this purpose.

⇒ Network layer :⇒ Security Measures at this layer can be applied to all applications; thus, they are Not application-specific. All Network Communications between two hosts or Networks can be Protected at this layer without modifying any application, In some environments, Network layer Security Protocol such as internet Protocol security (IPsec) Provides a much better Solution than transport or application layer Controls because of the difficulties in adding Controls to individual applications, However, security Protocols at this layer Provides less Communication flexibility that may be required by some application.

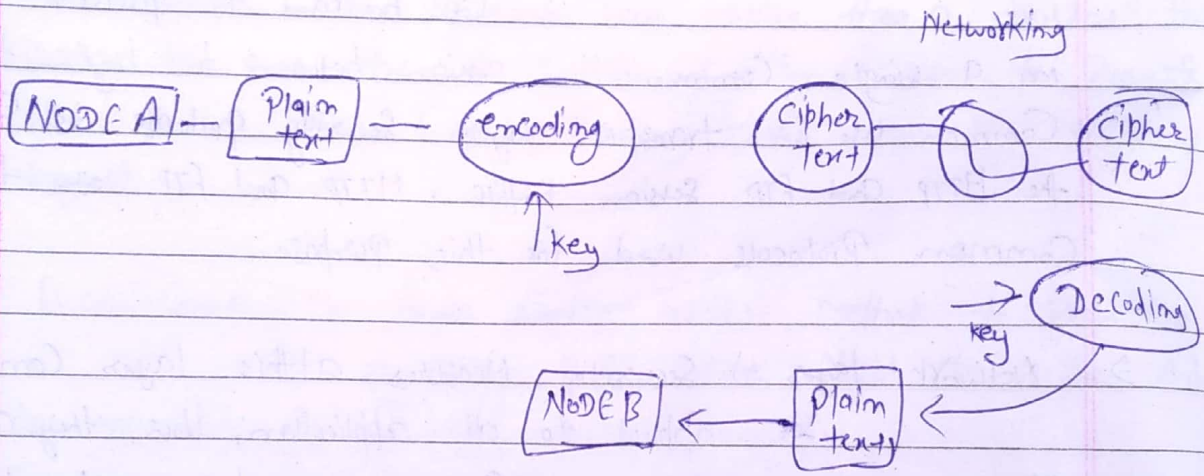
Teacher's Signature

Date / /
Page No.

→ Data Link layer :→ Data link layer in Ethernet Network is highly prone to several attacks.

Common attack are,

ARP spoofing
MAC Flooding
Port stealing
DHCP attack



Plain text :→ Origional Message sent by the text sender

Encoding :→ Proces of Converting plain text into Coded form (encoded form is NON-reading form)

Key :→ A Message is encoded with the help of key

Cipher text :→ An encoded Message which is NON-readable form is known as Cipher text

Teacher's Signature.....

Date / /
Page No.

Decoding :=> Converting encoded Message into plain text (cipher text to plain text Conversion)

Cryptography :=> Proces of encryption and decryption is cryptography (Converting cipher text to plain text or plain text to cipher text).

Cryptology :=> Study of cryptography is known as cryptology

Cryptanalysis :=> a Person who does the cryptography is known as cryptanalysis.

Cryptography :=> Cryptography involves creating written or generated code that allow information to be kept secret. cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data.

Information security uses cryptography on several levels. the information cannot be read without a key to decrypt it. The information maintains its integrity during transit and while being stored. cryptography also aids in nonrepudiation. this means that the sender and the delivery of a message can be verified.

cryptography also allows senders and receivers to authenticate each other through the use of key pairs. there are various types of algorithm for encryption, some common are :-

Teacher's Signature.....

- Secret Key Cryptography (SKC) :⇒ Here only one key is used for both encryption and decryption. this type of encryption is also referred to as Symmetric encryption.

