Security

Security, in information technology (IT), is the defense of digital information and IT assets against internal and external, malicious and accidental threats. This defense includes detection, prevention and response to threats through the use of security policies, software tools and IT services.

Network Security

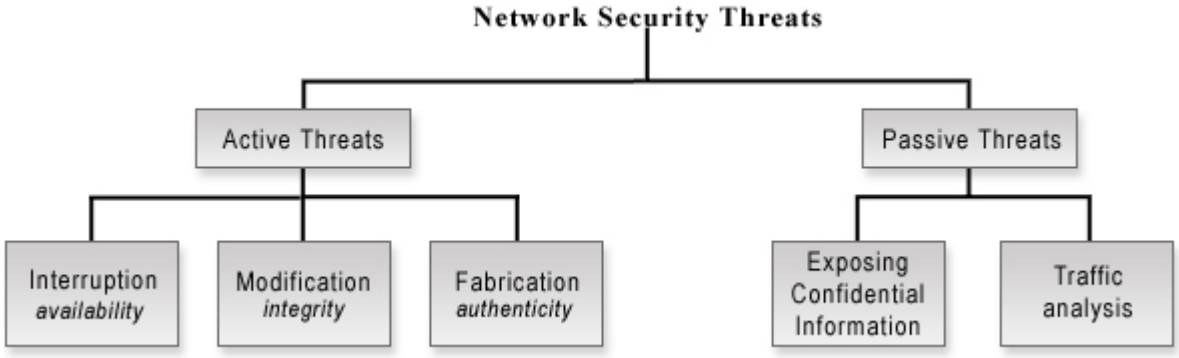
Network security is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading on your network.

Security Threat

Security Threat is defined as a risk that which can potentially harm computer systems and organization. Threat can be anything that can take advantage of a vulnerability to breach security and negatively alter, erase, harm object or objects of interest.

Security Attacks

There are four general categories of attack which are listed below.

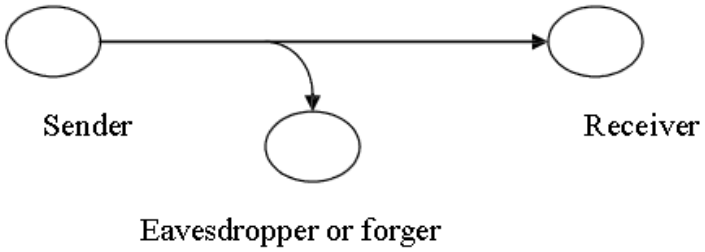


Interruption

An asset of the system is destroyed or becomes unavailable or unusable. This is an attack on availability e.g., destruction of piece of hardware, cutting of a communication line or Disabling of file management system.

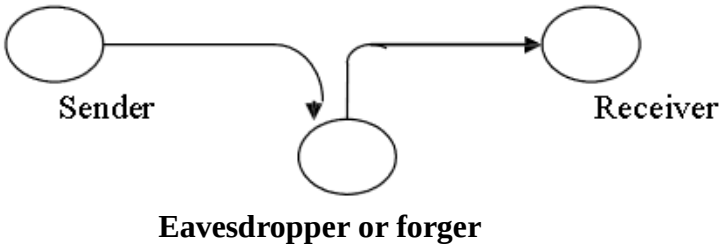
Interception

An unauthorized party gains access to an asset. This is an attack on confidentiality. Unauthorized party could be a person, a program or a computer. e.g., wire-tapping to capture data in the network, illicit copying of files.



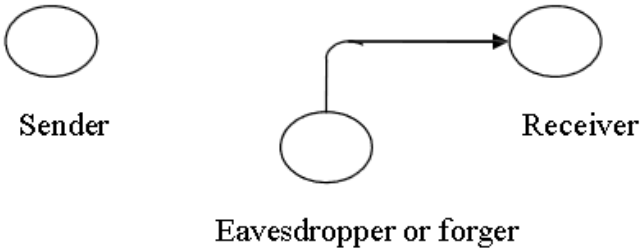
Modification

An unauthorized party not only gains access to but tampers with an asset. This is an attack on integrity. e.g., changing values in data file, altering a program, modifying the contents of messages being transmitted in a network.



Fabrication

An unauthorized party inserts counterfeit objects into the system. This is an attack on authenticity. e.g., insertion of spurious message in a network or addition of records to a file.

