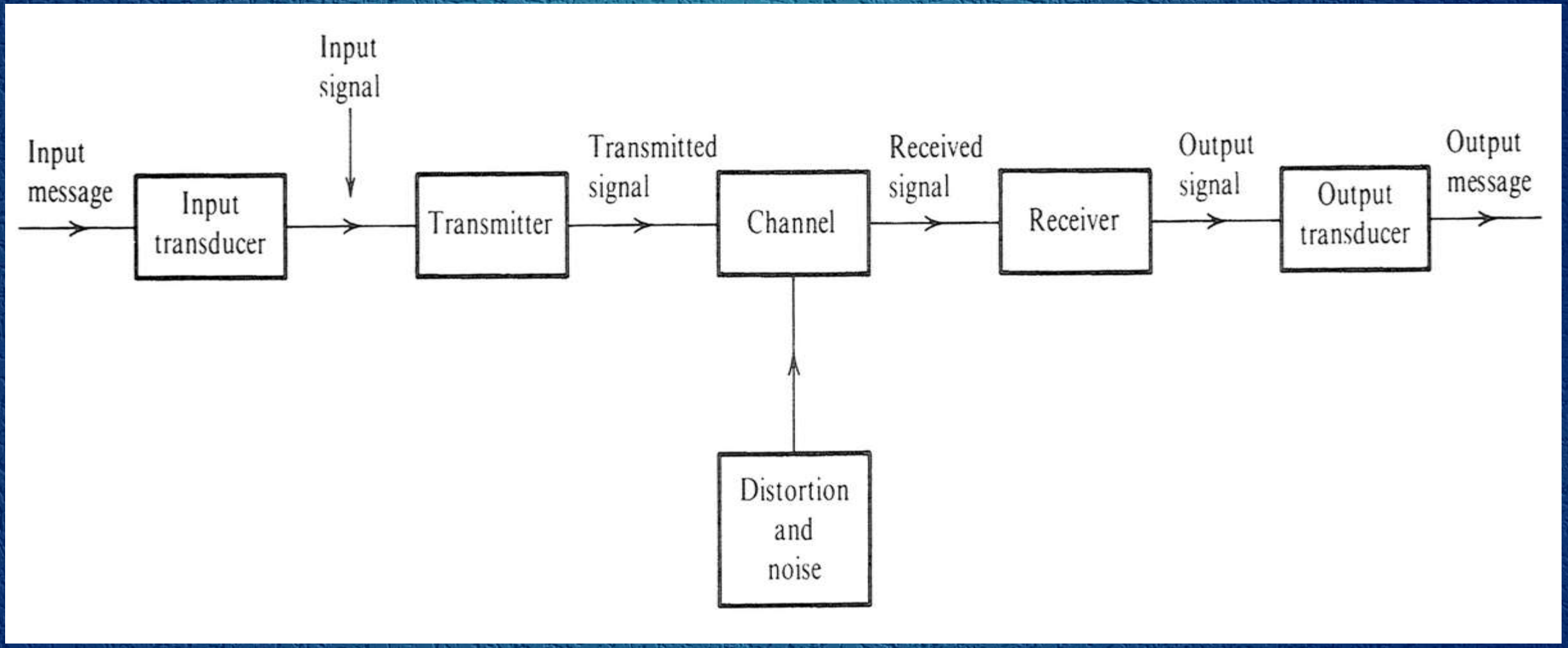
Wireless Communication Authentication, Encryption and Security