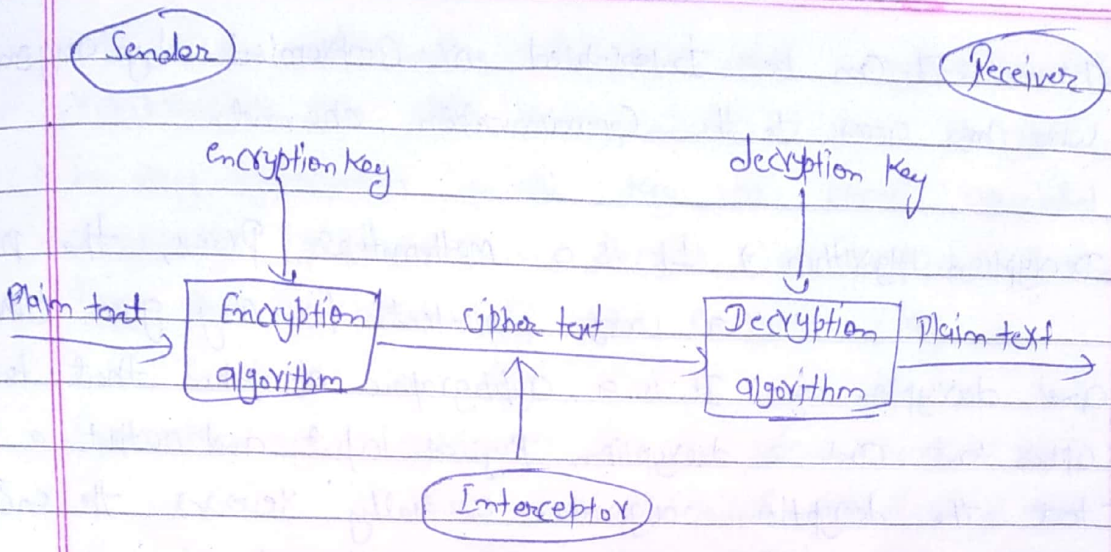
- Public Key Cryptography (PKC) :⇒ Here two key are used. this type of encryption is also called asymmetric encryption. One key is the Public key that anyone can access. the other key is the Private key, and only the owner can access it. the Sender encrypts the information using the receiver's public key. the receiver decrypts the message using his Private key. for non repudiation, the Sender encrypts plain text using a Private key, while the receiver uses the Sender's Public key to decrypt it. thus, the receiver knows who sent it.

- Hash function :⇒ these are different from SKS and PKC. they use no key and are also called one-way encryption. Hash function are mainly used to ensure that a file has remained unchanged.

CryptoSystem :⇒ A CryptoSystem is an implementation of cryptographic technique and their accompanying infrastructure to provide information security services. A CryptoSystem is also referred to as a cipher system

* the digram of simple model of a Cryptosystem that provides Confidentiality to the information being transmitted

Teacher's Signature.....



the illustration shows a Sender who wants to transfer some sensitive data to a receiver in such a way that any party intercepting or eavedropping on the communication channel cannot extract the data.
the objective of this simple cryptosystem is that at the end of the process, only the sender and the receiver will know the plaintext.

Components of a cryptosystem :=>

① Plaintext :=> it is the data to be protected during transmission

② Encryption Algorithm :=> it's a mathematical process that produces a cipher text for any given plaintext and encryption key. it is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.

③ cipher text :=> it is the scrambled version of the plaintext produce by the encryption algorithm using a specific the encryption key. the cipher text is not guarded. It flows on public

Teacher's Signature.....

Date / /
Page No.

channel. It can be intercepted or compromised by anyone who has access to the communication channel.

Decryption Algorithm :⇒ It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a cipher text and a decryption key as input, and outputs a plain-text. the decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.

Encryption key :⇒ It is a value that is known to the sender. the sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.

Decryption key :⇒ It is a value that is known to the receiver. the decryption key is related to the encryption key, but is not always identical to it. the receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

types of cryptosystems :⇒ two types of cryptosystems based on the manner in which encryption decryption is carried out in the same.

1. Symmetric key Encryption / Symmetric ciphers schemes
2. Asymmetric key Encryption / Asymmetric ciphers schemes

Teacher's Signature.....

