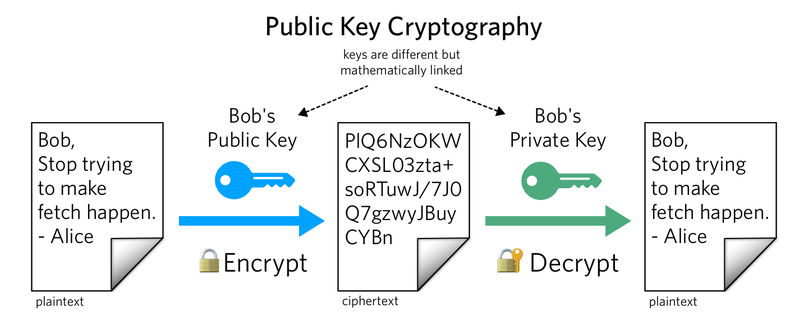
**Public key cryptography:**

Public key cryptography, also known as **asymmetric cryptography**, uses **two separate keys** instead of one shared one: a **public key and a private key**. Public key cryptography is an important technology for Internet security.

Public key cryptography is a method of **encrypting or signing data with** two different keys and making one of the keys**, the public key**, available for anyone to use. The other key is known as the private key. Data encrypted with the public key can only be **decrypted with the private key**. Because of this use of two keys instead of one, public key cryptography is also known as [asymmetric cryptography](https://www.cloudflare.com/learning/ssl/what-is-asymmetric-encryption/). It is widely used, especially for [TLS/SSL](https://www.cloudflare.com/learning/ssl/transport-layer-security-tls/), which makes [HTTPS](https://www.cloudflare.com/learning/ssl/what-is-https/) possible.



**In the above image, Alice sends Bob an encrypted message using Bob’s public key. Once Bob receives the message from Alice, Bob decrypts the message using his private key.**

* Public Key — to be shared
* Private Key — to be kept secret

These keys are generated at the same time using an algorithm and are mathematically linked. When using the RSA algorithm, the keys are used together in one of the following ways:

**1. Encrypting with a public key**

Use case: sending messages only the intended recipient can read.

Bob encrypts a plaintext message with Alice's public key, then Alice decrypts the ciphertext message with her private key. Since Alice is the only one with access to the private key, the encrypted message cannot be read by anyone besides Alice.

**2. Signing with your private key**

Use case: verifying that you're the one who sent a message.

Alice encrypts a plaintext message with her private key, then sends the ciphertext to Bob. Bob decrypts the ciphertext with Alice's public key. Since the public key can only be used to decrypt messages signed with Alice's private key, we can trust that Alice was the author of the original message.

These methods can also be combined to both encrypt and sign a message with two different key pairs.

When you create a crypto wallet with a wallet provider, you will receive all these four elements. Here is the role of each of these 4 concepts for you as a wallet user:

1. You create a **private key** when creating a crypto wallet. You never do anything with it consciously, but it is **used to sign your transaction when you send crypto assets.**
2. You create a **secret phrase and store it safely on a piece of paper**. You use it if you ever have to **restore your crypto wallet funds after losing the private key**.
3. The **public key is used to verify** **that you are the owner of a wallet address** and that you can receive crypto assets. You personally don’t use your public key when making or receiving a transaction.
4. You tell your **wallet address to the sender if you are to receive a transaction** or use it if you yourself send money there from another wallet of the same cryptocurrency. Likewise, you need the wallet address of a recipient if you are to send crypto assets to them.

*Note: To know more about wallet, refer documentation on wallet available on the github*