Symmetric Key Vs Asymmetric Key

The Basis for Comparison	Symmetric Encryption	Asymmetric Encryption
The Number of Cryptographic Keys Used	It requires just one key to help with both encryption (encoding) and decryption (decoding) of confidential data.	Requires a pair of matching keys i.e., public and private keys, to help with encryption and decryption purposes.
The Primary Purpose	Symmetric Encryption is mostly required when dealing with the transmission of bulk data. This is because it's quicker and easy to execute.	Asymmetric Encryption is a viable option if you only wish to get a secure environment for exchanging your secret keys. This is because of the complexity it has in execution and the slow speed in using it.
The Algorithms Used	Symmetric encryption uses these algorithms; AES QUAD RC4 3DES DES	Asymmetric encryption uses the following algorithms; DSA RSA EL GAMAL ECC Diffie Hellman
Ease of Use	Requires just one key hence very easy to use. No matching keys required for decrypting the encrypted data.	It requires both public and private keys, which must match for you to decrypt information. This makes it a bit difficult to use.
Performance	Simple in nature and easy to execute. Very swift.	There must be a pair of matching keys for it to work. Besides, comparing these keys can be a bit time confusing, making it another work on its own.