UNIT VI

: Network Security & Cryptography

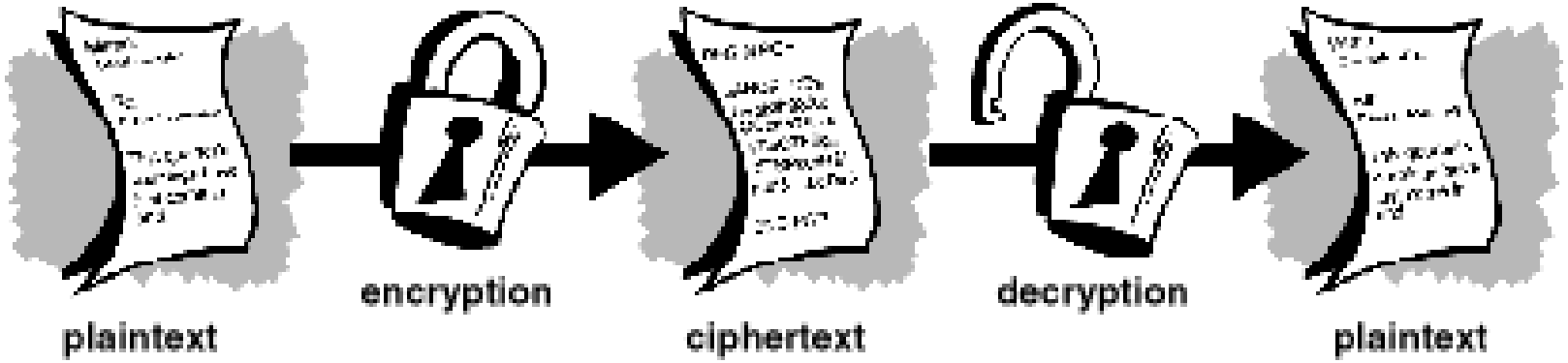
- **Unit VI : Network Security & Cryptography**
- Introduction to Security & Cryptography,
- Security concepts- Computer Security
- Network Security
- Information Security
- Firewall
- Working of Firewalls
- Conventional Cryptography
- Caesar’s Cipher
- public key Cryptography.

The Basics of Cryptography

- When Julius Caesar sent messages to his generals, he didn't trust his messengers.
- So he replaced every A in his messages with a D, every B with an E, and so on through the alphabet.
- Only someone who knew the "shift by 3" rule could decipher his messages.

Encryption and decryption

- Data that can be read and understood without any special measures is called *plaintext* or *cleartext.*
- The method of disguising plaintext in such a way as to hide its substance is called *encryption.*
- Encrypting plaintext results in unreadable gibberish called *ciphertext.*
- You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data.
- The process of reverting ciphertext to its original plaintext is called *decryption*.
- *Following Fiaure* illustrates this process.



What is cryptography?

- *Cryptography* is the science of using mathematics to encrypt and decrypt data. Cryptography enables you to store sensitive information or transmit it across insecure networks (like the Internet) so that it cannot be read by anyone except the intended recipient.
- While cryptography is the science of securing data, *cryptanalysis* is the science of analyzing and breaking secure communication. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding, patience, determination, and luck. Cryptanalysts are also called *attackers.*

Introduction to Security

- COMPUTER SECURITY:- The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity**, **availability** and **confidentiality** of information system resources which includes hardware, software, firmware, information/ data, and telecommunication.

Integrity

- Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.
- A loss of integrity is the unauthorized modification or destruction of information.

Availability

- Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system

Confidentiality

- Preserving authorized restriction on information access and disclosure, including means for protecting personal privacy and proprietary information.
- A loss of confidentiality is the unauthorized disclosure of information.