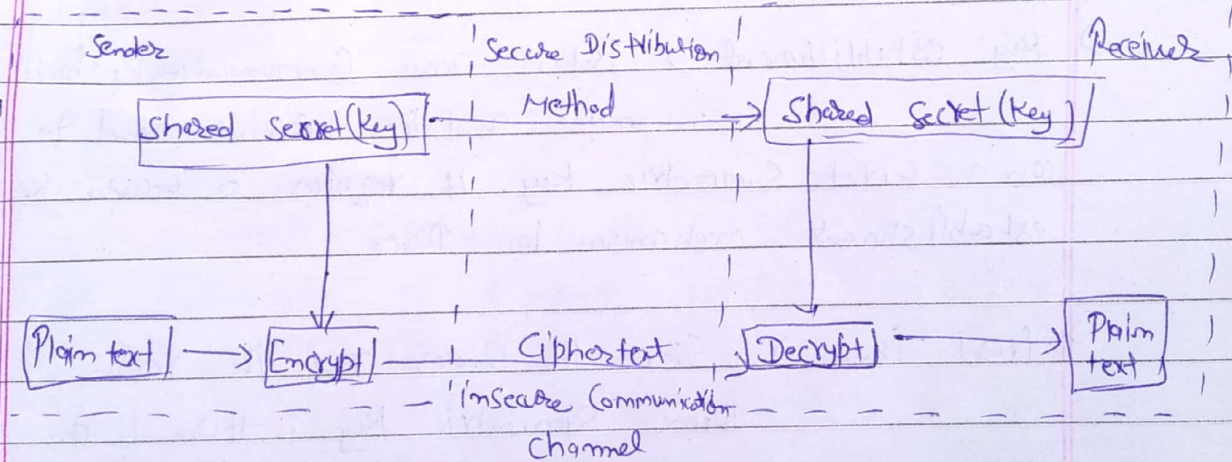
Date / /
Page No.

the main difference between these cryptosystems is the relationship b/w the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. it is practically impossible to decrypt the ciphertext with the key that is unrelated to the encryption key.

Symmetric Key Encryption:=> the encryption process where same keys are used for encrypting and decrypting the information is known as symmetric key encryption.

the study of symmetric cryptosystems is referred to as symmetric cryptography. Symmetric cryptosystem are also sometimes referred to as secret key cryptosystem.

A Example of symmetric key encryption methods are - Digital Encryption Standard (DES), Triple-DES (3DES), IDEA and BLOWFISH



Features of Symmetric key encryption →

→ Person using symmetric key encryption must share a common key prior to exchange of information.

→ Keys are recommended to be changed regularly to prevent any attack on the system.

Teacher's Signature.....

Date / /
Page No.

→ A robust mechanism needs to exist to exchange the key between the communicating parties, As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome.

→ in a group of n people, to enable two-party communication between any two persons, the number of key required for group in $n \times (n-1)/2$

→ Length of key (number of bits) in this encryption is smaller and hence, Process of encryption - decryption is faster than asymmetric key encryption.

→ Processing Power of computer system required to run Symmetric algorithm is less.

Challenges Symmetric Key Cryptosystems

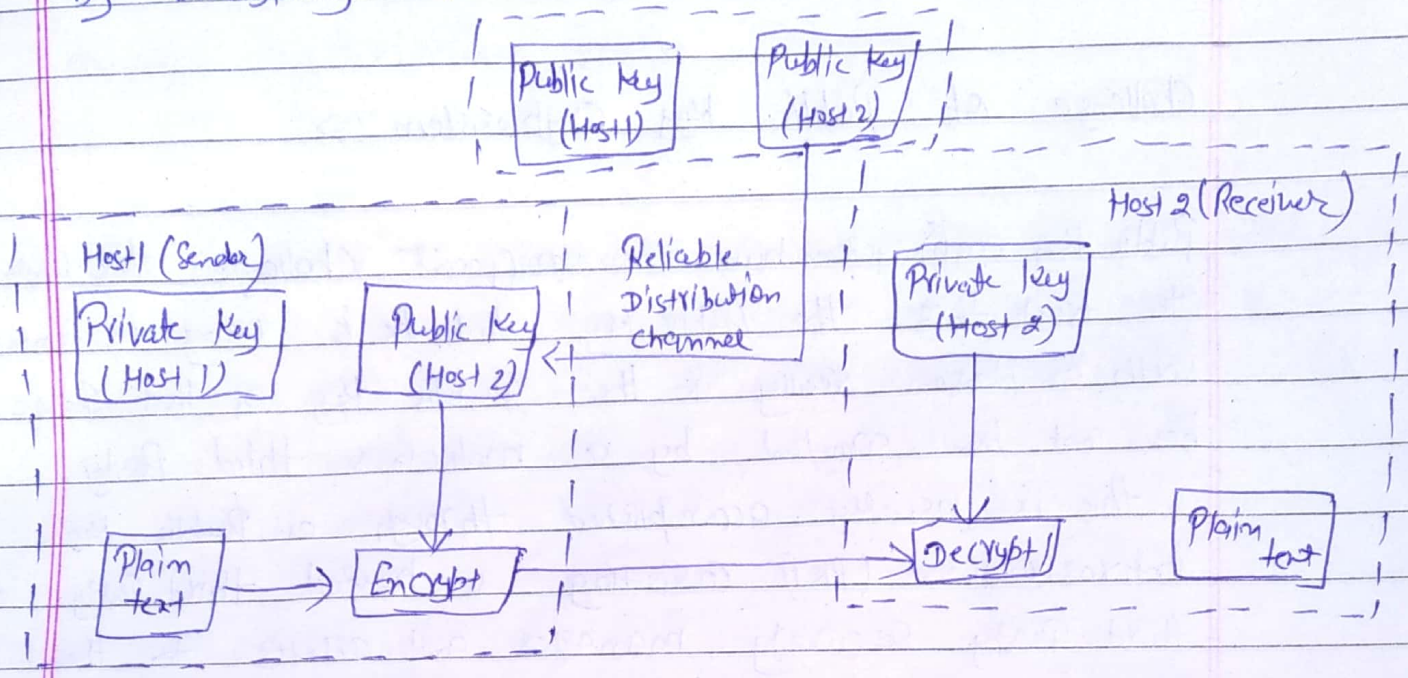
→ Key establishment → Before any communication, both the sender and the receiver need to agree on a secret Symmetric key. It requires a secure key establishment mechanism in place.

