Symmetric Key

Overview

In cryptography, an asymmetric key is a key that is used to encrypt and decrypt information. This means that decrypting information requires the same key that was used to encrypt it. In practice, keys represent a secret shared between two or more parties that can be used to maintain a private information connection. This requires that both parties have access to the secret key is one of the main disadvantages of symmetric key encryption compared to public-key encryption. By using symmetric encryption algorithms, the data is converted into a form that cannot be understood by anyone who doesn't have the secret key to decrypt it. Once the intended recipient, who has the key, has the message, the algorithm reverses its action to return the message to its original, understandable form. The secret key used by both sender and recipient can be a specific password/code or a random sequence of letters or numbers generated by a secure random number generator (RNG).

Following are types of symmetric encryption algorithms:

- **Block algorithms**. Fixed bit lengths are encrypted in electronic data blocks using a specific secret key. Since the data is encrypted, the system keeps it in its memory while waiting for entire blocks.
- **Flow algorithms**. Data is encrypted during transmission rather than stored in system memory.

The success depends on the strength of the random number generator used to generate the secret key. It is widely used today and mainly consists of two types of algorithms, block, and stream. Some common encryption algorithms include Advanced Encryption Standard and Data Encryption Standard. This type of encryption is generally much faster than asymmetric but requires that both the sender and the data recipient have the secret key. DES, one of the standard symmetric essential encryption methods, modifies the best symmetric essential methods by the National Institute of Standards and Technology. Your symmetric key is 56 bits long. When text is encrypted, it is divided into 64-bit components. Each component is encrypted with the symmetric key, after which all the ciphertext is sent to its destination over the Internet. At the goal, the

ciphertext is decrypted with the same key to generate the original text. Some examples of symmetric encryption algorithms are:

- AES (Advanced Encryption Standard)
- DES (Data Encryption Standard)
- IDEA (International Data Encryption Algorithm)
- Blowfish (Drop-in replacement for DES or IDEA)
- RC4 (Rivest Cipher 4)
- RC5 (Rivest Cipher 5)
- RC6 (Rivest Cipher 6)

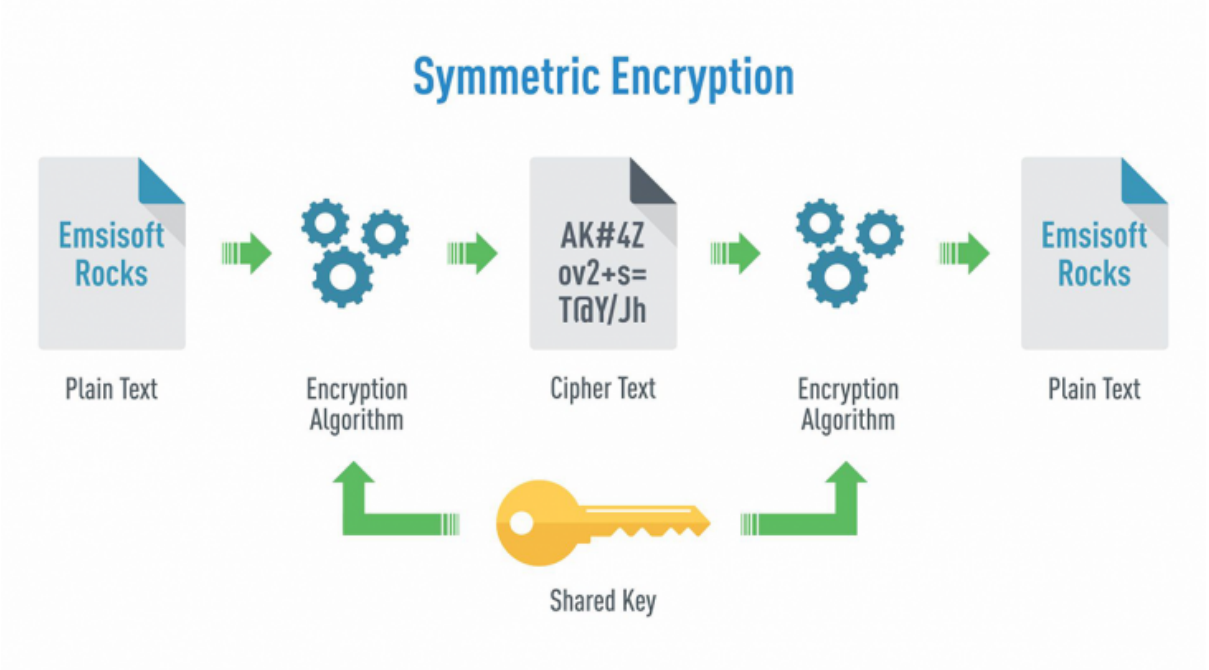

Figure 1: Symmetric Encryption