Programming fundamentals with Python

Pepe García

2020-04-20

Programming fundamentals with Python

Plan for today

Cryptography

Public key cryptography

PKI + HTTP

Blockchain

Cryptography

Cryptography studies how to secure communications

Cryptography

Simplest crypto algorithm we can think of?

Caesar's cypher

Cryptography

In Caesar's cypher both parties share the key (the number of traspositions to make to each letter) in order to hide communication

Symmetric encryption

Public key crypto

Public key crypto (or asymmetric crypto) is slightly different than symmetric.

One key encrypts the message

A different key decrypts the message

Public key crypto

Public key crypto

What advantages does this system have?

Public key crypto

In PKI, messages encrypted with the public key can only be decrypted with the private key, and messages encrypted with the private key can only be decrypted with the public key

But why is it useful to encrypt a message with my own private key, if anyone can decrypt it?

Signatures

Apart of encryption, the public-private key infrastructure (**PKI**) provides the ability to sign messages, allowing us to prove our identity or check others!

Public key crypto

Then, if PKI is that cool, why isn't everything using it?

Symmetric cryptography is faster

Symmetric cryptography can work on bigger chunks of data

Public key crypto

HTTPS

HTTPS uses the best of both worlds, symmetric and asymmetric encryption.

It uses asymmetric encryption to maintain a secure channel, and then both parties share a encrypted symmetric key

HTTPS

HTTPS

How does it actually work?

MiTM

Blockchains

The idea of blockchains is fairly simple. They are distributed ledgers, in which different parties try to write blocks and the actual balance can only be known by reading all rows in the ledger.

Blockchains

Blockchains

Let's do a ~~ledger~~ **blockchain** ourselves!

Exercises

Exercise 1

Investigate how to create a PGP key pair. When you do it, do not share the private key with anyone.

Exercise 3

Add your public key to your github profile. Follow the steps described in

https://help.github.com/articles/generating-a-new-gpg-key/