→ Trust issue :→ Since the Sender and the receiver use the same Symmetric key, there is an implicit requirement that the Sender and the receiver 'trust' each other for ex., it may happen that the receiver has lost the key to an attacker and the Sender is not informed.

Asymmetric Key Encryption :→ the encryption process where different keys are used for encrypting and decrypting the information is known as

Teacher's Signature.....

Asymmetric Key Encryption - though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting ciphertext is feasible.



Asymmetric Key Encryption to come over the necessity of Pre-shared secret key between communication persons.
the features of the Encryption scheme.

→ Every user in this system needs to have a pair of dissimilar keys, Private Key and Public Key. these key are Mathematically related - when one key is used for encryption, the other can decrypt the ciphertext back to the original Plain text.

→ it requires to put the Public Key in a Public repository and the Private Key as a well guarded secret. Hence, this schema of encryption is also called Public Key encryption.

→ though Public and Private Keys of the user are related, it is computationally not feasible to find one from another. this is a strength of this scheme.

→ length of keys (number of bits) in this encryption is large and hence, the process of encryption - decryption

Teacher's Signature.....

is slower than symmetric key encryption.

→ Processing Power of computer system required to run asymmetric algorithm is higher.

Challenge of Public Key Cryptosystem :=>

Public key cryptosystem have one significant challenge the user needs to trust that the public key that he is using in communication with a person really is the public key of that person and has not been spoofed by a malicious third party.

this is usually accomplished through a Public key infrastructure (PKI) consisting a trusted third party. the third party securely manages and attests to the authenticity of public keys. when the third ~~key~~ ~~is~~ party is requested to provide the public key for any communicating person X, they are trusted to provide the correct public key

Ciphertext :=> ciphertext is encrypted text, plaintext is what we have before encryption, and ciphertext is the encrypted result, the term cipher is sometimes used as a synonym for ciphertext, but it more properly means the method of encryption rather than the result.

Cryptanalysis :=> the art and science of breaking the cipher text is known as Cryptanalysis.

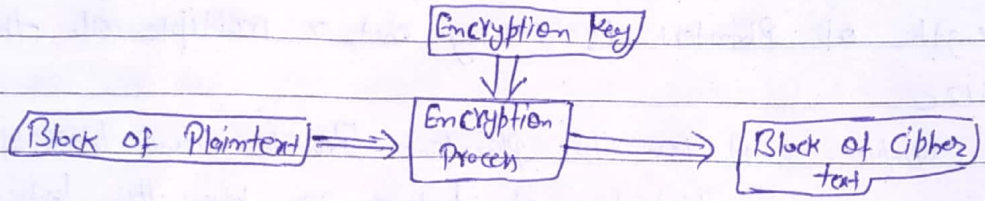
Cryptanalysis is the branch of Cryptography any they both Co-exist, the cryptographic process result in the cipher text

Teacher's Signature.....

Date / /
Page No.

for transmission or storage. It involves the study of cryptographic mechanism with the intention to break them. Cryptanalysis is also used during the design of the new cryptographic technique to test their security strengths.

Block ciphers:⇒ An encryption method that applies a deterministic algorithm along with a symmetric key to encrypt a block of text, rather than encrypting one bit at a time ~~as in stream cipher~~ a block of bit is encrypted



A block cipher takes a block of Plaintext bits and generates a block of ciphertext bits, generally of same size. the size of block is fixed in the given scheme. the choice of block size does not directly affect to the strength of encryption scheme, the strength of cipher depends up on the key length.

