# Keys in Cryptography

## Symmetric Key Cryptography

Symmetric Key is the type of key which uses only one key for encryption and decryption. This key is called secret key, and this type of key is also known as secure secret key.

Symmetric Key Cryptography uses only one key for encryption and decryption so it is easy to understand and implement. And the complexity of implementation is very less because this key cryptography uses only one key. And it can be easily hacked by the attackers if they know the secret key.

## Asymmetric Key Cryptography

Asymmetric Key is also known as Public Key Cryptography. This cryptography algorithm uses two keys "Public Key" and "Private Key". In this cryptography, the sender uses '**Public Key**' of the receiver on the plain text to make it **cipher** or **encrypted text**.

In this cryptography, an attacker cannot decrypt the message without the '**Private Key**' of the receiver. The complexity is of this cryptography is high and implementation is not easy. So this cryptography is slow than **Symmetric Key Cryptography**.

**Public Key:**

Public Key is the type of key which is known by everyone and the key which is shared key is also known as **Public Key**.

**Private Key:**

Private Key is the key that is only known by its private user and this key is not shared key.

**Active Attack:**

An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data on route to the target

**Passive Attack:**

A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities.

**Difference between Symmetric and Asymmetric Key**

| Symmetric Key | Asymmetric Key |
|---|---|
| i) This type of Cryptography uses single key concept. | **i)** This type of Cryptography uses two key concept. |
| **ii)** It uses Secret and Private Key Cryptography. | **ii)** Asymmetric Key uses Public Key Cryptography. |
| **iii)** Complexity of Symmetric key cryptography is less. | **iii)** Complexity of Asymmetric key cryptography is high. |

| | |
|---|---|
| **iv)** Complexity is less, So utilization of resources is less. | **iv)** Complexity is high, So utilization of resources is more. |
| **v)** This type of cryptography uses DES and AES algorithms. | **v)** This type of cryptography uses RSA and diffien-Hellman algorithms. |
| **vi)** In this key cryptography Transmission of data in Bulk. | **vi)** In this key cryptography exchanging the key is Securely. |
| **vii)** In Symmetric Key Security is less, So the uses of resources is less. | **vii)** In Asymmetric Key Security is high, So the uses of resources is high. |

**Stream Cipher**

When we apply keys & algorithms on every bit of data or msg. is called stream cipher.

Example: One Time Pad.

**Key Stream Generator**

Key Stream Generator, generates the key in the form of bits.

**Block Cipher**

Block Cipher divides plain text into the blocks. And every block size is 64 bits. In this **Keys** & **Algorithms** applies on every block of the plain text.

**Example:** DES.

## Connect with Geeks Help Team

Website: Geeks Help

Linkedin: Raju Sheoran

Instagram: Raju Sheoran