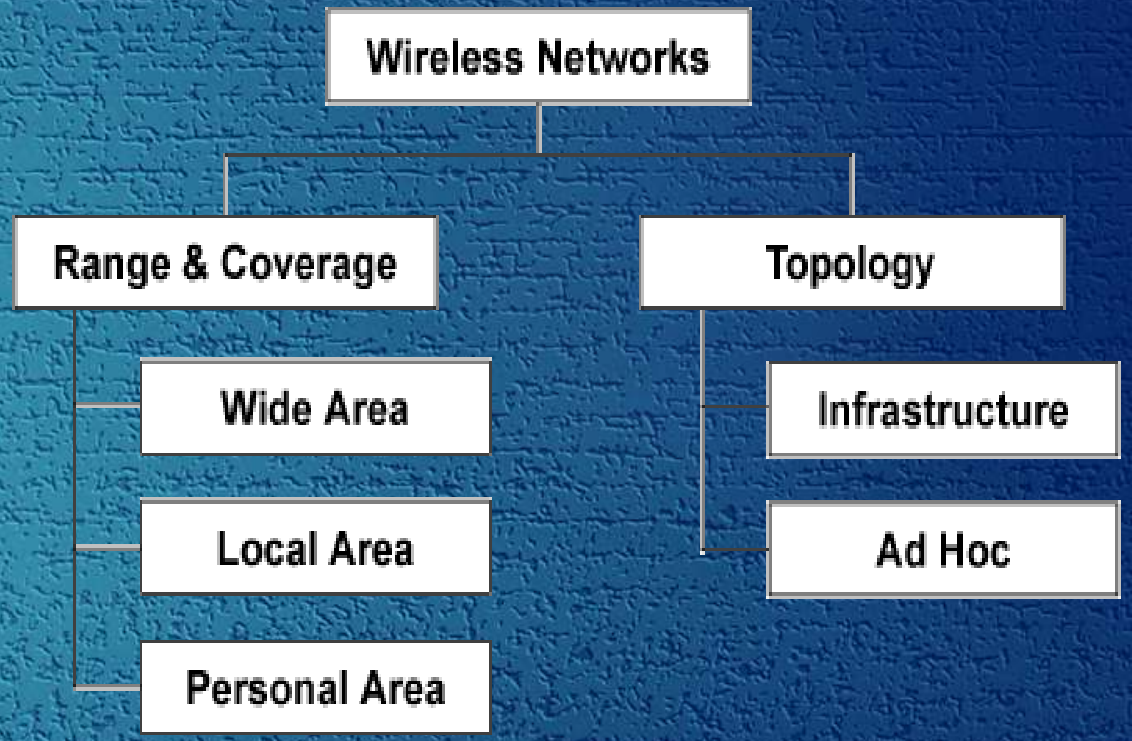
PREPARED BY: Prof. Suresh

Communication System



'What is WIRELESS TECHNOLOGIES?'

- Wireless technologies can be classified in different ways depending on their range and topologies.
- wireless technology is designed to serve a specific usage segment.
- The requirements of that's are based on a variety of variables, including Bandwidth needs, Distance needs and Power.
- The classification we see in the figure