Security Attacks

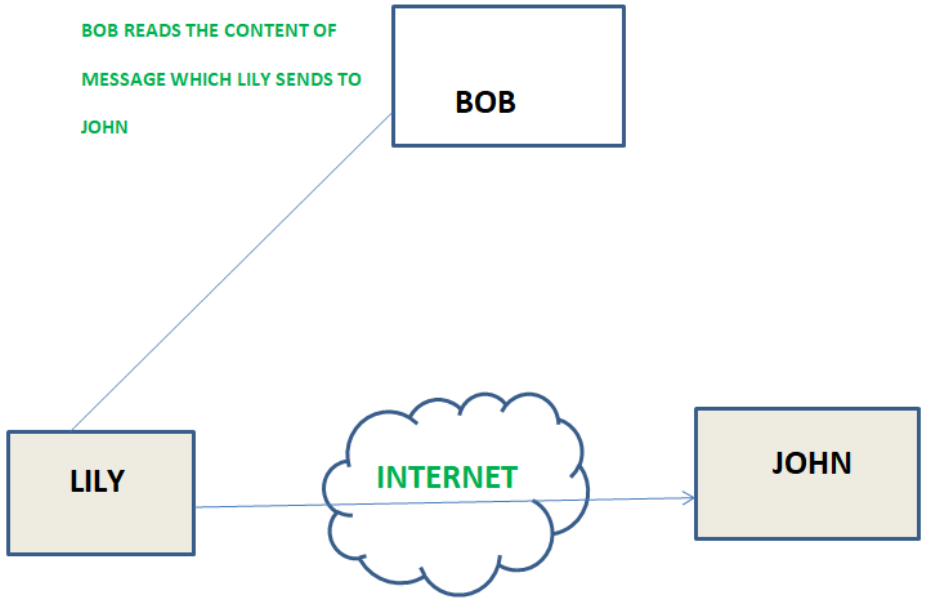
- There are two types of Security attacks
  - Passive Attacks
  - Active Attacks

Passive Attacks:

- A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring of transmission. The goal of the opponent is to obtain information is being transmitted. Types of Passive attacks are as following:
- **release of message content**
- **Traffic analysis**

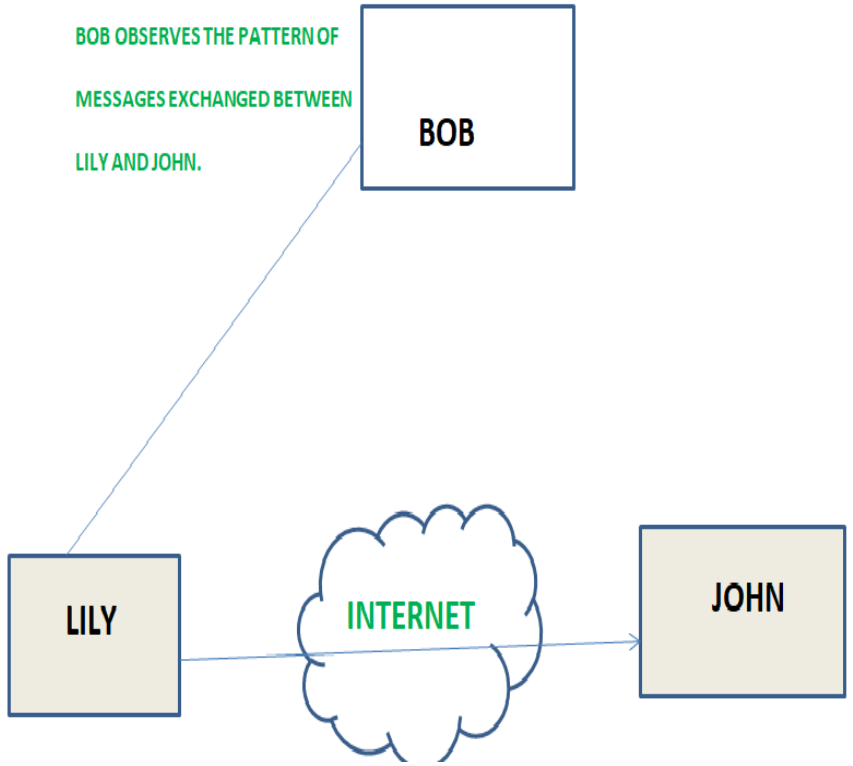
The release of message content –

- Telephonic conversation, an electronic mail message or a transferred file may contain sensitive or confidential information. We would like to prevent an opponent from learning the contents of these transmissions.