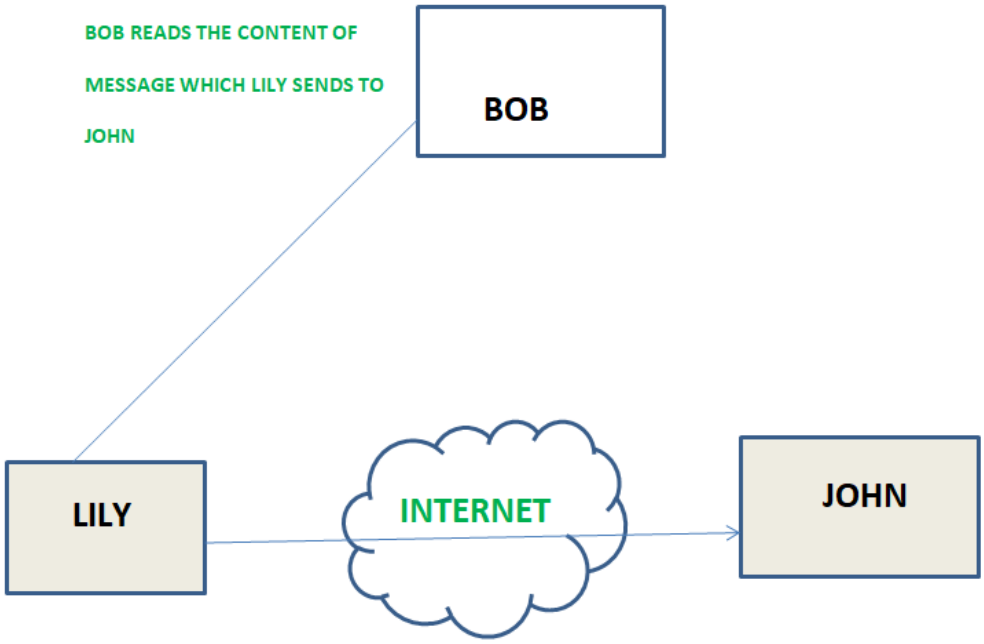


Cryptographic Attacks

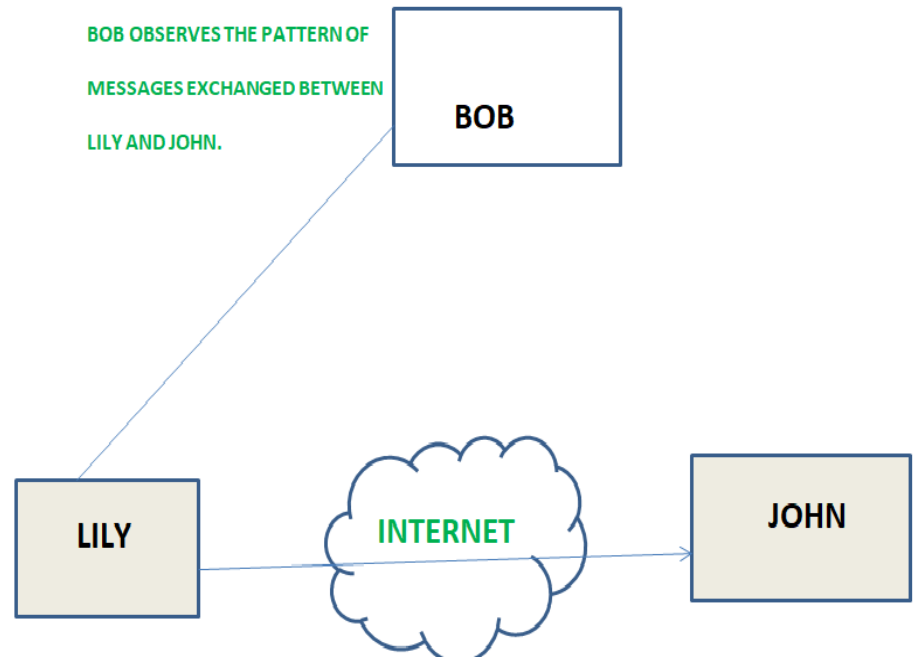
Passive Attacks

Passive Attacks Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the opponent is to obtain information that is being transmitted.
Passive attacks are of two types:

1. **Release of message contents:** A telephone conversation, an e-mail message and a transferred file may contain sensitive or confidential information. We would like to prevent the opponent from learning the contents of these transmissions.



2. **Traffic analysis:** If we had encryption protection in place, an opponent might still be able to observe the pattern of the message. The opponent could determine the location and identity of communication hosts and could observe the frequency and length of messages being exchanged. This information might be useful in guessing the nature of communication that was taking place.

