**Symmetric Encryption**: In this encryption, a single key is used for both the encryption and decryption of the data. This means that both the sender and the receiver use the same key.

The main challenge with symmetric encryption is securely sharing the key between the communicating parties. If a third party intercepts the key during the key exchange, they could potentially decrypt the communication.

**Asymmetric Encryption**: Asymmetric encryption, also known as public-key cryptography, uses a pair of keys: a public key and a private key. The public key is used for encryption, while the private key is used for decryption.

The public key can be freely distributed, allowing anyone to encrypt messages that only the possessor of the corresponding private key can decrypt. This eliminates the need for a secure key exchange.