TP digital signatures

October 26, 2020

1 Preliminaries

Find an implementation of a signature scheme in your language. List of signatures schemes:

- ECSDA
- EdDSA
- RSA
- Schnorr

Map the given API to the one in the course. Then try to generate some keys and sign a message. You will maybe need a random generator, usually you can use the OS's one.

2 Public Key Infrastructure

2.1 Authority

Generate a pair of public private key and store them (this will be the keys of the authority)
Create a function that takes as input a public key and output the signature of the public key under the authority's key

2.2 Sub Authorities

Generates another key pair (this will be the sub authority's keys). Create a function that takes as input a public key, the authority secret key and outputs the sub authority public key, and the authority's signature of it.
Generate another key pair for a sub sub authority, and sign it with the sub authority.

2.3 User

Create a function that has harcoded the authority's public key, and takes as input a public key and a signature of the authority, and outputs a boolean indicating whether the key is signed by the authority
Create a function that has hardcoded the authority's public key and takes as input a public key signed by the sub auhtority, the sub auhtority public key, the auhtority's signature of the sub auhtority public key, and outputs a boolean indicating whether the key is valid

Create a function that has hardcoded the authority's public key and takes as input a public key signed by the sub sub authority, the necessary public keys and signatures and outputs a boolean indicating whether the key is valid