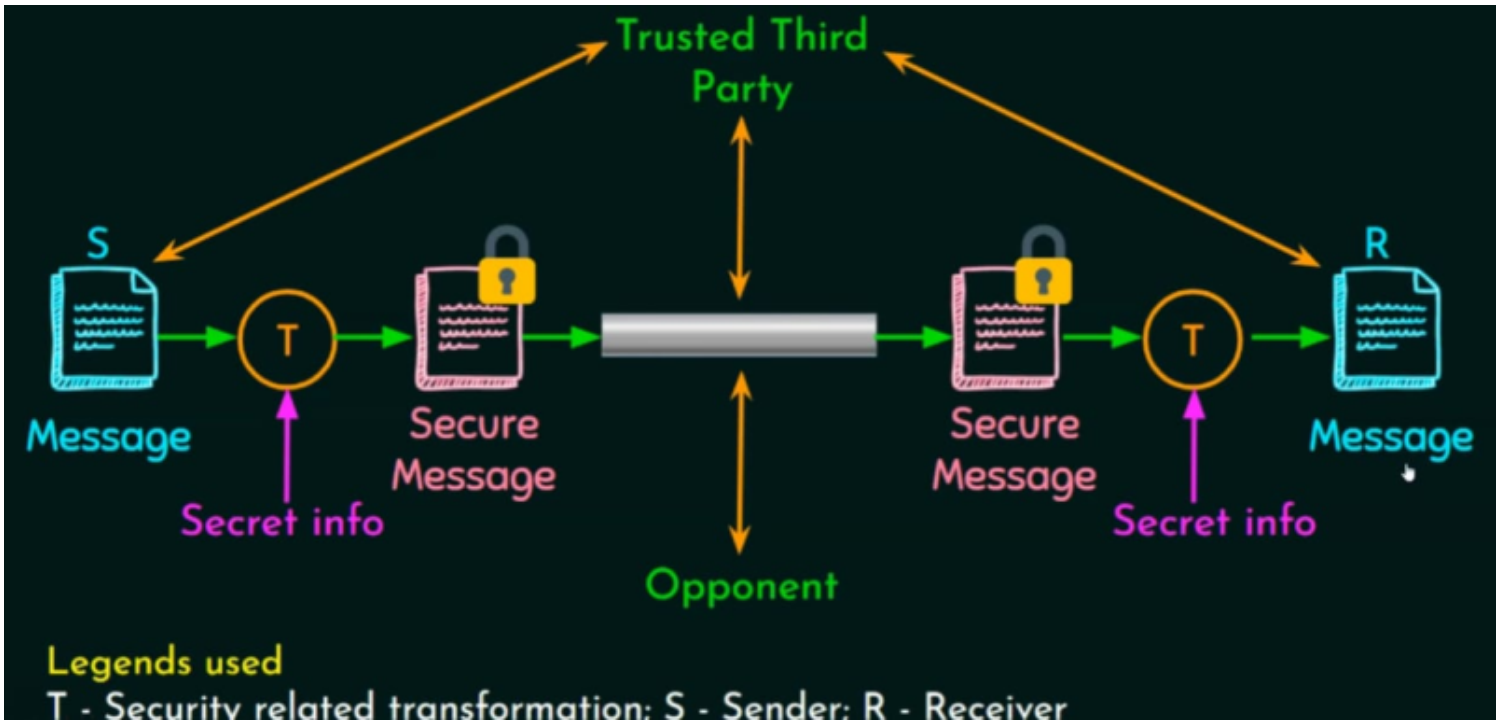
NETWORK SECURITY MODEL:



