**Symmetric and Asymmetric encryption**

**Encryption** means that the sender converts original information into another form and sends the unintelligible message over the network. It helps us to secure data that we send, receives, and store. Data can be text messages saved on our cell phone, logs stored on our fitness watch, and details of banking sent by your online account.

It is the procedure of taking ordinary text, such as a text or email, and transforming it into an unreadable type of format known as "cipher text." The ciphertext is converted back to the real form when the recipient accesses the message, which is known as decryption. It helps to protect the digital information either saved on or spread through a network such as an internet on computer systems.

**Symmetric encryption**

Symmetric encryption encrypts and decrypts the information using a single password. In this encryption technique, the message is encrypted with a key, and the same key is used for decrypting the message. It is the simplest and commonly known encryption technique. It makes it easy to use but less secure.

It is called symmetric encryption because the same key is responsible for encrypting or decrypting the data. The single key used in symmetric encryption is used to encrypt plain text into ciphertext, and that same key is used to decrypt that ciphertext back into plain text.

Symmetric encryption is also called secret key encryption. The algorithm behind the symmetric encryption executes faster and less complex, so it is the preferred technique to transmit the data in bulk.

**Asymmetric encryption**

Asymmetric encryption uses two keys for encryption and decryption. It is based on the technique of public and private keys. A public key, which is interchanged between more than one user. Data is decrypted by a private key, which is not exchanged. It is slower but more secure. The public key used in this encryption technique is available to everyone, but the private key used in it is not disclosed.

The drawback of this encryption is that it takes more time than the symmetric encryption process. Asymmetric encryption is slower than secret-key encryption because, in secret key encryption, a single shared key is used to encrypt and decrypt the message, while in public-key encryption, two different keys are used, both related to each other by a complex mathematical process. Therefore, we can say that encryption and decryption take more time in public-key encryption.

In asymmetric encryption, a message that is encrypted using a public key can be decrypted by a private key, while if the message is encrypted by a private key can be decrypted by using the public key. Asymmetric encryption is widely used in day-to-day communication channels, especially on the internet.

That's about the description of both encryption techniques. Both encryption techniques have their own benefits and limitations, but from a security perspective, asymmetric encryption is a better choice.