Blockchains – Feuille de TME #3

4 octobre 2021

Le but de TME est d'implémenter un serveur d'authentification basé sur la vérification de signatures cryptographiques. Ce TME peut être réalisé dans le langage de programmation de votre choix. L'algorithme de signature utilisé sera `EdDSA` [1] avec l'implémentation `Ed25519`. La plupart des langages offre une bibliothèque implémentant cet algorithme.

Exercice 1. À l'aide de la bibliothèque implémentant Ed25519, générez une paire : clé publique × clé privée. Vous vérifierez que les clés publiques et privées font exactement 32 octets.

Exercice 2. À partir d'une donnée arbitraire et en utilisant votre clé privée (sk) précédemment générée, créez une signature. Vous vérifierez que la taille de la signature est de 64 octets. Vérifiez cette signature à l'aide votre clé publique (pk). *i.e.* `verify(pk, data, sign(sk, data)) = true`. Vous testerez également que, pour une mauvaise clé publique, la vérification échoue.

Exercice 3. À partir du jeu de donnée fourni sur la page de l'UE, vérifiez l'ensemble des données et des signatures. Cinq données sont incorrectement signées : vous vous assurerez de trouver le bon résultat.

Les données du fichier sont encodées en hexadécimal, séparées par une ligne blanche, et organisées sous la forme suivante :

```
<clé publique>
<signature>
<donnée>
```

Exercice 4. Définissez un serveur et client TCP (légers) implémentant la spécification suivante :

- Le serveur dispose d'un ensemble d'identités autorisées (sous la forme de clés publiques).
- À chaque nouvelle connexion, le serveur va :
  1. Attendre que le client lui envoie une clé publique ;
  2. Vérifier que la clé publique appartienne aux utilisateurs autorisés ;
  3. Envoyer une donnée arbitraire *aléatoire* de taille fixée au client ;
  4. Attendre une signature du client ;
  5. Vérifiez la signature ;
  6. Envoyer `"ok"` au client si la signature est correcte ou `"ko"` sinon.
- Les comportements inattendus se traduisent par une terminaison de la connexion.

Vous testerez la robustesse de votre implémentation : *e.g.* identifiant incorrect, identifiant correct mais mauvaise signature, etc.

1. `https://en.wikipedia.org/wiki/EdDSA`