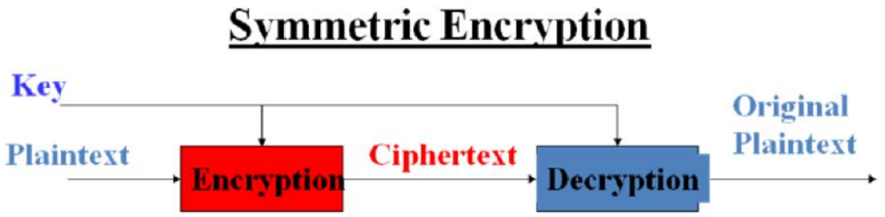
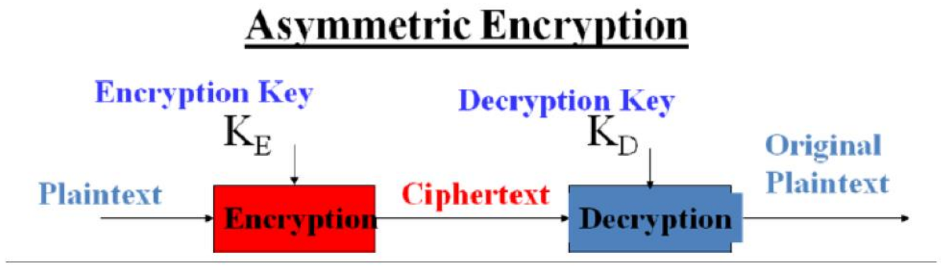
Cryptography

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.
  - ✓ **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 secret-key or single key or conventional encryption).
  - ✓ If the sender and receiver use different keys then it is said to be asymmetric (or public key) encryption.





- The way in which the plain text is processed
  - ✓ A block cipher processes the input as 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.

Security Attacks, Services and Mechanisms

To assess the security needs of an organization effectively, the manager responsible for security needs some systematic way of defining the requirements for security and characterization of approaches to satisfy those requirements. One approach is to consider three aspects of information security:

Security attack – Any action that compromises the security of information owned by an organization.

Security mechanism– A mechanism that is designed to detect, prevent or recover from a security attack.

Security service – A service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the service.

Security Services

The classification of security services are as follows:

1. **Availability**: Requires that computer system assets be available to authorized parties when needed.
2. **Authentication**: - assurance that the communicating entity is the one claimed.
3. **Access Control**:- prevention of the unauthorized use of a resource.
4. **Data Confidentiality**:- protection of data from unauthorized disclosure.
5. **Data Integrity**: - assurance that data received is as sent by an authorized entity.
6. **Non-Repudiation**: - protection against denial by one of the parties in a communication.

Security Mechanisms

One of the most specific security mechanisms in use is cryptographic techniques.

Encryption or encryption-like transformations of information are the most common means of providing security. Some of the mechanisms are

1. Cryptography.

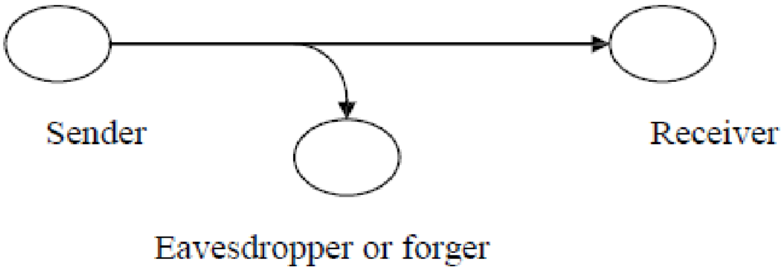
2. Digital Signature.