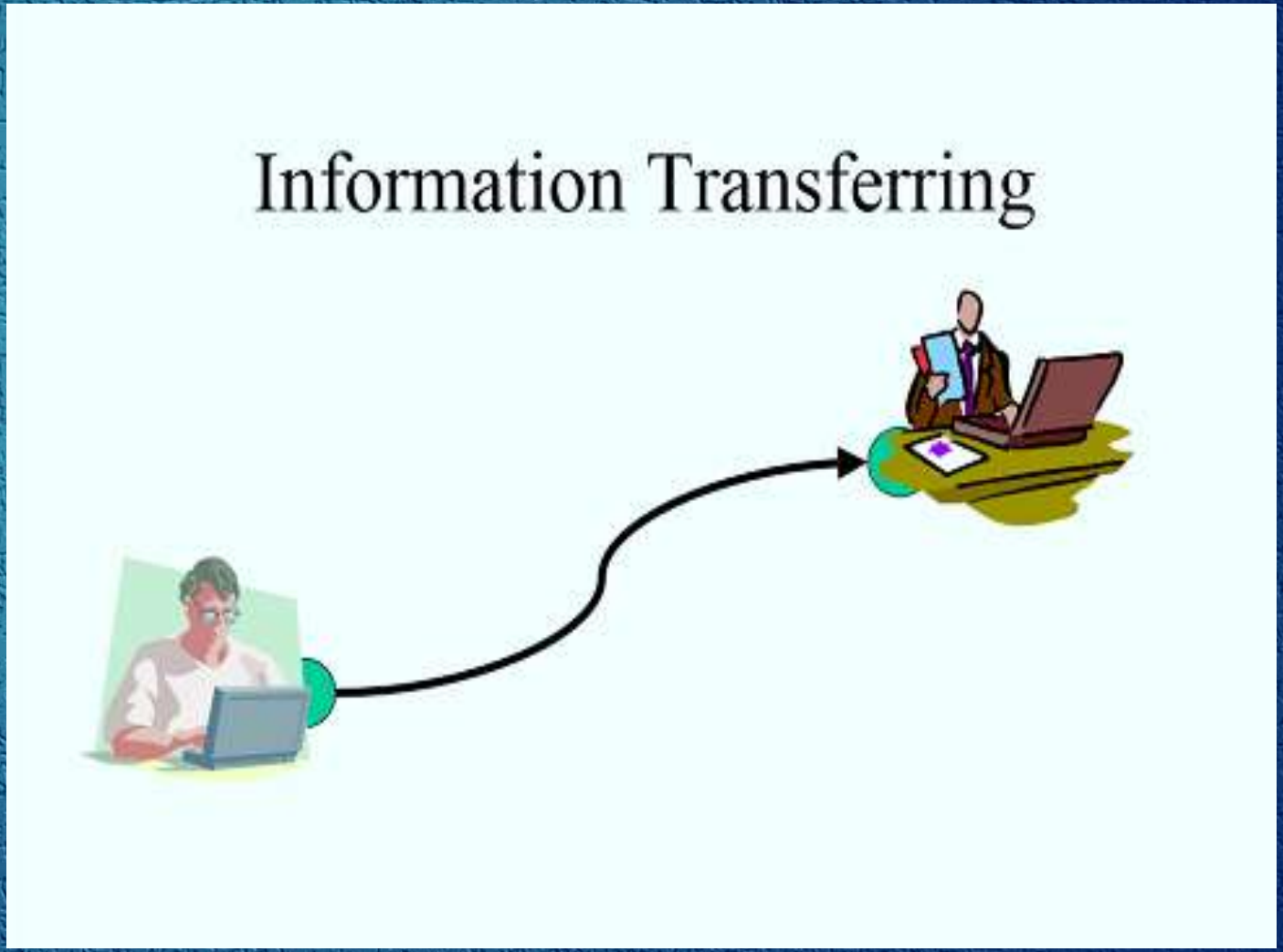


Security threats on radio communication link

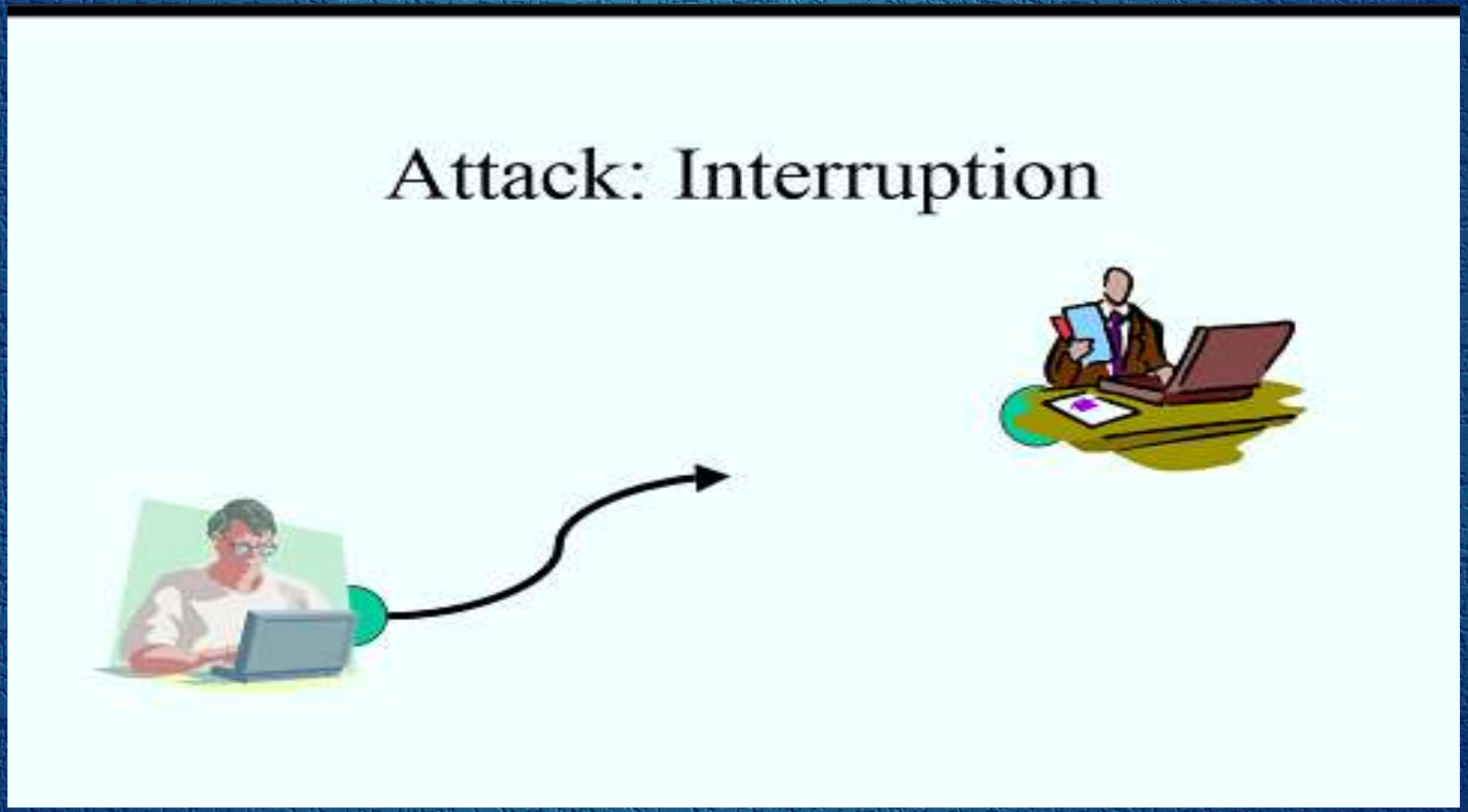
- There are mainly 4 kinds of threats related to security, that's are
- **Unauthorised disclosure (violation of confidentiality)**
- Confidentiality is a set of rules or a promise that limits access or places restrictions on certain types of information.
- An attacker listens to packets transferred on the wireless transmission medium, without being detected, and stores them.
- The packets contain user related data, either transmitted alone or in connection with user traffic.
- The user related data might be encrypted, if not the attacker is able to read, This data can be used to track user behaviour and is a privacy problem.