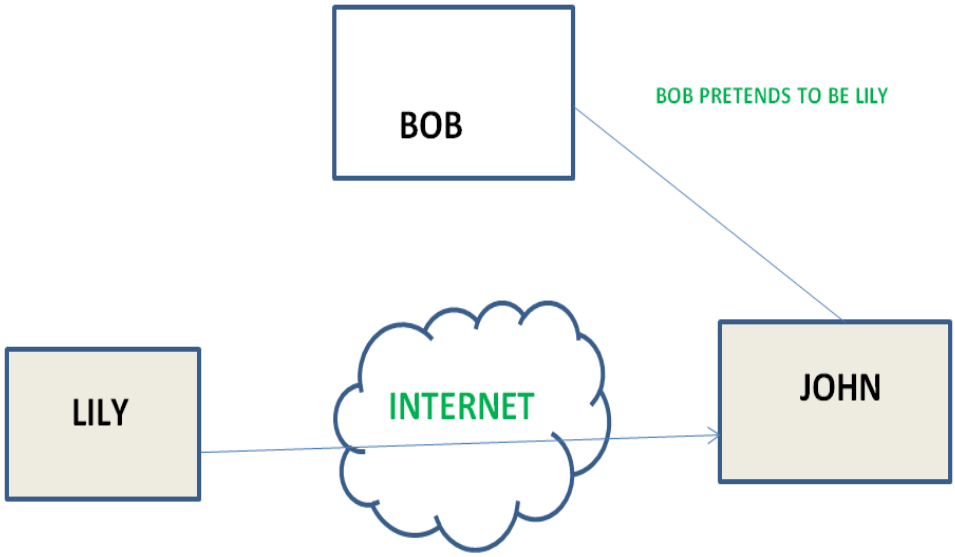


Passive attacks are very difficult to detect because they do not involve any alteration of data. However, it is feasible to prevent the success of these attacks.

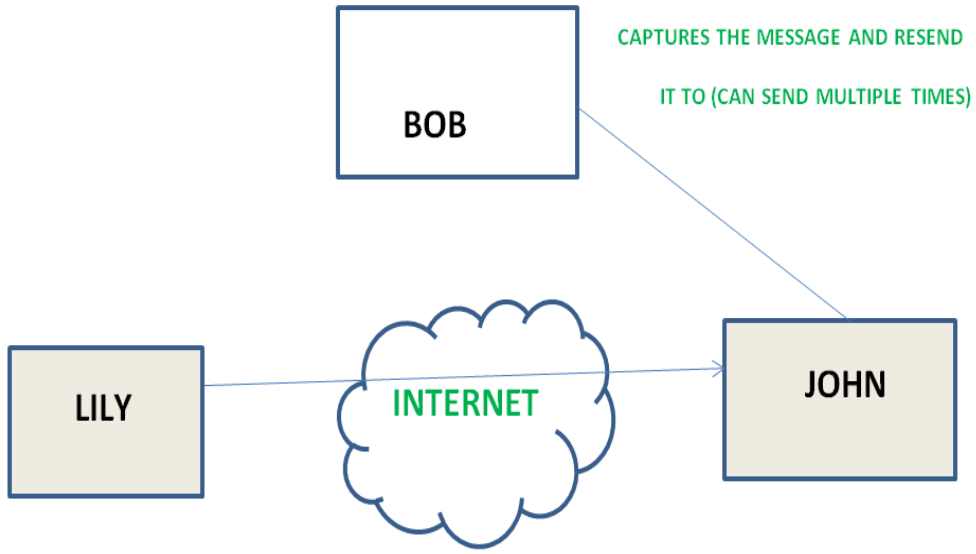
Active attacks

These attacks involve some modification of the data stream or the creation of a false stream. These attacks can be classified in to four categories:

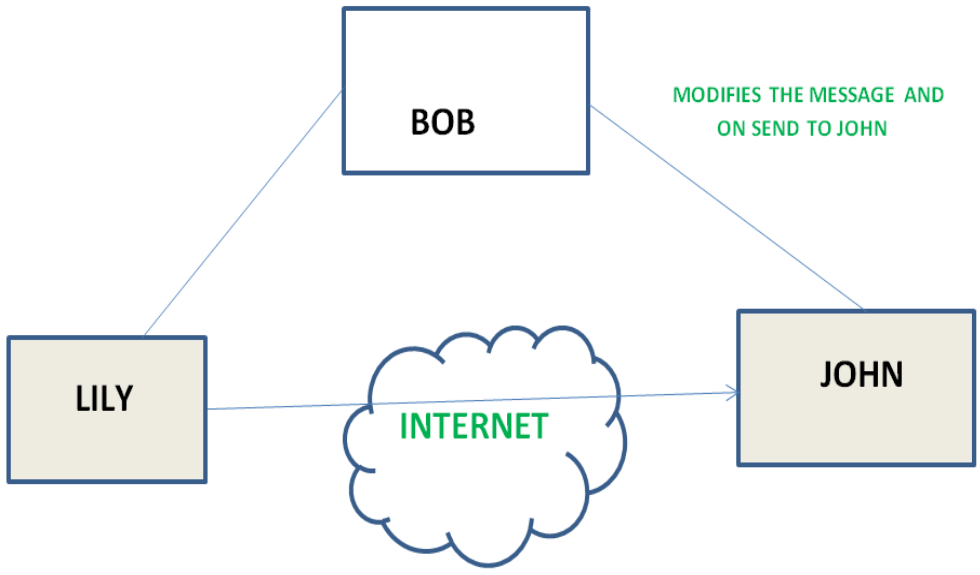
1. **Masquerade:** One entity pretends to be a different entity.



2. **Replay:** involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.

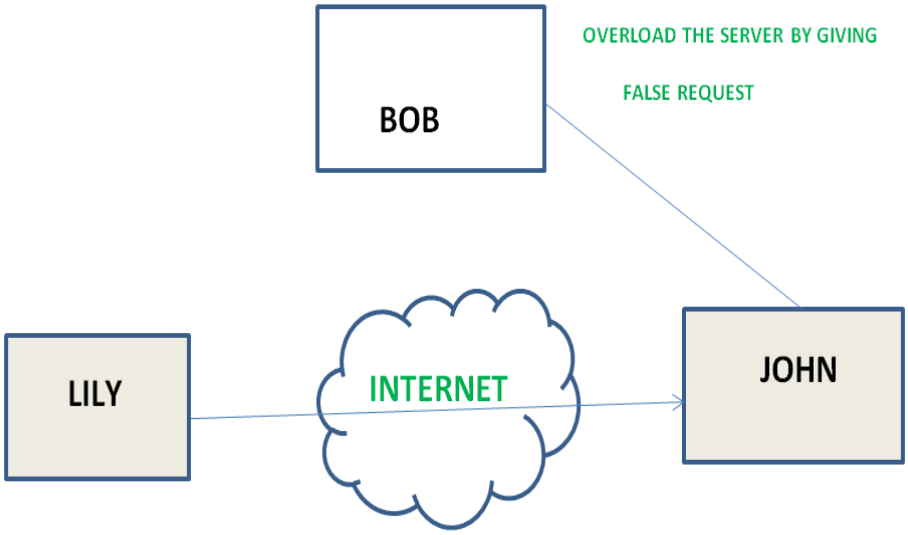


3. **Modification of messages:** Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.



4. **Repudiation:** This attack is done by either sender or receiver. The sender or receiver can deny later that he/she has send or receive a message. For example, customer ask his Bank "To transfer an amount to someone" and later on the sender (customer) deny that he had made such a request. This is repudiation.

5. **Denial of service:** Prevents or inhibits the normal use or management of communication facilities. Another form of service denial is the disruption of an entire network, either by disabling the network or overloading it with messages so as to degrade performance.



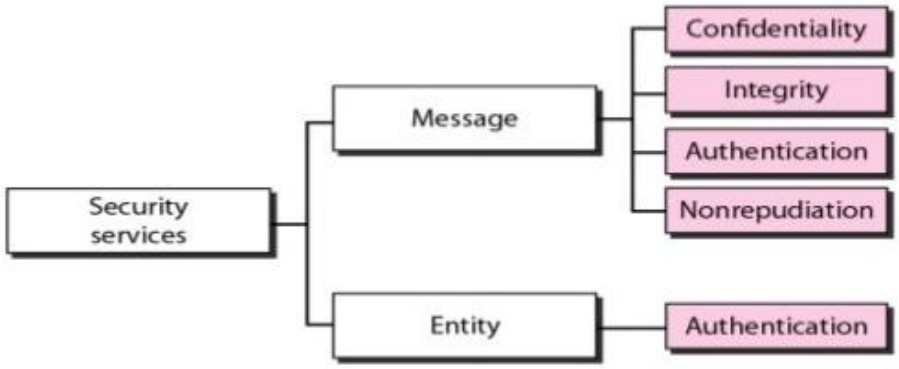
It is quite difficult to prevent active attacks absolutely, because to do so would require physical protection of all communication facilities and paths at all times. Instead, the goal is to detect them and to recover from any disruption or delays caused by them.

