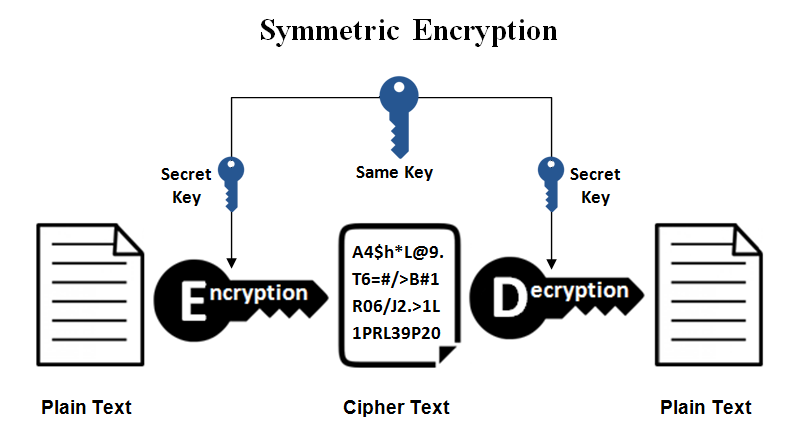
Encryption is a form of cryptography that scrambles plain text into unintelligible cipher text. They are two types of encryption which include the following: symmetric encryption and Asymmetric encryption.

**SYMMETRIC ENCRYPTION**

Symmetric encryption is also called the secret key encryption and it uses just one key called a shared secret for both encrypting and decrypting. The sender and the recipient share the key or password to gain access to the information. The key can be a word, phrase, symbols and numbers.



**Common Symmetric key algorithms:**

Symmetric encryption uses algorithms to convert data into a form that can be understood by those who have access to the secret key and they include the following.

Data Encryption Standard (DES): This is a standardized method for encrypting various models of electronic communication e.g Three-Key DES(3DES) among others.

Advanced Encryption Standard (AES) among others.

**Advantages of Symmetric encryption**

Its inexpensive relative to the protection they offer.

It is less resource intensive than Asymmetric encryption and it is an efficient way pf protecting large volumes of data. The biggest disadvantage of symmetric encryption is key management which means you need to create too many keys as the number of user’s increase.

**Application of symmetric encryption in data security.**

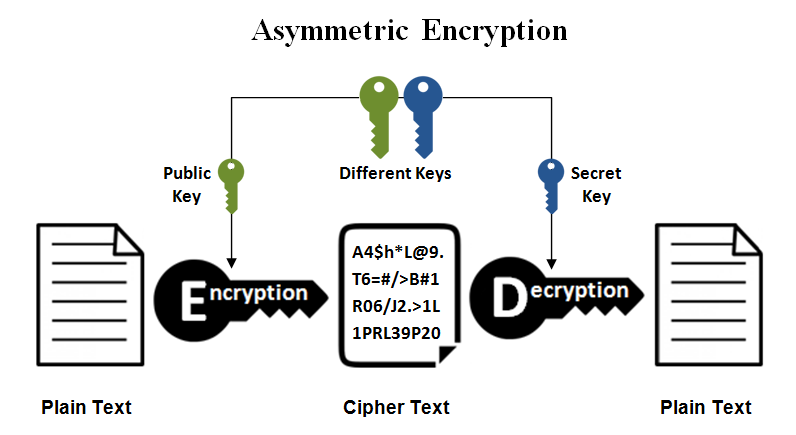
Securing messaging apps e.g watsup, signals. Messaging apps use symmetric encryption such as signal protocol to ensure that messages are encrypted end to end allowing only the intended recipients to read the content.

File encryption software e.g. Ax crypt, Vera Crypt: Symmetric algorithms like AES are employed by file encryption software to protect sensitive data stored on devices, ensuring data remains secure even if the device is lost or stolen.

BitLocker: When you activate Bit locker on windows computer to encrypt all hard drives.BY unlocking the PC with his/her password, the user will decrypt data without the risk of exposing its secret encryption key.

**ASYMMETRIC ENCRYPTION**

Asymmetric encryption is also known as the public key cryptography. Asymmetric Encryption encrypts and decrypts data using two separate keys. These keys are known as the public key and a private key. The private key is used for decrypting while the public key is used for encryption. Some of the examples of asymmetric key encryption include the following: Rivest Shamir Adelman(RSA), Digital Signature Standard(DSS) among others



**How does Asymmetric Encryption work?**

Asymmetric Encryption uses two distinct, yet related keys. One key, the public key, is used for encryption and the other the private key is used for decryption. The private key is intended to be private so that only the authenticated recipient can decrypt the message. A public key is available for anyone who needs to encrypt a piece of information. This key does not work for the decryption process. A user needs to have a secondary key, private key to decrypt the information.

**How asymmetric encryption is applied in data security.**

Digital Signatures for document authenticity and integrity e. g adobe sign i. e when a user signs a document digitally, their private key is used to create a unique signature. The recipient can then verify the authenticity and integrity of the document using the senders public key. This conforms the identity of the of the signer.

Security key exchange and establishment in SSL protocol for secure websites. Asymmetric encryption is used for secure exchange of a symmetric encryption key which is then used to encrypt and decrypt data for the remainder of the session.

Securing email communication. Asymmetric encryption is used in securing email communication protocol such as pretty Good Privacy(PGP) where these protocols act as a leverage between public and private keys to encrypt email content ensuring that only the intended recipient with the correct private key can decrypt and read the message.

**Benefits of asymmetric encryption**

The key distribution is eliminated because there is no need for exchanging keys

Security is increased since private keys don’t have to revealed.

**Disadvantages of asymmetric key encryption**

It is slow process compared to symmetric

If an individual loss his private key, he can’t decrypt the message.