# CHAPTER 8:- NETWORK SECURITY

One of the most common ways to solve network security issues is to focus on the three most important security properties: availability, integrity, and secrecy. This is called CIA Triad.

**Confidentiality** involves protecting information from unauthorized parties. Most people think of this when they hear "network security."

**Integrity** is verifying that the information you received was not altered by an opponent.

**Availability** prevents systems and services from crashing, overloading, or being intentionally put up wrong. Denial-of-service attacks, which disrupt banks, airlines, and high schools around test time, are examples of availability reduction. Secrecy, integrity, and availability are usually the most critical security factors.


### 8.1.1 Fundamental Security Principles

It is important to deal with security issues at all levels of the network stack, but it can be hard to tell when you have done enough and when you have done it all. To put it another way, making sure security is hard. Instead, we follow a set of security standards to try to make security better as much as possible. As early as 1975, Jerome Saltzer and Michael Schroeder came up with the following classic security principles:

1. **Principle of economy of mechanism:** This idea is also known as the concept of simplicity. Bugs are more likely to be in complicated systems these days than in easy ones. Also, some people might not fully understand them and use them in a bad or unsafe way. Things that are simple to use work well.
2. **Principle of fail-safe defaults:** Let's say you need to set up how people can get to a resource. There are clear rules about when people can access the resource that are better than trying to figure out when people shouldn't be able to access it. To put it another way, a default of not having permission is better.

3. **Principle of complete mediation:** Everyone who tries to use a resource should be checked to make sure they are allowed to. This means we need a way to find out where a request came from (the requester).
4. **Principle of least authority:** Basically, this concept, which is also known as POLA, says that each subsystem should only have the power it needs to do its job. In other words, if attackers get into such a system, they only gain the bare minimum of authority.
5. **Principle of least common mechanism:** A tricky principle suggests that we should reduce the quantity of shared and dependent mechanisms among several users. Consider implementing a network routine in a user space library, which is private to the user process, rather than in the operating system, where global variables are shared by all users. The shared data in the operating system can facilitate communication between users.
6. **Principle of open design:** These states plain and simple that the design should not be secret and generalizes what is known as Kerckhoffs' principle in cryptography.
7. **Principle of psychological acceptability.** The final principle is not a technical one at all. Security rules and mechanisms should be easy touse and understand.

### 8.4.1 Introduction to Cryptography

The art of breaking ciphers, known as cryptanalysis, and the art of devising them (cryptography) are collectively known as cryptology.

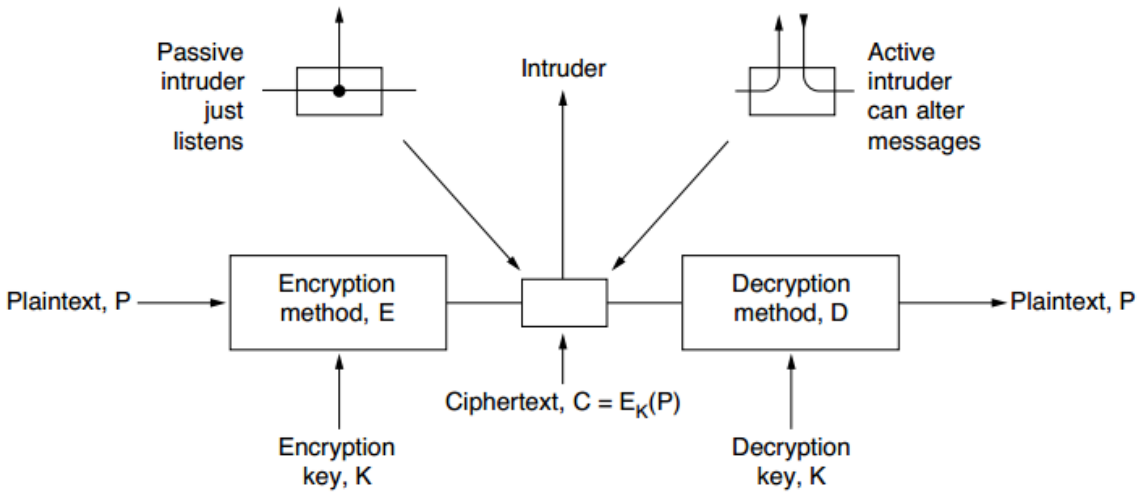


**Figure 8-9.** The encryption model (for a symmetric-key cipher).

**Plaintext:** The messages to be encrypted.

**Encryption**: Plaintext, are transformed by a function using a key.

**Ciphertext:** The output of the encryption process, known as the ciphertext, is then transmitted

**Intruder:** The enemy or unauthorized person, hears or alter messages.

### 8.4.2 Two Fundamental Cryptographic Principles

**Redundancy:** The first principle is that all encrypted messages must contain some redundancy, that is, information not needed to understand the message.

Cryptographic principle 1: Messages must contain some redundancy.

**Freshness:** The second cryptographic principle is that measures must be taken to ensure that each message received can be verified as being fresh, that is, sent very recently. This measure is needed to prevent active intruders from playing back old messages.

Cryptographic principle 2: Some method is needed to foil replay attacks