Unauthorised modification of data (violation of integrity)

- In this kind of security threats, the send the data or message to receiver.
- But while transferring that data or message, the third person(hacker) hack the data or message of sender.
- Then modified them and then send to receiver.
- That's kind of security threats called as violation of integrity

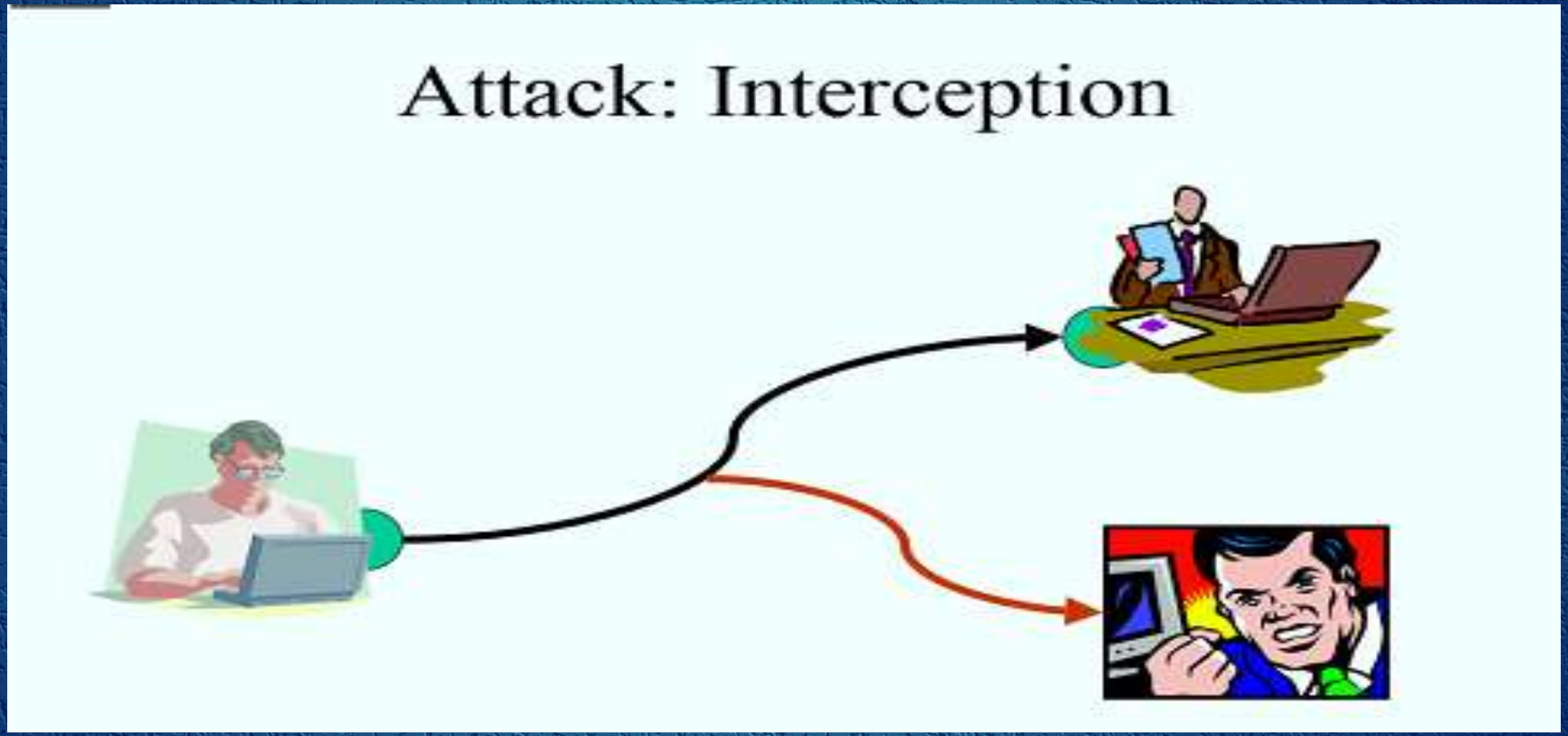


‘Unauthorised modification of data (violation of integrity)’