Traffic analysis

- Suppose that we had a way of masking (encryption) of information, so that the attacker even if captured the message could not extract any information from the message.
- The opponent could determine the location and identity of communicating host and could observe the frequency and length of messages being exchanged.
- This information might be useful in guessing the nature of the communication that was taking place.

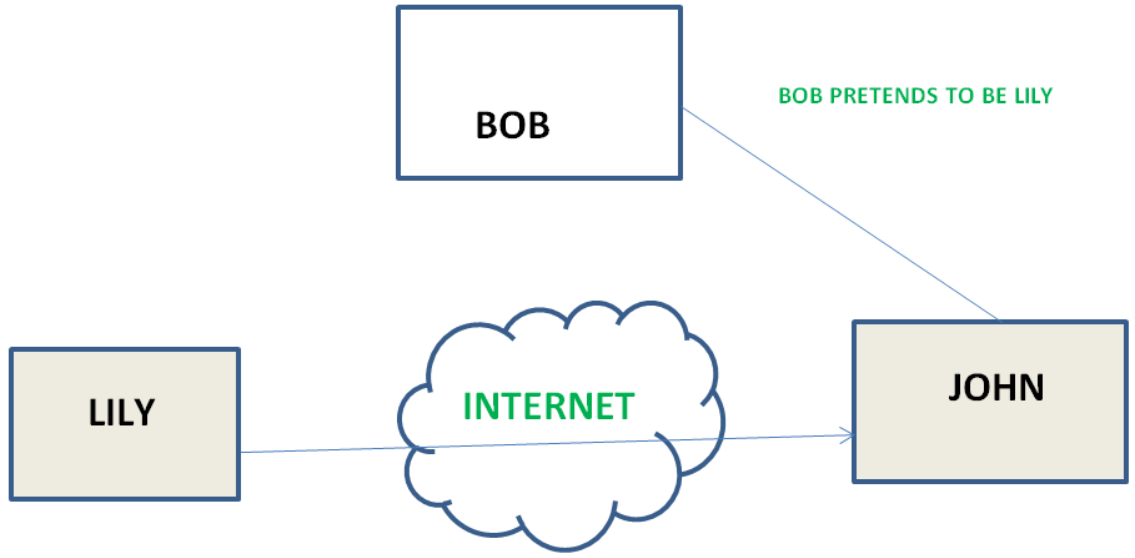


Active attacks

- **Active attacks:** An Active attack attempts to alter system resources or effect their operations. Active attack involve some modification of the data stream or creation of false statement. Types of active attacks are as following:
  - **Masquerade**
  - **Modification of messages**
  - **Repudiation**
  - **Replay**
  - **Denial of Service**

