Asymmetric Key

Overview

Asymmetric cryptography is a technique that uses a related key pair, a public key and a personal key, to encrypt and decrypt a message and reserve it to guard against unauthorized access or unauthorized use. A public key's a cryptographic key that anyone can use to encrypt a message so that only the intended recipient can decrypt using their private key. A personal key also referred to as a secret key, is merely shared with the initiator of the key. When someone sends an encrypted message, they will extract the recipient's public key from a public directory and then use it to encrypt the message before sending it. The recipient of the message can decrypt the message with its associated private key. If the sender encrypts the message together with his private key, the message can only be decrypted; thereupon, the sender's public key authenticates. These encryption and decryption processes are administered automatically; Users don't get to lock and unlock the message physically. Many protocols are supported asymmetric cryptography, including the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocols, which enable HTTPS.
The encryption process is additionally employed by software programs that require determining a secure connection over an insecure network, like a network. B. Internet browsers or that require to validate of a digital signature. Higher data security is that the main advantage of asymmetric cryptography. It's the original secure encryption method because users never need to reveal or divulge their private keys, reducing the prospect that a cybercriminal will discover a user's private key in transit. Asymmetric cryptography also can be applied to systems where many users may have to encrypt and decrypt messages, including:

- **Encrypted email.** A public key is often wont to encrypt a message, and a personal legend is often wont to decrypt it.
- **SSL / TLS.** Asymmetric encryption is additionally used when establishing encrypted connections between websites and browsers.
- **Cryptocurrencies.** Bitcoin and other cryptocurrencies are supported asymmetric cryptography. Users have public keys that anyone can see and

personal keys that are kept secret. Bitcoin uses a cryptographic algorithm to make sure that only the rightful owners can spend it.

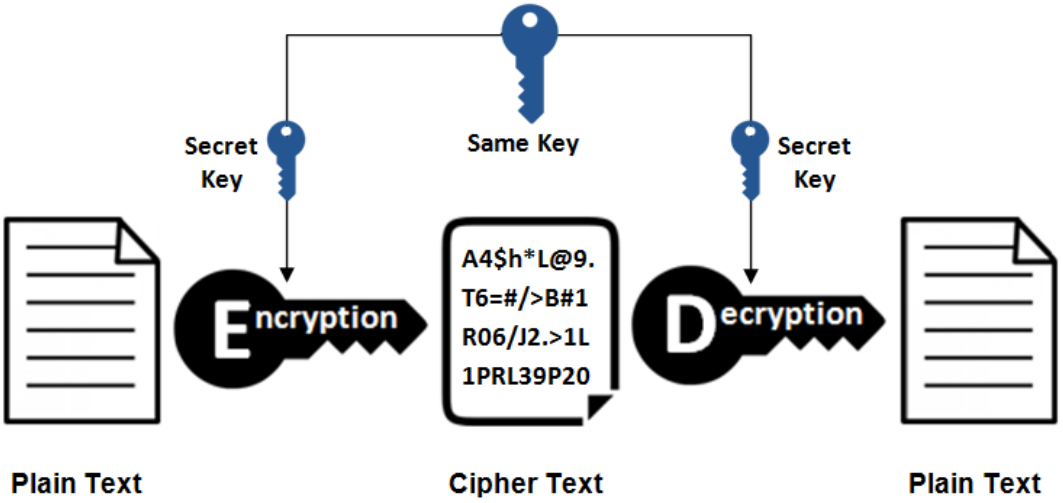

Figure 1: Asymmetric Encryption