Symmetric Encryption In this simple encryption method, only one secret key is used to both cipher and decipher information.A query to a web server sends back a copy of the digital certificate, and a public key can be extracted from that certificate, while the private key stays private.While the oldest and best-known encryption technique, the main drawback is that both parties need to have the key used to encrypt the data before they can decrypt it. Symmetric encryption algorithms include AES-128, AES-192, and AES-256.Because it is less complex and executes faster, symmetric encryption is the preferred method for transmitting data in bulk.Asymmetric Encryption Also known as public key cryptography, asymmetric encryption is a relatively new method that uses two different but related keys to encrypt and decrypt data.Websites are secured using Secure Socket Layer (SSL) or Transport Layer Security (TLS) certificates.Asymmetric encryption presents a much stronger option for ensuring the security of information transmitted over the internet.The public key is used to encrypt data, and the private key is used to decrypt (and vice versa).Security of the public key is not needed because it is publicly available and can be shared over the internet.One key is secret and one key is public.