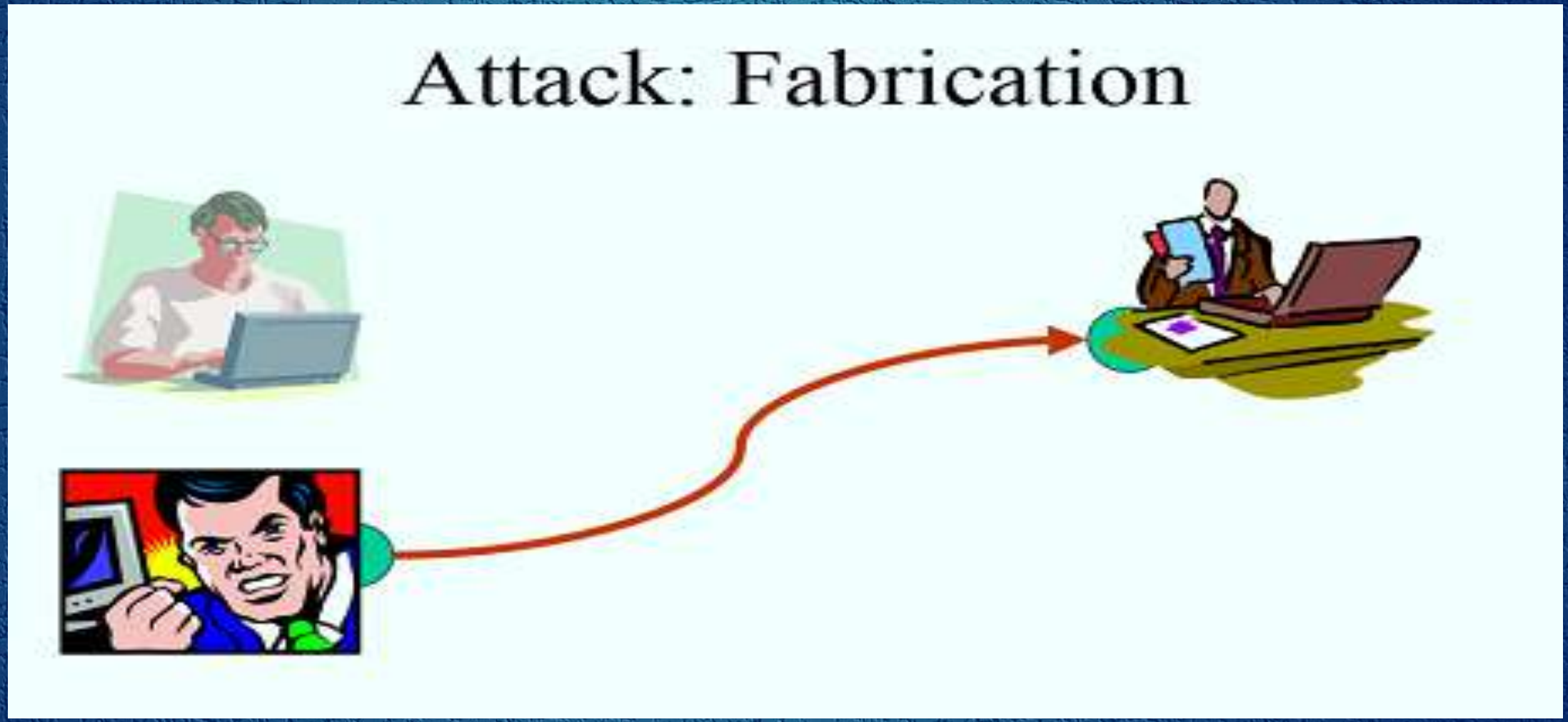


Security Threats

‘Unauthorised modification of data (violation of integrity)’



‘Unauthorised modification of data (violation of integrity)’



Disturbing network services (violation of availability)

- This threat basically allows the attacker to use the wireless network to send and receive messages without authorization.
- An attacker intentionally interferes with the wireless transmission by sending a bogus signal on the frequencies used by the wireless transmission.
- That’s called the Physical Jamming.
- An attacker intentionally sends messages on the wireless medium to confuse the victim.
- This could for example be a management message telling the victim‘s wireless device to disconnect.
- That’s called the Logical jamming.

Repudiation

- The sender can deny that he sent a particular message, which was received by another wireless device.
- This threat imposes problems for the receiving party, to reply and act on received messages.
- The receiver of a particular message can deny the reception of that message.
- The sending party can therefore not reply on messages sent.