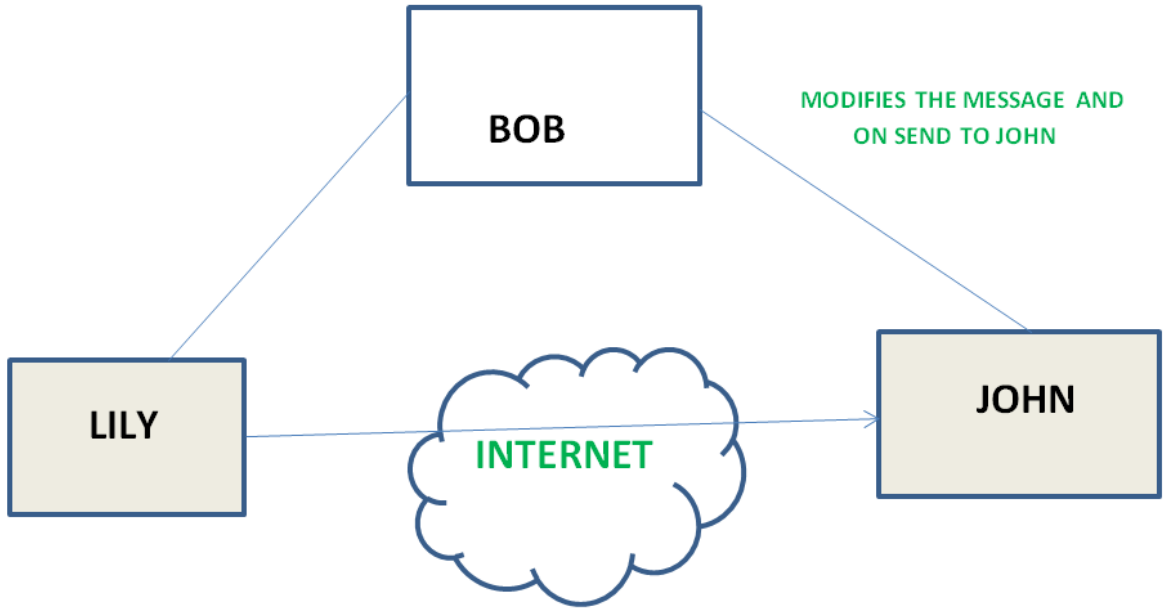
Masquerade

Masquerade attack takes place when one entity pretends to be different entity.
A Masquerade attack involves one of the other form of active attacks.



Modification of messages

- It means that some portion of a message is altered or that message is delayed or reordered to produce an unauthorised effect.
- For example, a message meaning “Allow JOHN to read confidential file X” is modified as “Allow Smith to read confidential file X”.

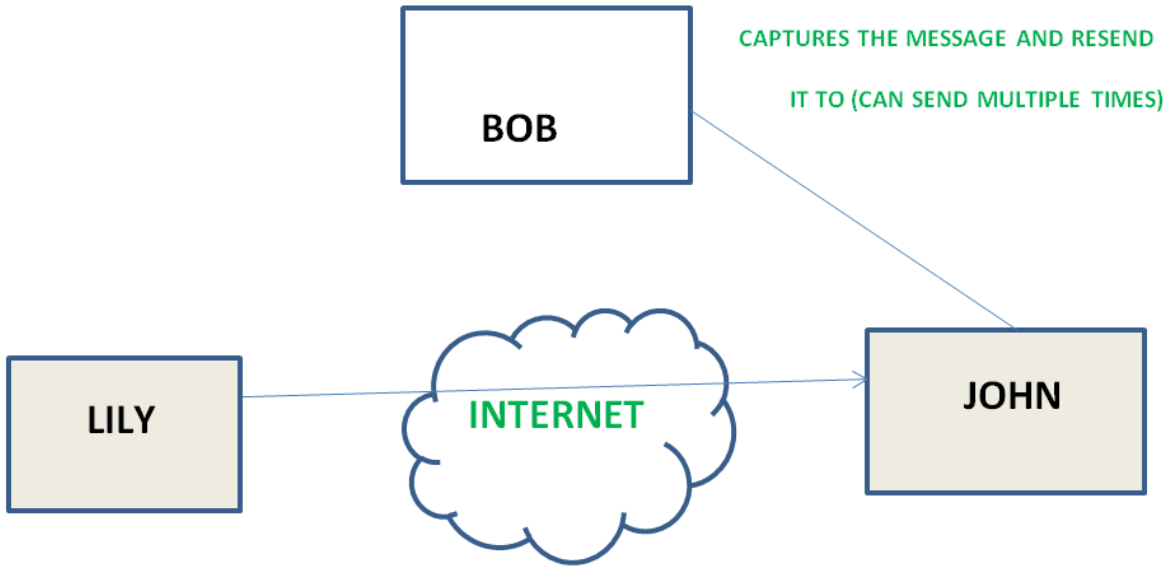


Repudiation

- 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.