Security Services/Principles of Network Security

The classification of security services are as follows:

1. **Confidentiality:** Ensures that the information in a computer system and transmitted information are accessible only for reading by authorized parties. E.g. Printing, displaying and other forms of disclosure.
2. **Authentication:** Ensures that the origin of a message or electronic document is correctly identified, with an assurance that the identity is not false.
3. **Integrity:** Ensures that only authorized parties are able to modify computer system assets and transmitted information. Modification includes writing, changing status, deleting, creating and delaying or replaying of transmitted messages.
4. **Non repudiation:** Requires that neither the sender nor the receiver of a message be able to deny the transmission.
5. **Access control:** Requires that access to information resources may be controlled by or the target system.

6. **Availability:** Requires that computer system assets be available to authorized parties when needed.



Security Mechanisms

Security mechanisms are technical tools and techniques that are used to implement security services. A mechanism might operate by itself, or with others, to provide a particular service.

The various security mechanisms to provide security are as follows-

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. Public and private keys can be used.

4. Authentication Exchange:

In this two entities exchange some messages to prove their identity to each other.

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 available routes between sender and receiver to prevent the opponent from eavesdropping on a particular route.

7. Notarization:

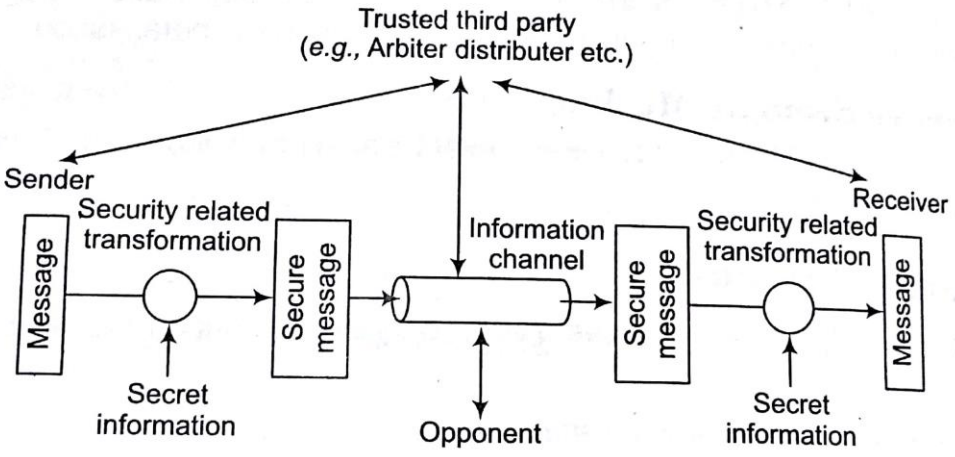
Notarization means selecting a third trusted party to control the communication between two entities. The receiver can involve a trusted third party to store the sender request in order to prevent the sender from later denying that she has made a request.

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 passwords and PINs.

Network Security Model

The **network security** involves all tools, devices, strategies and activities which enterprises and organizations undertake to protect their networks, data and operations. An effective network security strategy must include the most effective set of tools for identification and reflection various threats and attacks. Creation of well thought-out **network security model** will effectively help you in realization your network's security. The network security model (NSM) is a scheme that reflects the general plan and the policy of ensuring the network security.



A general Netwok Security Model (NSM)

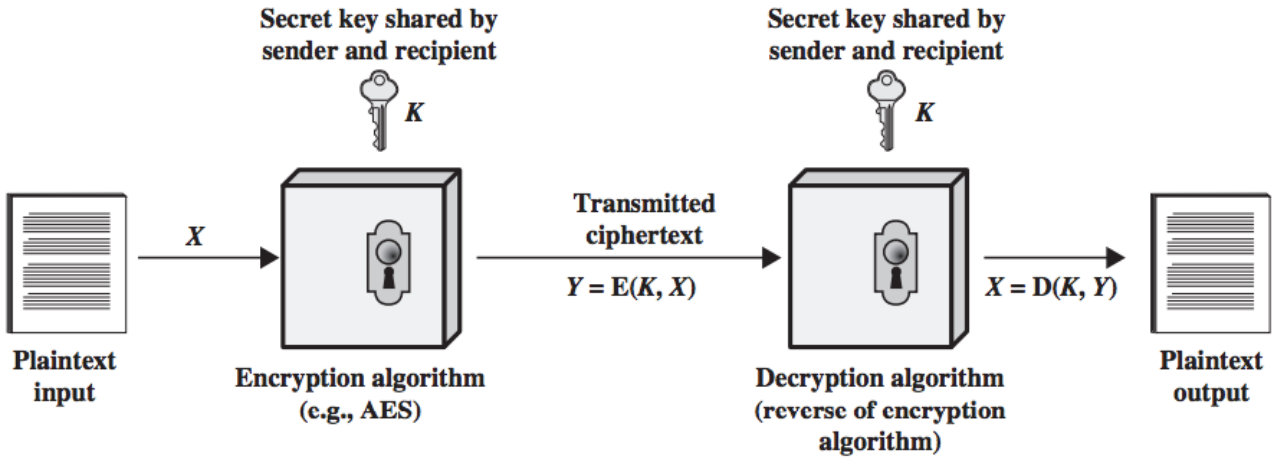
A message is to be transferred from one party to another across some sort of internet. The two parties, who are the principals in this transaction, must cooperate for the exchange to take place. A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals:

1. Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on. All the techniques for providing security have two components:

   - A security-related transformation on the information to be sent. Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

   - Some secret information shared by the two principals and, it is hoped, unknown to the opponent. An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.

2. Part Two discusses a form of encryption, known as public-key encryption, in which only one of the two principals needs to have the secret information.



A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

This general model shows that there are four basic tasks in designing a particular security service:

1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.

2. Generate the secret information to be used with the algorithm.

3. Develop methods for the distribution and sharing of the secret information.

4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

Some basic terminologies used:

Cryptography: The art or science encompassing the principles and methods of transforming an intelligible message into one that is unintelligible, and then retransforming that message back to its original form.

Plain text: The original intelligible message.

Cipher text: The transformed message.

Cipher: An algorithm for transforming an intelligible message into one that is unintelligible by transposition and/or substitution methods.

Key: Some critical information used by the cipher, known only to the sender& receiver.

Encipher (encode): The process of converting plaintext to cipher text using a cipher and a key.

Decipher (decode): the process of converting cipher text back into plaintext using a cipher and a key.

Cryptanalysis: The study of principles and methods of transforming an unintelligible message back into an intelligible message without knowledge of the key. Also called **code breaking.**

Cryptology: Both cryptography and cryptanalysis.

Code: An algorithm for transforming an intelligible message into an unintelligible one using a code-book.

Cryptography

Cryptographic systems are generally classified along 3 independent dimensions:

Type of operations used for transforming plain text to cipher text

All the encryption algorithms are based on two general principles: substitution, in which each element in the plaintext is mapped into another element, and transposition, in which elements in the plaintext are rearranged.

The number of keys used

If the sender and receiver uses same key then it is said to be **symmetric key (or) single key (or) conventional encryption.**

If the sender and receiver use different keys then it is said to be public key encryption.

The way in which the plain text is processed

A **block cipher** processes the input and block of elements at a time, producing output block for each input block.

A **stream cipher** processes the input elements continuously, producing output element one at a time, as it goes along.

Cryptanalysis

The process of attempting to discover X or K or both is known as cryptanalysis. The strategy used by the cryptanalysis depends on the nature of the encryption scheme and the information available to the cryptanalyst.

There are various types of cryptanalytic attacks based on the amount of information known to the cryptanalyst.

Cipher text only – A copy of cipher text alone is known to the cryptanalyst.

Known plaintext – The cryptanalyst has a copy of the cipher text and the corresponding plaintext.

Chosen plaintext – The cryptanalysts gains temporary access to the encryption machine. They cannot open it to find the key, however; they can encrypt a large number of suitably chosen plaintexts and try to use the resulting cipher texts to deduce the key.

Chosen cipher text – The cryptanalyst obtains temporary access to the decryption machine, uses it to decrypt several string of symbols, and tries to use the results to deduce the key.

