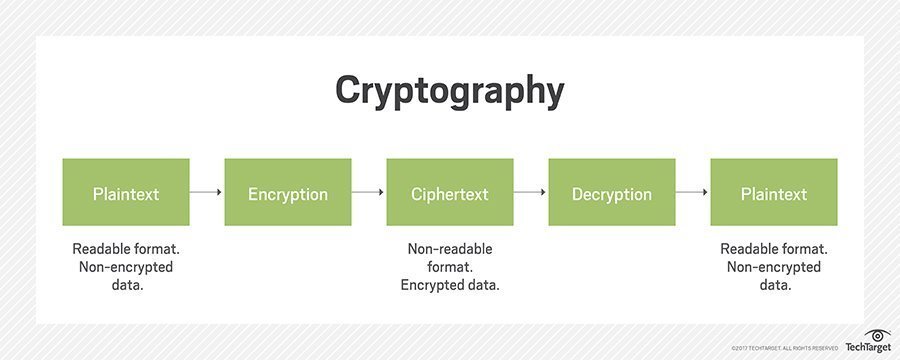
[INTRODUCTION TO INFORMATION AND NETWORK SECURITY](#_2wm8ukrn83gq) **1**

# **INTRODUCTION TO INFORMATION AND NETWORK SECURITY**

What is Cryptography ?

Cryptography is a method of protecting information and communications through the use of codes so that only those for whom the information is intended can read and process it. The prefix "crypt" means "hidden" or "vault" and the suffix "graphy" stands for "writing."

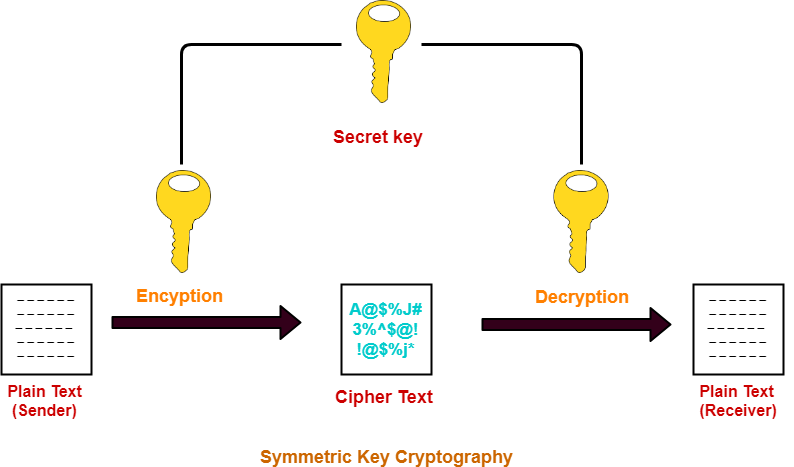


2. What is Symmetric and Asymmetric Cryptography ?

**Symmetric Key Cryptography**

Anencryption system in which the sender and receiver of a message share a single, commonkey that is used to encrypt and decrypt the message. Contrast this withpublic key cryptography which utilizes two keys - a public key to encrypt messages and a private key to decrypt them.

Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Public-key encryption avoids this problem because the public key can be distributed in a non-secure way, and the private key is never transmitted.Symmetric-key cryptography is sometimes called secret-key cryptography*.*



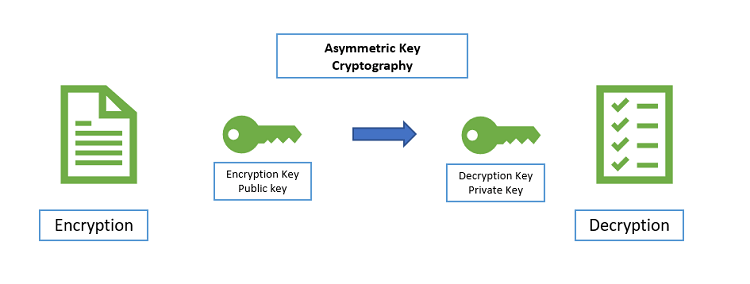
Symmetric cryptosystems have a problem of key transportation. The secret key is to be transmitted to the receiving system before the actual message is to be transmitted. Every means of electronic communication is insecure as it is impossible to guarantee that no one will be able to tap communication channels. So the only secure way of exchanging keys would be exchanging them personally.

**Asymmetric Key Cryptography**

Asymmetric [cryptography](https://searchsecurity.techtarget.com/definition/cryptography), also known as public key cryptography, uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric).

One key in the pair can be shared with everyone; it is called the [public key](https://searchsecurity.techtarget.com/definition/public-key).

The other key in the pair is kept secret; it is called the [private key](https://searchsecurity.techtarget.com/definition/private-key).



A message that is encrypted using a public key can only be decrypted using the private key, while also, a message encrypted using a private key can be decrypted using a public key. Security of the public key is not required because it is publicly available and can be passed over the internet. Asymmetric key has a far better power in ensuring the security of information transmitted during communication.

References:

<https://searchsecurity.techtarget.com/definition/asymmetric-cryptography>

https://www.webopedia.com/TERM/S/symmetric\_key\_cryptography.html