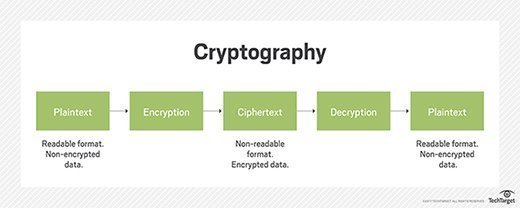
**What is cryptography?**

Cryptography or cryptology is the practice and study of techniques for secure communication in the presence of third parties called adversaries.

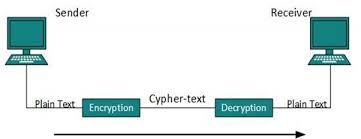
Cryptography involves creating written or generated codes that allow information to be kept secret. Cryptography converts data into a format that is unreadable for an unauthorized user, allowing it to be transmitted without unauthorized entities decoding it back into a readable format, thus compromising the data.



**Use of cryptography:**

Modern **cryptography** uses sophisticated mathematical equations (algorithms) and secret keys to encrypt and decrypt data. Today, **cryptography** is **used to** provide secrecy and integrity to our data, and both authentication and anonymity to our communications.

How it work:

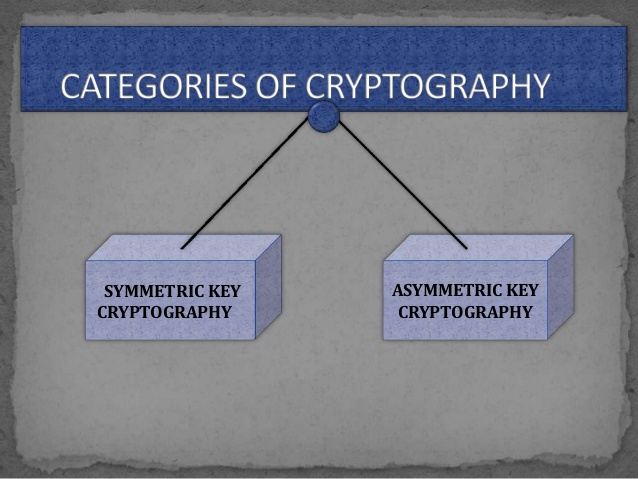


**Importance of cryptography:**

Cryptography can be used for non-technological reasons like hiding physical messages, or creating ciphers so that only you and your friends can read your messages, but nowadays it is used for more vital reasons. It is the basis for Data Encryption.   
Cryptography is used to make sure all of the things that I listed above *shouldn't* happen. I say shouldn't because nothing is perfect, and people can usually find loops holes or ways around the rules. Cryptography takes math and uses it to develop algorithms for computer systems to use to secure data either before data transfer or just for secure data storage.

**Types of cryptography:**

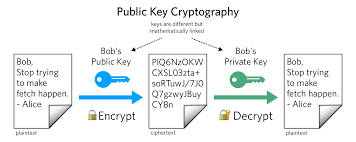
A cryptographic system typically consists of algorithms, keys, and key management facilities. There are two **basic** types of cryptographic systems: symmetric ("private key") and asymmetric ("public key").

****

**Public key cryptography (asymmetric cryptography):**

**Public key cryptography** (PKC) is an **encryption** technique that uses a paired **public** and **private key** (or asymmetric**key**) algorithm for secure data communication. A message sender uses a recipient's **public key** to encrypt a message. To decrypt the sender's message, only the recipient's **private key** may be used.

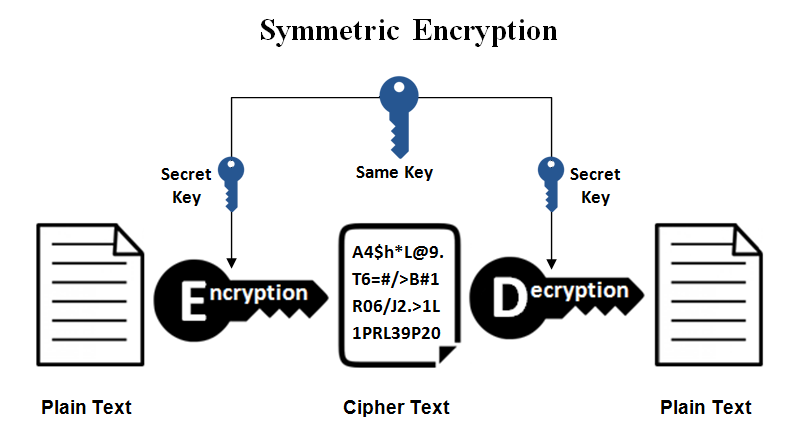
PKC is also known as public key encryption, asymmetric encryption, asymmetric cryptography, asymmetric cipher, asymmetric key encryption and Diffie-Hellman encryption.

****

**Private key cryptography (symmetric key cryptography):**

A **private key** is a tiny bit of code that is paired with a **public key** to set off algorithms for text **encryption** and decryption. It is created as part of **public key cryptography** during asymmetric-**key encryption** and used to decrypt and transform a message to a readable format.

A private key is also known as a secret key, symmetric cryptography.



**Transposition Ciphers**

References:

<https://www.edureka.co/blog/what-is-cryptography/>

<https://www.slideshare.net/kusum21sharma/cryptographyppt>

<https://www.quora.com/What-is-cryptography-and-why-is-it-important>

<https://www.techopedia.com/definition/1770/cryptography>