Types of Cryptosystems

Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system −

- Symmetric Key Encryption
- Asymmetric Key Encryption

Symmetric Key Encryption

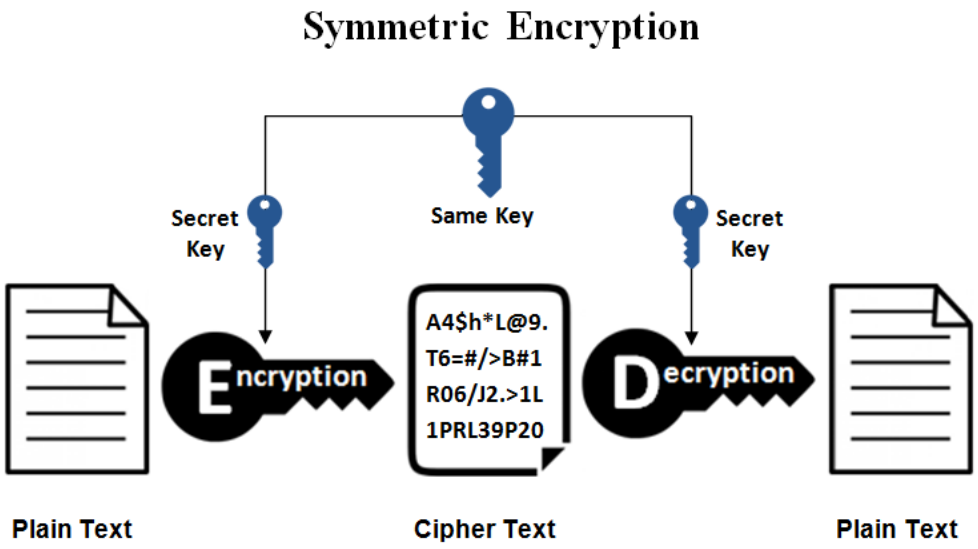
Symmetric Encryption is an Encryption algorithm where the same key is used for both Encryption and Decryption. The key must be kept secret, and is shared by the message sender and recipient.

Symmetric encryption, also known as single-key and/or private-key encryption, uses a secret key (could be a number, a word, a random string of characters) as a means to modify or mask the content of a given message.

There are two types of symmetric encryption algorithms:

Block algorithms. Set lengths of bits are encrypted in blocks of electronic data with the use of a specific secret key. As the data is being encrypted, the system holds the data in its memory as it waits for complete blocks.

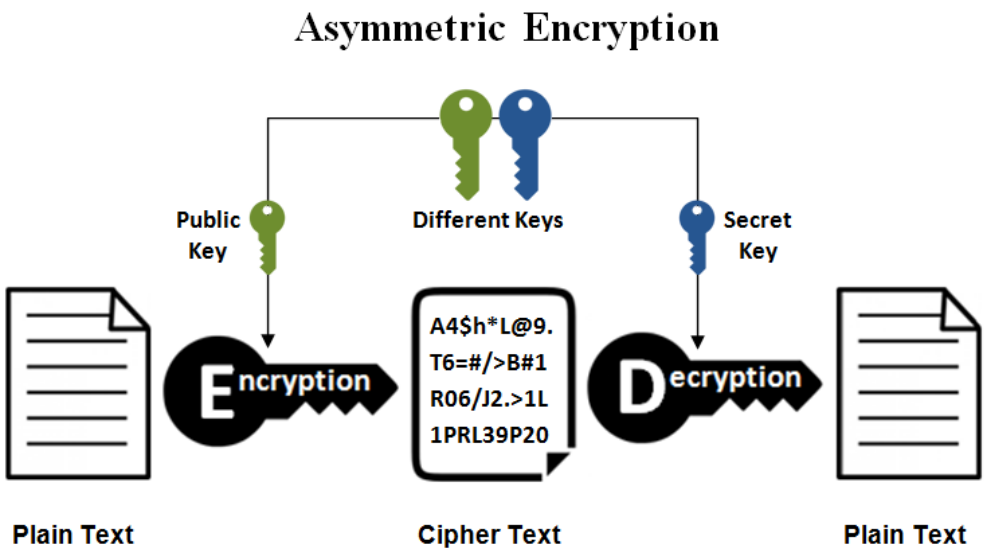
Stream algorithms. Data is encrypted as it streams instead of being retained in the system's memory.



Asymmetric Key Encryption

Asymmetric Encryption is a form of Encryption where keys come in pairs. What one key encrypts, only the other can decrypt.

Asymmetric Encryption is also known as Public Key Cryptography, since users typically create a matching key pair, and make one public while keeping the other secret.