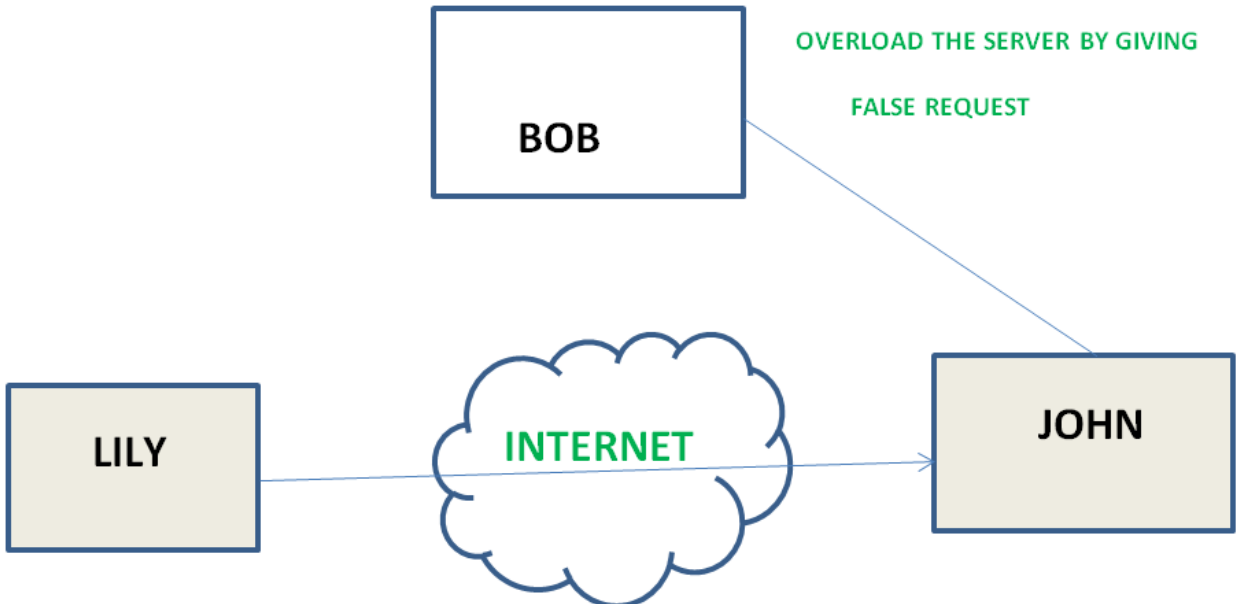
Replay

- It involves the passive capture of a message and its subsequent the transmission to produce an authorized effect.