DIFFERENT KINDS OF WIRELESS ATTACKS

- Many different kinds of wireless attacks are possible, but we focus on some main attacks, that's are describe below.
- **Accidental association**
- Unauthorized access to company wireless and wired networks can come from a number of different methods and intents.
- **Malicious association**
- "Malicious associations" are when wireless devices can be actively made by crackers to connect to a company network through their cracking laptop instead of a company access point (AP).

DIFFERENT KINDS OF WIRELESS ATTACKS

- **Identity theft (MAC spoofing)**
- Identity theft (or MAC spoofing) occurs when a cracker is able to listen in on network traffic and identify the MAC address of a computer with network privileges.
- **Denial-of-service attack**
- A Denial-of-Service attack occurs when an attacker continually bombards a targeted AP (Access Point) or network with bogus requests, premature successful connection messages, failure messages, and/or other commands. These cause legitimate users to not be able to get on the network and may even cause the network to crash.

SECURITY GOALS

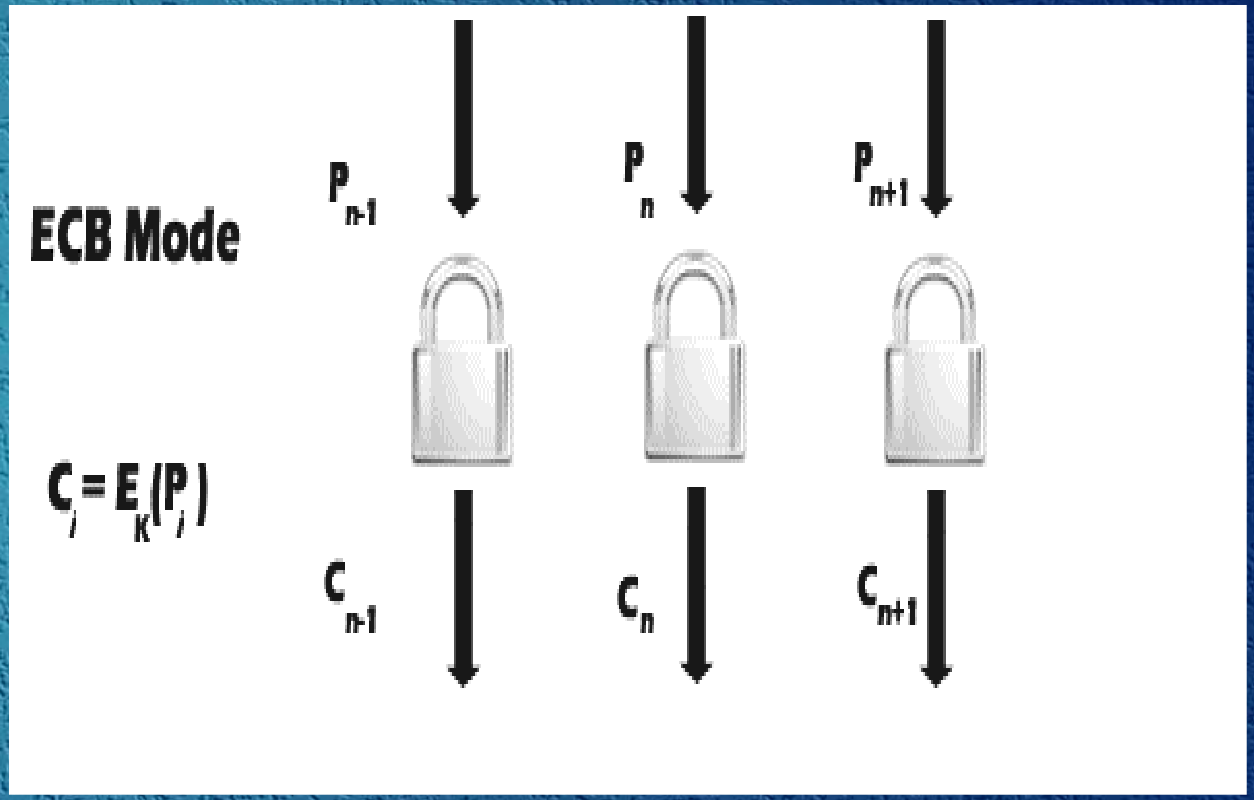
- **Authentication:**
- This means that before sending and receiving data using the system, the receiver and sender identity should be verified.
- **Secrecy or Confidentiality:**
- Usually this function (feature) is how most people identify a secure system.
- It means that only the authenticated people are able to interpret the message (date) content and no one else.
- Examples: Block Chipher and Stream Chipher

SECURITY GOALS

- **Integrity:**
- Integrity means that the content of the communicated data is assured to be free from any type of modification between the end points (sender and receiver). The basic form of integrity is packet check sum in IPv4 packets. Examples: Cryptography
- **Non-Repudiation:**
- This function implies that neither the sender nor the receiver can falsely deny that they have sent a certain message.
- **Service Reliability and Availability:**
- Since secure systems usually get attacked by intruders, which may affect their availability and type of service to their users. Such systems should provide a way to grant their users the quality of service they expect.