Block size:-

→ Avoid very small block size → a block size is m bits. then the possible plaintext bits combinations are then 2^m, if the attacker discovers the plain text blocks corresponding to some previously sent ciphertext blocks, then the attacker can launch a type of 'dictionary attack' by building up a dictionary of plaintext / ciphertext pairs sent using that encryption key. A larger block size makes attack harder as the

Teacher's Signature.....

dictionary needs to be larger

→ Do Not have very large block size → with very large block size, the cipher becomes inefficient to operate. such plaintexts will Need to be padded before being encrypted

→ multiples of 8 bits :⇒ A preferred block size is a multiple of 8 as it is easy for implementation as most Computer Processor handle datas in multiple of 8 bits

Block cipher Process blocks of fixed size (say 64 bits). the length of Plaintext is mostly not a multiple of the block size.

For example :- A 150 - bit plaintext Provides two block of 64 bits each with third block of balance 22 bits. the last blocks of bits needs to be Padded up with redundant information so that the length of the final block equal to block size of the schema. In this example the remaining 22 bits Need to have additional 42 redundant bits added to provide a Complete block. the Process of adding bits to the last block is referred to as padding.

~~Block Cipher Schemes~~

Stream ciphers :⇒ A stream cipher is a symmetric key cipher where Plaintext digits are Combined with a pseudorandom cipher digit stream (key stream). In a stream cipher, each Plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the ciphertext stream. Since encryption of each digit is dependent

Teacher's Signature.....

on the current state of the cipher, it is also known as state cipher. ~~in Practice~~

the pseudorandom keystream is typically generated serially from a random seed value using digit shift registers. the seed value serves as the cryptography key for decrypting the cipher text stream. Stream cipher represents a different approch to symmetric encryption from Block ciphers, Block cipher operates on large block of digit with a fixed, unvarying transformation. this distinction is not always clear-cut: in some modes of operation, a block cipher primitive is used in such a way that it acts effectively as a stream cipher, stream cipher typically execute at a higher speed than block ciphers and have lower hardware complexity. However, stream ciphers can be susceptible to serious security problem if used incorrectly in particular, the same starting state must never be used twice.

⇒ in stream cipher the Plain text is encrypted one bit at a time the decryption also happens one bit at a time.

Steganography :⇒ it is a technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extracted as its destination. the use of steganography can be combined with encryption as an extra space for hidding or Protecting data.

⇒ it can be used to conceal almost any time of digital content, including text, image, video or audio content; the data to be hidden can be hidden inside almost any other type of digital content. the content to be concealed through steganograph - called hidden text is often encrypted before being incorporated into the innocuous-seeming cover text file or data stream, if not encrypted, the hidden text is commonly processed in some way in order to

Teacher's Signature.....

Date / /
Page No.

increase the difficulty of detecting the secret content.

→ Steganography is practiced by those wishing to convey a secret message or code. While there are many legitimate uses for Steganography, malware developers have also been found to ~~be~~ use Steganography to obscure the transmission of malicious code.

Steganography techniques! => in modern digital Steganography, data is first encrypted or obfuscated in some other way and the inserted, using a special algorithm, into data that is part of a particular file format such as JPEG image, audio or video file. the secret message can be embedded into ordinary data files in many different ways. One technique is to hide data in bits that represent the same color pixels repeated in a row in an image file. By applying the encrypted data to this redundant data in some inconspicuous way, the result will be an image file that appears identical to the original image but that has "noise" patterns of regular, unencrypted data.

How Steganography is different from Cryptography ?

Ans Cryptography and Steganography are both methods used to hide or protect secret data, However, they differ in the respect that cryptography makes the data unreadable, or hides the meaning of the data, while Steganography hides the existance of the data.

→ Cryptography is similar to writing a letter in a secret language ! People can read it, but won't understand what it

Teacher's Signature.....

Date / /
Page No.

means, However the existence of a message would be obvious to anyone who sees the letter, and if someone either knows or figures out our secret language, they can be easily read

→ In the same steganography situation, we would hide a letter inside a pair of socks that we would be gifting the intended reciplent of the letter. to whose look like there was nothing more to our gift than the socks. But the intended recipient knows what to look for, and finds the message hidden in them.

Similarly, if two users exchanged media files over the Internet, it would be more difficult to determine whether these files contain hidden messages, than if they were communicating using Cryptography