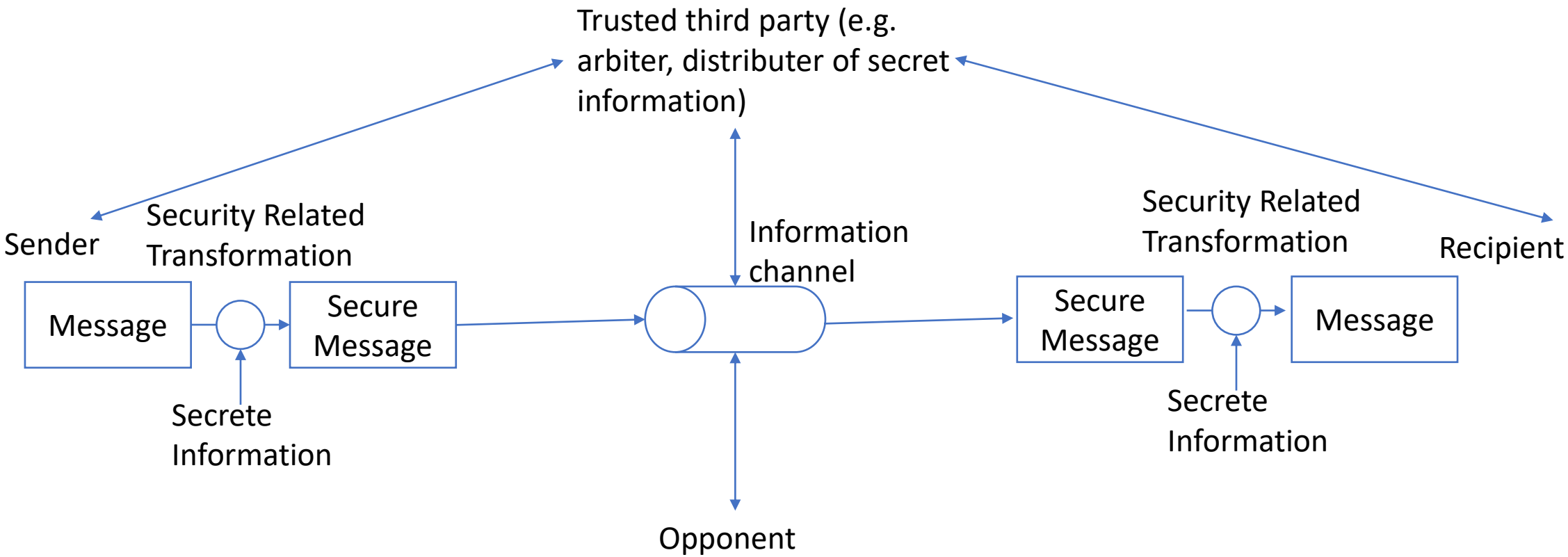
Denial of Service

- It prevents normal use of communication facilities. This attack may have a specific target. For example, an entity may suppress all messages directed to a particular destination.
- Another form of service denial is the disruption of an entire network wither by disabling the network or by overloading it by messages so as to degrade performance.



Network Security

- A Model for Network Security: A message is to be transferred from one party to another across some sort of Internet Service.
- There are two practices which are the principles in the transactions. A Logical information channel is established by defining a route through the Internet from source to destination.
- 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 & so on..


Trusted third party (e.g. arbiter, distributer of secret information)
Sender
Security Related Transformation
Information channel
Security Related Transformation
Recipient
Message
Secure Message
Secure Message
Message
Secrete Information
Secrete Information
Opponent

- 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.
- A trusted third party may be needed to achieve secure transmission. For example it is responsible for distributing the secrete information to the two principles while keeping it from any opponent.

- This general model shows that there are four basic tasks in designing a particular security services:
  - Designing a algorithm such that an opponent cannot defeat its purpose.
  - Generate the secrete information to be used with the algorithm.
  - Develop methods for the distribution and sharing of the secret information.
  - 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.

Information Security

- **Information Security** is not all about securing information from unauthorized access. Information Security is basically the practice of preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. Information can be physical or electrical one.
- Information can be anything like Your details or we can say your profile on social media, your data in mobile phone, your biometrics etc. Thus Information Security spans so many research areas like Cryptography, Mobile Computing, Cyber Forensics, Online Social Media etc.
- Information Security programs are build around 3 objectives, commonly known as CIA – Confidentiality, Integrity, Availability.

- **Confidentiality –** means information is not disclosed to unauthorized individuals, entities and process.
- For example if we say I have a password for my Gmail account but someone saw while I was doing a login into Gmail account. In that case my password has been compromised and Confidentiality has been breached.
- **Integrity –** means maintaining accuracy and completeness of data. This means data cannot be edited in an unauthorized way.
- For example if an employee leaves an organisation then in that case data for that employee in all departments like accounts, should be updated to reflect status to JOB LEFT so that data is complete and accurate and in addition to this only authorized person should be allowed to edit employee data.

- **Availability –** means information must be available when needed. For example if one needs to access information of a particular employee to check whether employee has outstanded the number of leaves, in that case it requires collaboration from different organizational teams like network operations, development operations, incident response and policy/change management.
  Denial of service attack is one of the factor that can hamper the availability of information.