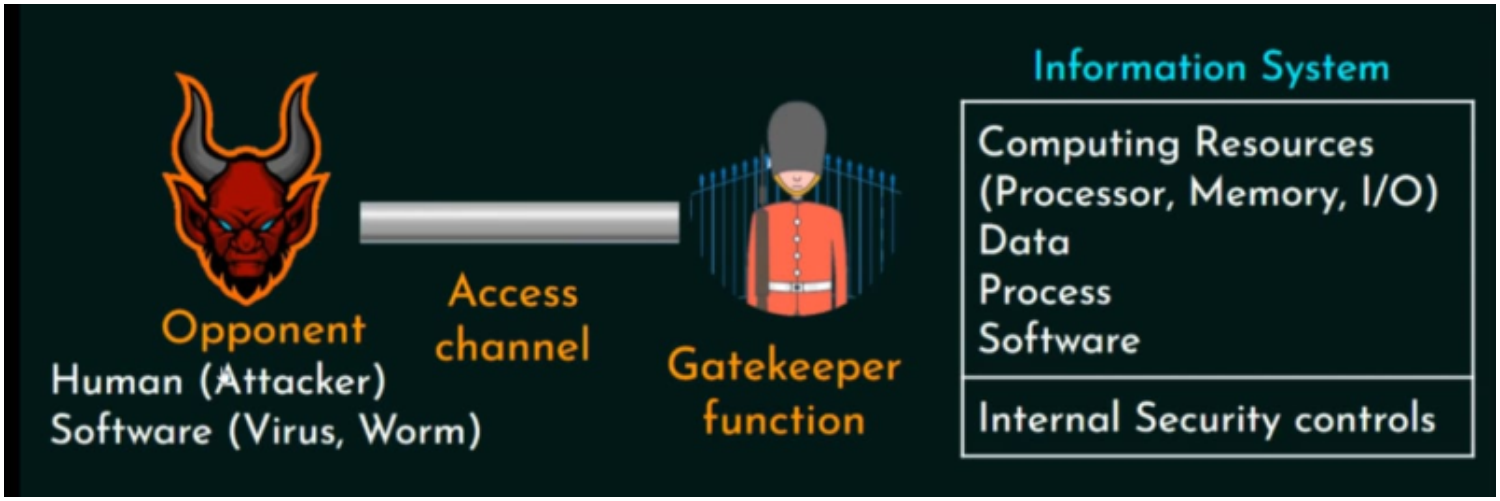
• Sender passes the message to be send from security related transformations along with the secret information to make the message a secure one.
• Then it is placed on the internet. It travels on the internet and then the receiver receives the secure message.
• The receiver tries to undo the security related transformation by applying the secret information applied to the message by the sender to get the original message.
• In this whole scenario, we can see that there is a security related transformation in both sender as well as the receiver side.
• So sender and receiver are not communicating messages, rather they are communicating secure messages.
• So this is the ultimate goal of network security model more precisely, network security.
• If some webserver uses SSL certs, which is the cert that this server is providing a secure communication. These kinds of certs are provided by these Trusted 3rd party. These parties also play a role to avoid repudiation. Shortly, a trusted 3rd party is involved between sender and receiver in order to handle certain level of security.

• There are also opponents or attacker on the internet who will try to know what is the conversation or may have some other intentions. But they will get secure messages, so the real security depends on the security related transformation.
• The security related transformation can be encyption where the secret information is the key or it may be steganography which use password as the secret info (No password needed for revealing at receiver side if password is not applied on the sender side) to reveal the message hidden inside the multimedia or it may be some other kind of security applied to make the message secure.

4 MAJOR TASKS FOR DESIGNING A NETWORK SECURITY MODEL:

1. Design an algorithm (Encryption and decryption algorithm)
2. Generate the secret informaton.
3. Develop methods for distributing and sharing of information (How particular information is going to go on the the internet, or how in symmetric cryptography, the key are going to be exchanged in a secured manner between the sender and the receiver)
4. Specify a protocol (Selecting a secure protocol which will be used by both sender and receiver, and the protocol will have all the security requirements used by sender and receiver as well as on the internet)

NETWORK ACCESS SECURITY MODEL:



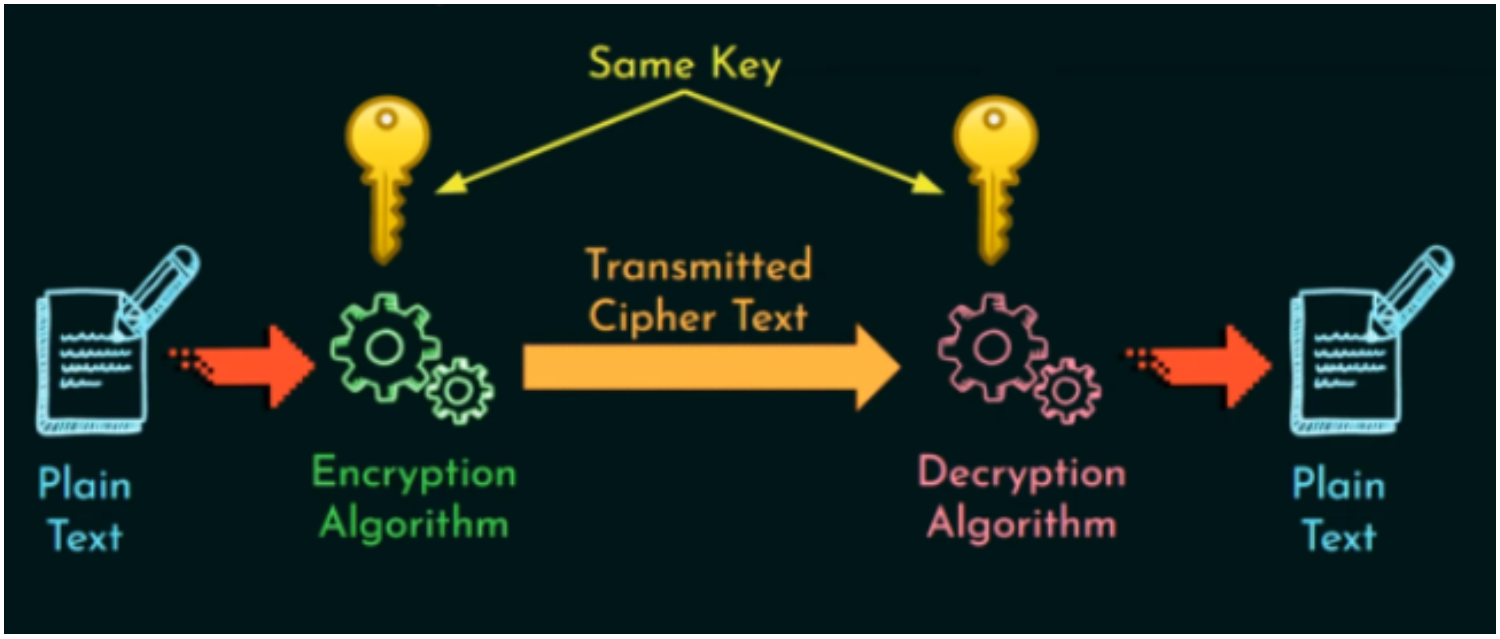
• There is an opponent which is a human who is trying to attack the information system which requires high level of security either by using his tactics or by using some kind of software like viruses, trojans etc. In that case, the software will be also considered an opponent.
• The attacker can also be a person working in the same organization, trying to attack it, which is also an opponent but internal opponent or internal threat. But internal threats are always lesser that external threats, for which access control mechanisms are enough if an attacker is not sharp enough.
• The internal security controls will protect the information system from internal as well as external attacks to some extent but the attacker will always try to gain access to the information security or cause some damage to it.
• To handle this we have a gatekeeper function which will try to filter the traffic before giving the data to the information system. This gatekeeper function can be a firewall or some other security mechanism to check whether a legit user is trying to access or is it an attacker.
• Internal security controls examples can be antivirus in the infomration system.
• The firewall will filter the incoming as well as the outgoing data. Outgoing is also necessary because if someone succeded to bypass the firewall and the attacker is remotely connected to information system. Now he is trying to send the data to his machine. So in that case we configure a firewall insuch a way that we tell it not to allow this sensitive file go outside the network. The data can also be sent to the remote hacker by the person working inside the organization.

