# What is Public Key Cryptography?

I am not qualified to explain public key cryptography. Please refer to this link for more information.
(https://auth0.com/blog/how-to-explain-public-key-cryptography-digital-signatures-to-anyone/)

Public key cryptography generally refers to we have 2 keys that are mathematically linked to each other which are public and private key. Public key cryptography generally has 3 types which are public key encryption (asymmetric encryption), digital signature (not the same as electronic signature) and Diffie Hellman Key Exchange.

Through the link you may have already understand the first 2 types of public key cryptography which are asymmetric encryption and digital signature. The argument of public key cryptography was it's impossible to find back the private key given any public key. However, given any private key it's possible to find or generate the public key.

In asymmetric encryption, when we want to decrypt the message by using the private key, the bigger the private key in sizes, the slower the process gets whereas in digital signature, when we want to encrypt the message by using the private key, the bigger the private key in sizes, the slower the process gets.

Depending on the situation, you may or may not need to know what's diffie hellman key exchange. (https://www.youtube.com/watch?v=NmM9HA2MQGI) – Explain through color mixing, (https://www.youtube.com/watch?v=Yjrfm_oRO0w) – Explain through mathematics. This is in general how Diffie Hellman Key Exchange works.