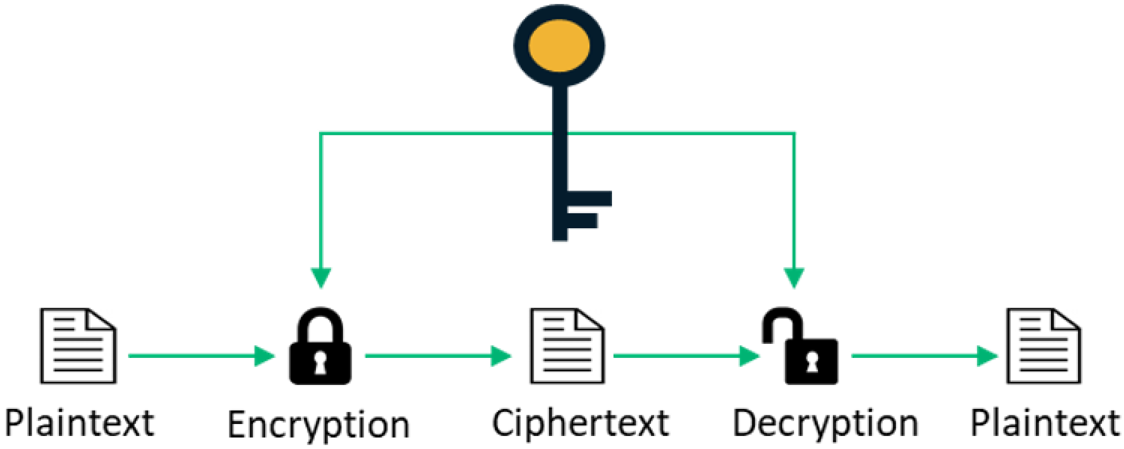
# Preliminary explanations and definitions

**Plain text :** Data that is easy to understand and there is no particular ambiguity in understanding them is called **Plain text**.
**Encryption :** The method that causes plain text to lose its comprehensibility is called **Encryption**.

### Encryption and decryption methods:



***notice :**

The algorithm or method by which text is encrypted must be reversible in order to access the original text.

**Cipher :**

It is the transformation of a character into a character or bit by bit without paying attention to the linguistic content (literature) of that message.

**Code:**

It means a conversion that replaces a word with another word or symbol.

## Kerckhoffs's principle :

1. The system must be practically, if not mathematically, indecipherable;
2. It should not require secrecy, and it should not be a problem if it falls into enemy hands;
3. It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will;
4. It must be applicable to telegraph communications;
5. It must be portable, and should not require several persons to handle or operate;
6. Lastly, given the circumstances in which it is to be used, the system must be easy to use and should not be stressful to use or require its users to know and comply with a long list of rules.

"Keep in mind that your encryption algorithm is known to the enemy, and keep your system secure by keeping the encryption key secret," Karkhoff said. Of course, this does not necessarily mean that the encryption method and algorithm should be available to everyone, but when building any algorithm, it should be assumed that everyone has access to it, in other words, system security does not depend on hiding the algorithm.