Cryptography is an Ancient Greek word in which "*crypto*" means "hidden" and "*graphy*" means "writing." It is the practice and study of [techniques](https://latesthackingnews.com/2016/11/25/brief-introduction-cryptography/) used for securing communication in the presence of third parties. Hence, only the intended person can read and process it. More precisely, it is about analyzing and developing methods and protocols that keep third parties or outsiders from accessing our private information.

In Computer Science, cryptography refers to techniques for data protection derived from mathemetical estimations called *Cryptographic Algorithms.* These algorithms change our messages in ways that are difficult for third parties to decrypt. Hence, we use them for many purposes such as encryption and decryption of messages; digital signing for message verification and authentication; private and public crypto key generation for encryption and decryption; and key exchange between sender and receiver.

**Features of Cryptography**

The five main features of Cryptography are:

1. **Confidentiality/ Privacy:** Ensuring that only the intended receiver can see the received information or message and no other person can access it.
2. **Authentication:** Confirming the identities of sender and receiver and verification of source and destination of the message.
3. **Integrity:** Assuring that the message you send to the receiver reaches them in its original form without any alteration.
4. **Non-Repudiation:** Proving that the sender sent the message and no other parties made any addition to the received message.
5. **Key Exchange:** Sharing of public and private crypto keys between sender and receiver for encryption and decryption of messages.

**Methods of Cryptography**

There are two Cryptographic methods:

**Symmetric Key Cryptography**

In this method, both sender and receiver use a single key. The sender encrypts the message using that key. The intended receiver receives the encrypted message and uses the same key to decrypt it. The problem is to send that key to the receiver in a secure way.

**Asymmetric Key Cryptography**

In this method, the sender encrypts the message using a public key, which is then sent to the receiver who decodes it using a private key. It is safer because only the receiver has the private key.

We should use encryption in today's life to protect sensitive data like personal records, company data, accounts and family photos. If this information gets into wrong hands, it may cause security issues. Nowadays, there are many Cryptographic Service Providers (CSP) for Windows, Mac, and Linux which encrypt our Fingerprint security protections, passwords, PIN, secure our emails and add digital signatures to everything which needs to be protected.