3. Access Control.

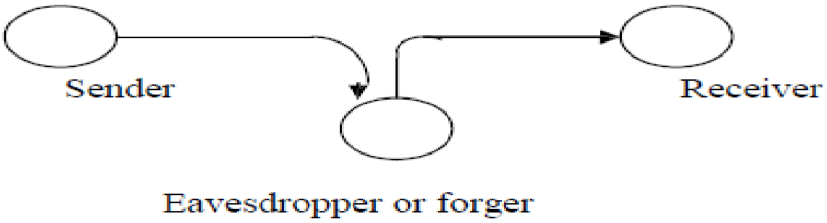
Security Attacks

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

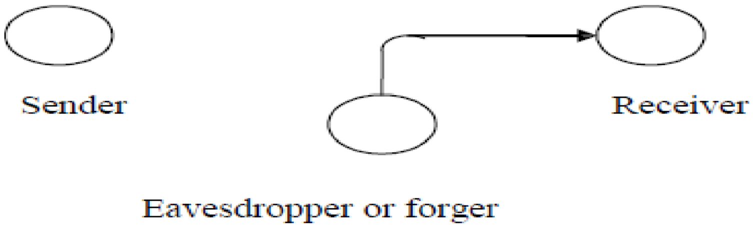
1. **Interruption**
   An assets of the system is destroyed or becomes unavailable or unusable. This is an attack on availability e.g., destruction of piece of hardware, cutting of a communication line or Disabling of file management system.
2. **Interception**
   An unauthorized party gains access to 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.



3. **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.



4. **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

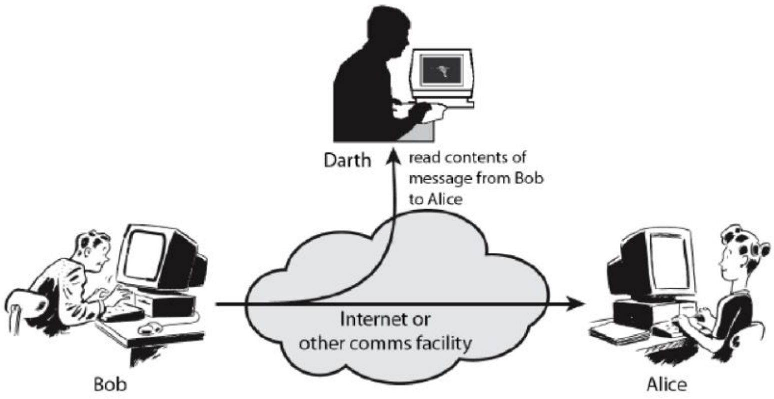
There are two types of cryptographic attacks:

1- 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:

- **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.
- **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.


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

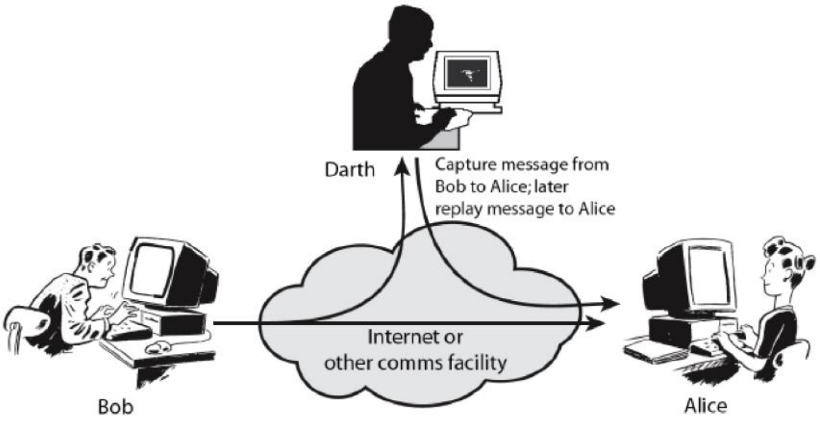
Passive Attacks

2- 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:

- **Masquerade** – One entity pretends to be a different entity.
- **Replay** – involves passive capture of a data unit and its subsequent transmission to produce an unauthorized effect.
- **Modification of messages** – Some portion of message is altered or the messages are delayed or recorded, to produce an unauthorized effect.
- **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.


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

Active Attacks