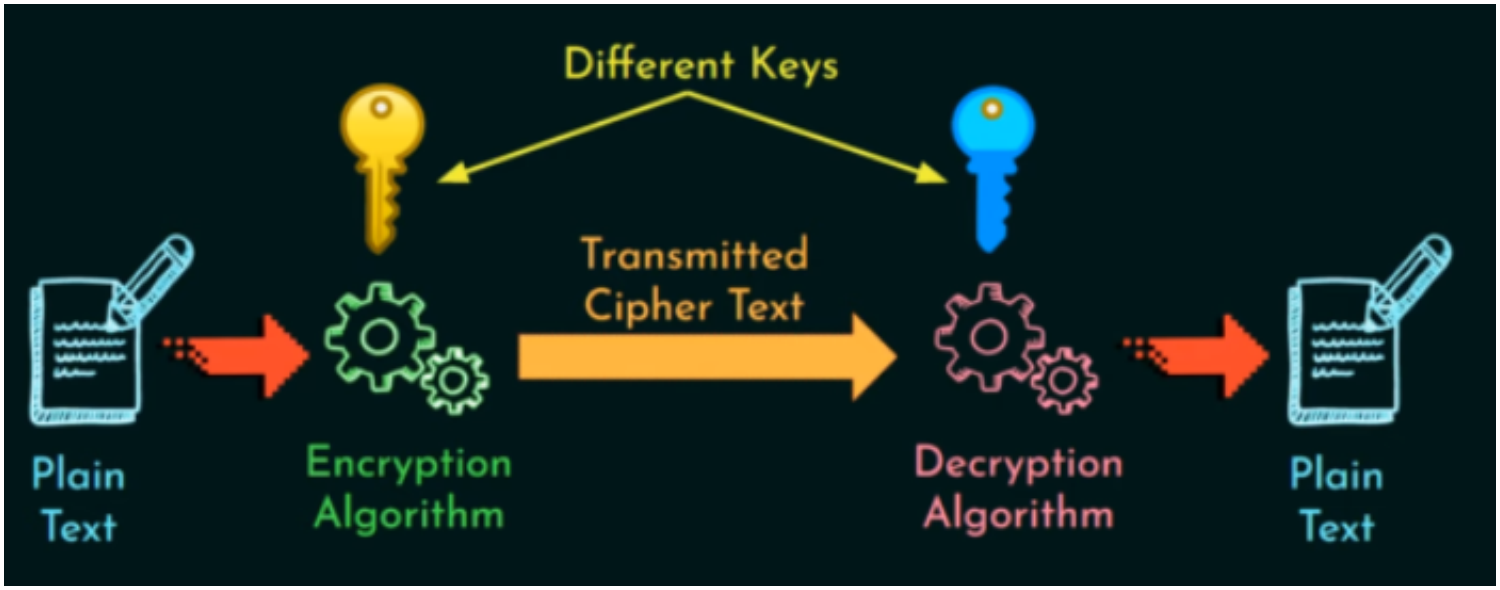
CRYPTOGRAPHY:

The science that deals with the methods of converting the plain text to cipher text using an encryption algorithm and a key and converting the cipher text back to the plain text using decryption algorithm and the key.

TYPES OF CRYPTOGRAPHY:

Cryptography can be Symmetric or Private Key Cryptography(Using same keys for encryption and decryption) or Assymmetric a.k.a Public Key Cryptography (Using different keys for encryption and decryption).





2 IMPORTANT PROPERTIES ANY ENCRYPTION ALGORITHM SHOULD POCESS:

When an encryption algorithm is designed, it should be confirmed that it should have the following properties:

1. UNCONDITIONALLY SECURE:

An encryption algorithm is said to be unconditionally secure if the amount of cipher text, no matter how much it is available to the attacker, he is still unable to guess the plain text i.e : It have no clue about the plain text.

2. COMPUTATIONALLY SECURE:

An encryption algorithm is said to be computationally secure if the cost of cipher exceeds the value of the cipher text or the time required to break the cipher text exceeds the useful lifetime of the information. The cost and the time reqired to break the cipher text exceeds the value. This value can be the value of the encrypted information or the life time of the encrypted information.