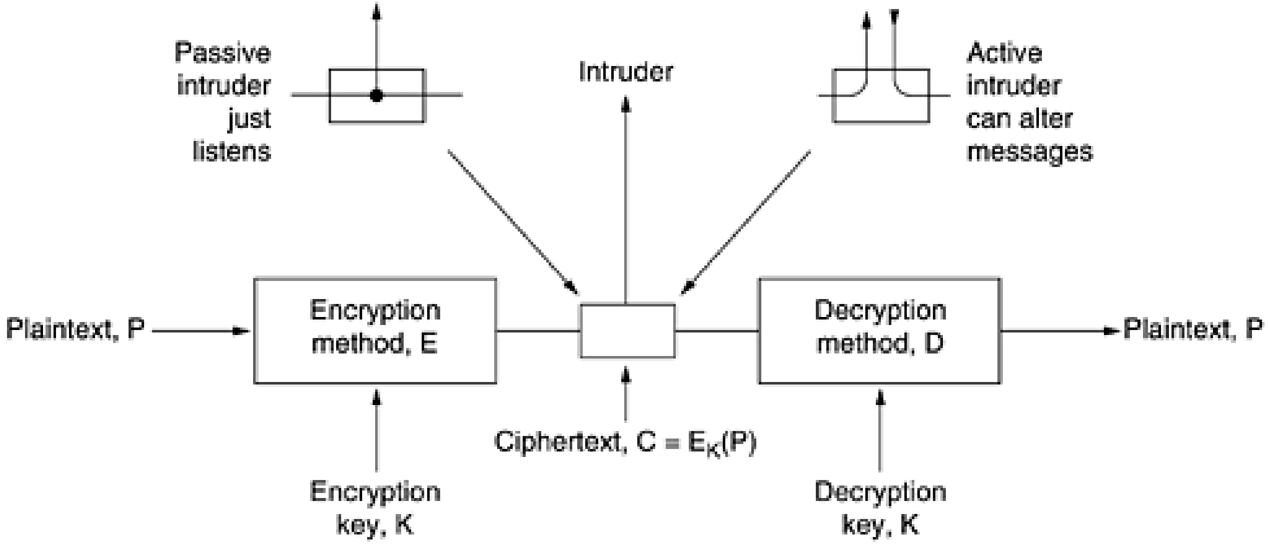
Network Security

- **Cryptography** is the study and practice of techniques for secure communication in the presence of third parties called adversaries.
- It deals with developing and analyzing protocols which prevents malicious third parties from retrieving information being shared between two entities thereby following the various aspects of information security.
- Secure Communication refers to the scenario where the message or data shared between two parties can’t be accessed by an adversary.
- In Cryptography, an Adversary is a malicious entity, which aims to retrieve precious information or data thereby undermining the principles of information security.
- Consider two parties Alice and Bob. Now, Alice wants to send a message m to Bob over a secure channel. So, what happens is as follows.
- The sender’s message or sometimes called the Plaintext, is converted into an unreadable form using a Key k. The resultant text obtained is called the Ciphertext. This process is known as Encryption. At the time of receival, the Ciphertext is converted back into the plaintext using the same Key k, so that it can be read by the receiver. This process is known as Decryption.

Figure 8-2. The encryption model (for a symmetric-key cipher)



- The messages to be encrypted, known as the **plaintext**, are transformed by a function that is parameterized by a **key**.

- The output of the encryption process, known as the **ciphertext**, is then transmitted, often by messenger or radio.
- We assume that the enemy, or **intruder**, hears and accurately copies down the complete ciphertext. However, unlike the intended recipient, he does not know what the decryption key is and so cannot decrypt the ciphertext easily.
- Sometimes the intruder can not only listen to the communication channel (passive intruder) but can also record messages and play them back later, inject his own messages, or modify legitimate messages before they get to the receiver (active intruder).
- The art of breaking ciphers, called **cryptanalysis**, and the art devising them (cryptography) is collectively known as **cryptology**.