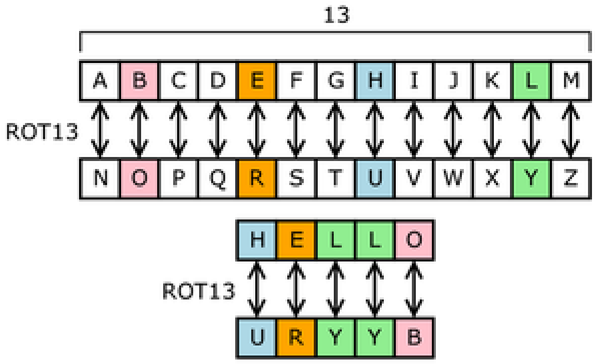
Cryptography

Why are these blockchain-based digital assets called *crypto*currencies? Sure, they represent value and can be circulated like currency—but where does the *crypto* part come into play? Interestingly enough, the backbone of blockchain technologies lies in mathematical cryptography that has been studied for decades.

> *Task:* Watch this video as an introduction to the principles of cryptography.

Symmetric Cipher

Symmetric ciphers are encryption schemes in which the parties involved share a secret that is used to encode and decode messages. Consider the example of a substitution cipher, in which characters from a given alphabet are mapped to a new alphabet (often the same symbols in a different order).



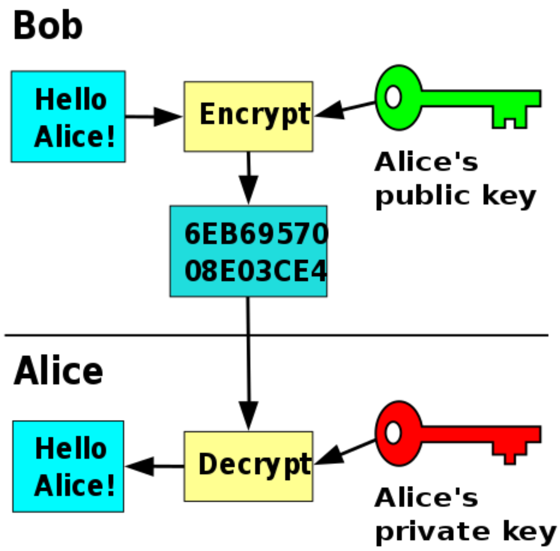
Now imagine Alice wants to send a secret message to Bob. She would substitute the plaintext characters with their cipher text counterparts according to the mapping she defined. Let's say an eavesdropper named Eve intercepted the message while in transit—the message would appear as gibberish to her! Once Bob receives the message, he can decrypt it by reversing the substitutions that Alice made. The important thing to note is that both Alice and Bob would need to know how the letters are mapped in order to encrypt and decrypt messages. The fact that the same secret must be known between Alice and Bob is what characterizes a symmetric cipher.

Symmetric ciphers are not used in blockchain, but the principle of a secret being used to securely transmit messages certainly is. The next section introduces asymmetric ciphers, which have the same goal of encryption and decryption, but a different approach.

Public-key Cryptography

In contrast, *asymmetric* ciphers are characterized by the fact that only one end of communication needs to hold a secret to decrypt messages. Asymmetric cryptography is more commonly referred to as public-key cryptography, due to its use of a public/private key pair.

In such cryptosystems, anyone who intends to receive messages must create a pair of keys—one of which is public and can be published openly, and another which remains private. The public key can be used by anyone to encrypt messages; however, only the holder of the corresponding private key can decrypt those messages. The discrepancy of information between the two parties is what makes the cryptosystem "asymmetric". The process looks like this:



In the context of bitcoin, instead of Bob sending "Hello Alice!" as his message, he may send an amount of BTC. He encrypts this message with Alice's public key and sends it. Because Alice kept her private key a secret, only she will be able to decrypt the message and spend the bitcoin.

One-way Functions

As was explained in the previous sections, public-key cryptography uses a pair of cryptographic keys to encrypt and decrypt messages. For all intents and purposes, a private key is just a "random" number between 0 and 2^{256}.

The private key is used to generate the public key through the use of an one-way functions. The defining principle of a one way function is that given inputs, the output is easily calculable; but when an output is known, the corresponding input is virtually impossible to deduce. As an illustration, imagine you were given two different colors of paint. You can mix the paint easily, but un-mixing the paint is a whole different story. That's the idea of a one-way function.

There is a one-way function involving elliptic curve cryptography that takes the private key as input and produces the public key as output. You can freely use the public key without compromising the private key, thanks to *one-way* functions.