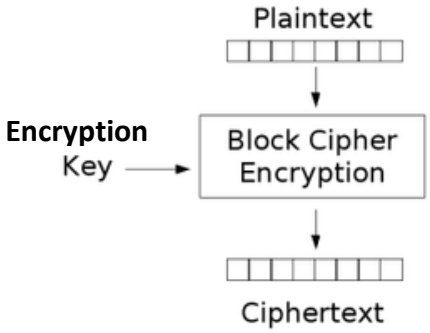


Symmetric v/s Asymmetric

Characteristic	Symmetric Key Cryptography	Asymmetric Key Cryptography
Key used for encryption / decryption	Same key is used for encryption and decryption	One key used for encryption and another, different key is used for decryption
Speed of encryption / decryption	Very fast	Slower
Size of resulting encrypted text	Usually same as or less than the original clear text size	More than the original clear text size
Key agreement / exchange	A big problem	No problem at all
Number of keys required as compared to the number of participants in the message exchange	Equals about the square of the number of participants, so scalability is an issue	Same as the number of participants, so scales up quite well
Usage	Mainly for encryption and decryption (confidentiality), cannot be used for digital signatures (integrity and non-repudiation checks)	Can be used for encryption and decryption (confidentiality) as well as for digital signatures (integrity and non-repudiation checks)

Block Cipher

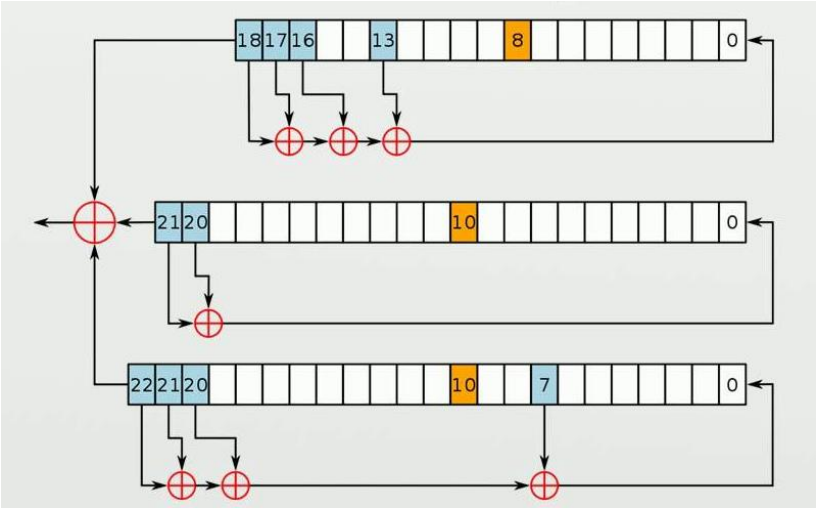
In cryptography, a block cipher is a symmetric key cipher which operates on fixed-length groups of bits, termed blocks, with an unvarying transformation. When encrypting, a block cipher might take (for example) a 128-bit block of plaintext as input, and output a corresponding 128-bit block of cipher text. The exact transformation is controlled using a second input — the secret key. Decryption is similar: the decryption algorithm takes, in this example, a 128- bit block of cipher text together with the secret key, and yields the original 128-bit block of plaintext. To encrypt messages longer than the block size (128 bits in the above example), a mode of operation is used.



Stream Cipher

A stream cipher encrypts plaintext messages by applying an encryption algorithm with a pseudorandom cipher digit stream (key stream). Each bit of the message is encrypted one by one with the corresponding key stream digit. Stream ciphers are typically used in cases where speed and simplicity are both requirements.

It uses an infinite stream of pseudorandom bits as the key. For a stream cipher implementation to remain secure, its pseudorandom generator should be unpredictable and the key should never be reused. Stream ciphers are designed to approximate an idealized cipher, known as the One-Time Pad.



Steganography:

Steganography is the technique of embedding hidden messages /data in such a way that no one can detect the existence of the messages, except the sender and intended receiver(s). The main aim of steganography is to hide the secret message or information in such a way that no one is able to detect it. If they found any suspicion data, then goal is defeated.

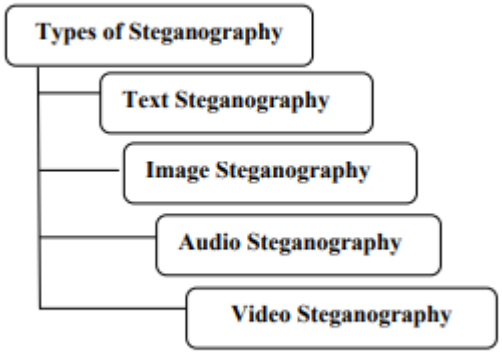
The various types of data in steganography can be audio, video, text and images etc.

The basic model of Steganography consists of three components:

- **The Carrier image:** The carrier image is also called the cover object that will carry the message/data which is used to be hidden.
- **The Message:** A message can be anything like data, file or image etc.
- **The Key:** A key is used to decode/decipher the hidden message.

Basic Model of Steganography

1. TYPES FOR STEGANOGRAPHY:



Techniques of Steganography