# Difference between symmetric and asymmetric encryption

You all must be aware that encryption is when the form of a message is changed to prevent someone else from reading it. Thus, it provides data security. There are two types of encryption available: symmetric and asymmetric encryption. Symmetric encryption is an old technique but asymmetric encryption is relatively new which overcame the data security flaws of symmetric. The main difference between these two encryption techniques is the use of keys to encrypt and decrypt the message.

## Symmetric key encryption

In symmetric encryption, there is only one key that is used to encrypt and decrypt the message. In other words, the data security of symmetric key encryption is less because if the key for encryption is figured out then the message can be easily decrypted. You will need a safe path to transfer the encryption key to the other end for decryption. However, this encryption is generally fast than asymmetric.

## Asymmetric key encryption

In asymmetric key encryption, there are two different keys for encryption and decryption of message. It is based on public encryption key and private decryption key concept. Thus, it provides more data security in sending encrypted message but, it is slower than symmetric key encryption.

## Some other differences

Other than the key and speed of symmetric and asymmetric encryption, there are some other differences between the two methods.

### Size of cipher text:

In symmetric encryption, the size of cipher text is smaller than the original text. On the other hand, in asymmetric, the size of cipher text is larger than the original.

### Usage:

Symmetric encryption is used when large amount of data is to be transferred whereas; asymmetric encryption is used when small amount of data is send.

### Resource utilization:

In symmetric encryption resources utilization is low as compared to the resource utilization in asymmetric encryption.

### Length of keys:

In symmetric encryption the length of keys is usually 128 or 256 bits whereas in asymmetric encryption, the length of key is large. The recommended RSA key length is 2048 bits.

### Examples

The examples for symmetric encryption algorithms include: RC4, AES, DES, 3DES, and many more. Likewise, the examples for asymmetric encryption algorithm include: RSA, Diffie-Hellman, ECC, etc.

## Conclusion

Data security is very crucial and you should choose your encryption technique very carefully. Both symmetric and asymmetric encryptions have their own benefits and flaws. The method which best suits your needs should be given priority.