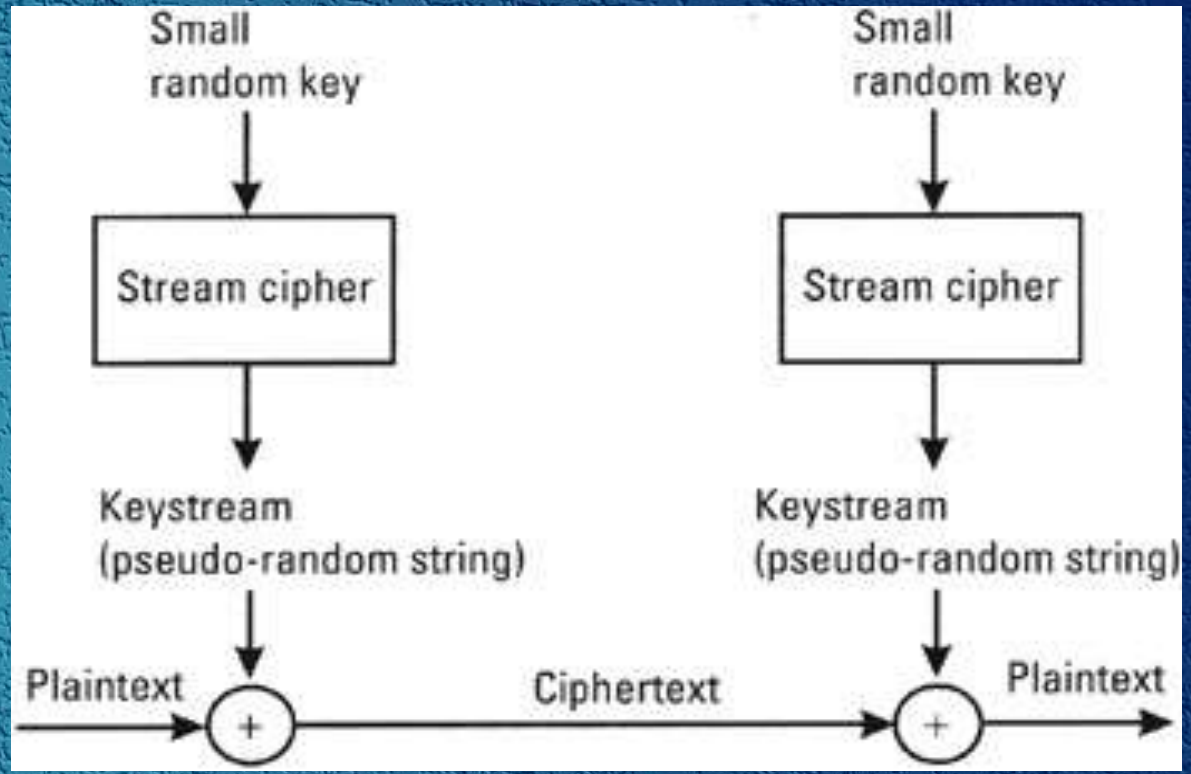
SECURITY GOALS-BLOCK CIPHER

- In this method data is encrypted and decrypted if from of blocks.
- In its simplest mode, we divide the plain text into blocks which are then fed into the cipher system to produce blocks of cipher text.
- There are many variances of block cipher, where different techniques are used to strengthen the security of the system.
- The most common methods are: ECB (Electronic Codebook Mode).
- ECB is the basic form of clock cipher where data blocks are encrypted directly to generate its correspondent ciphered blocks



SECURITY GOALS-STREAM CIPHER

- Stream cipher functions on a stream of data by operating on it bit by bit. Stream cipher consists of two major components: a key stream generator, and a mixing function.
- Mixing function is usually just an XOR function, while key stream generator is the main unit in stream cipher encryption technique.



SECURITY GOALS-DATA ENCRYPTION STANDARDS

- **DES**
- DES (Data Encryption Standard), was the first encryption standard to be recommended by NIST (National Institute of Standards and Technology).
- It is based on the IBM proposed algorithm called Lucifer.
- **AES**
- AES(Advanced Encryption Standard), is the new encryption standard recommended by NIST to replace DES.
- Both AES and DES are block ciphers.

SECURITY GOALS-DATA ENCRYPTION STANDARDS

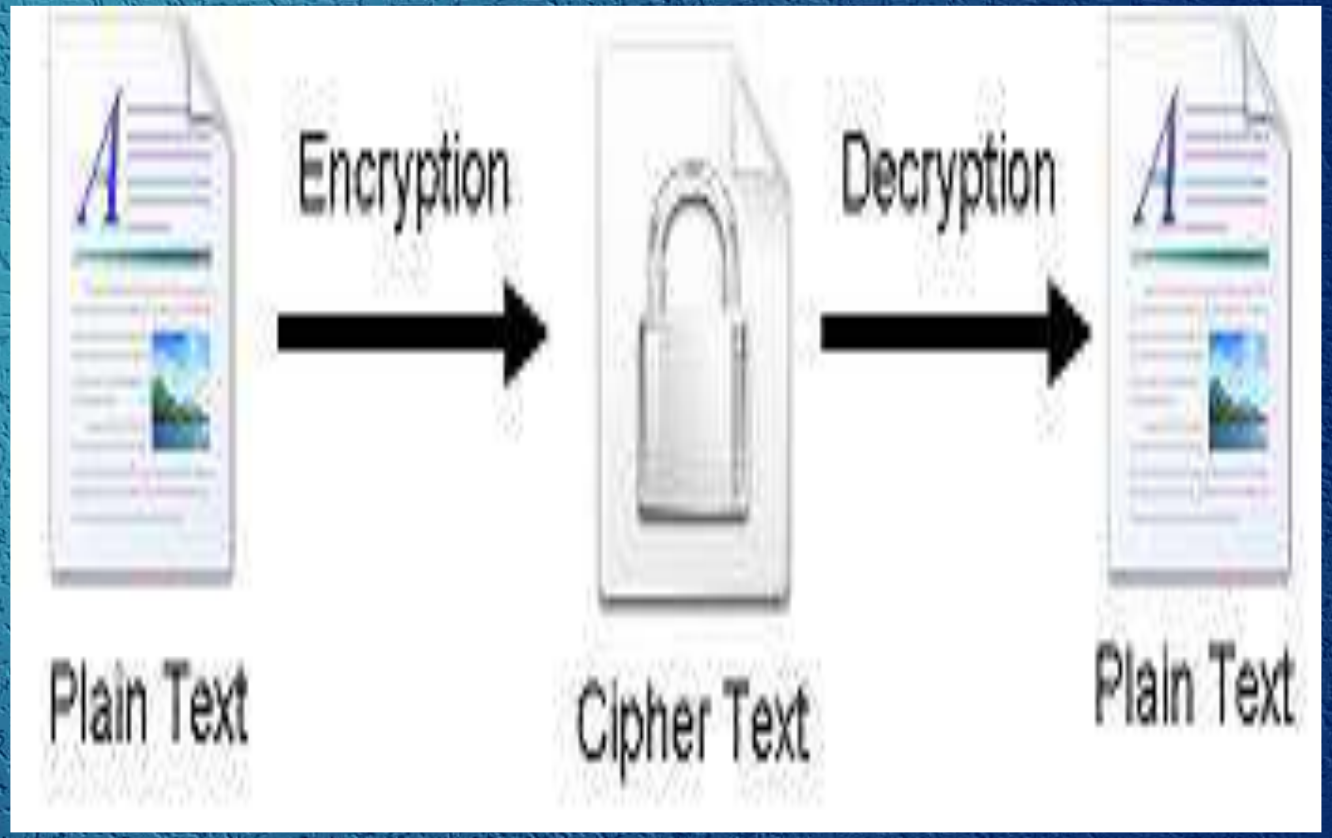
- **RC4**
- RC4 or ARC-Four is the most widely used stream cipher.
- It is used with SSL (Secure socket Layer), which is used to secure identification information and money transfers over the Internet.

SECURITY GOALS-DATA ENCRYPTION

- **CRYPTOGRAPHY**
- To send data securely between two nodes, the system must encrypt the data or "systematically scramble information so that it cannot be read without knowing the coding key".
- This concept is called as the Cryptography.
- This operation determines to a certain level the strength of the security system, the harder it is to break the encrypted message the more secure the system is to be.

SECURITY GOALS-DATA ENCRYPTION

- plain text means the " The original intelligible message" and Cipher text " The transformed message".
- Data encryption procedures are mainly categorized into two categories depending on the type of security keys used to encrypt/decrypt the secured data.
- These two categories are:
- Asymmetric and Symmetric encryption techniques.



SECURITY GOALS-DATA ENCRYPTION

1. Symmetric Encryption

- In this type of encryption, the sender and the receiver agree on a secret (shared) key.
- Then they use this secret key to encrypt and decrypt their sent messages.

2. Asymmetric Encryption

- Asymmetric encryption is the other type of encryption where two keys are used.
- In that Key1 can encrypt only Key2 can decrypt, and vice versa.
- It is also known as Public Key Cryptography (PKC), because users tend to use two keys: public key, which is know to the public, and private key which is known only to the user.