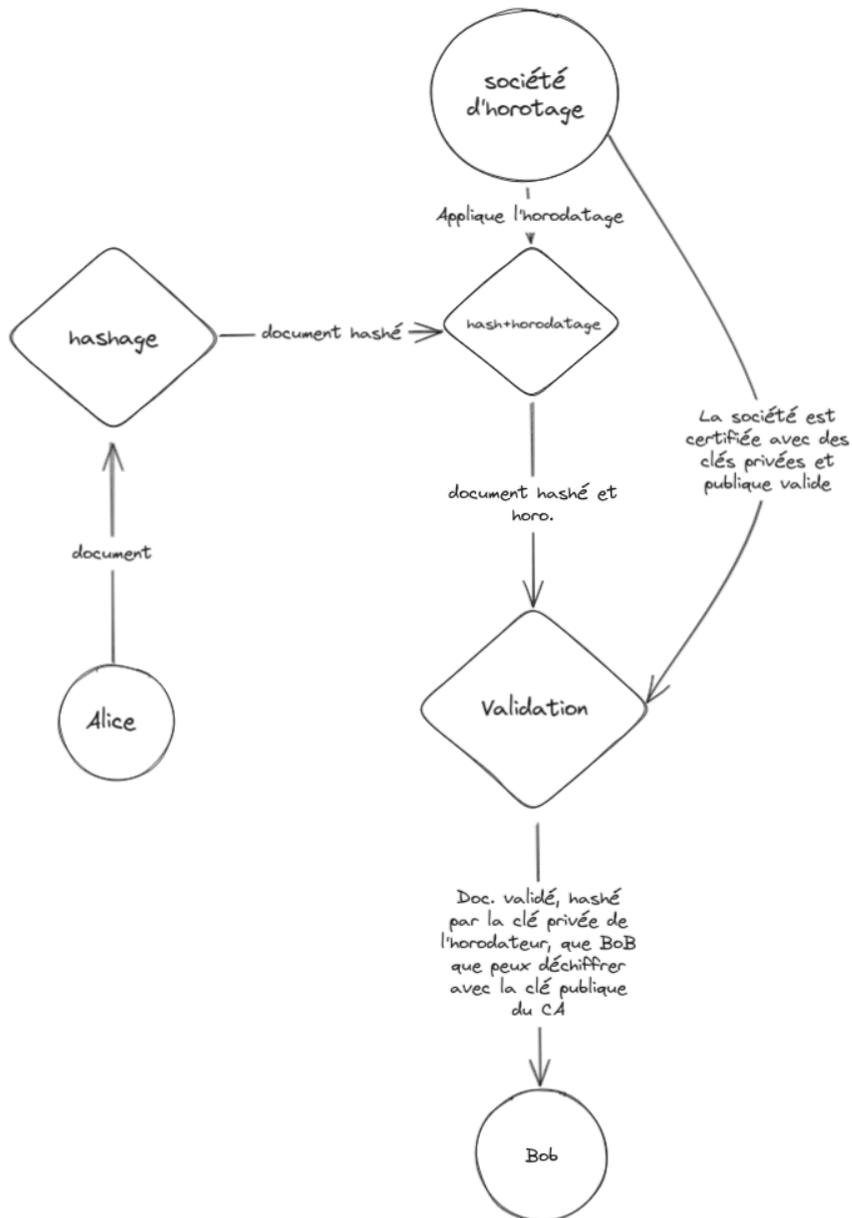


Horodatage

Exercice 1 :

J'ai mis sous forme d'un schéma simple la chaîne de processus pour l'horodatage d'un document que Bob veut envoyer à Alice :



Exercice 2 :

Voir code fournis

Exercice 3 :

On lance simplement notre programme qui va créer les différents documents.

Dans un premier temps Bob créer son document, dont nous pouvons consulter le contenu dans "bob_document.txt".

Puis dans un second temps on encrypt ce document dans "bob_document.txt.enc", nous ne pouvons donc plus accéder à son contenu, il est encrypté avec sa clé privée.

La société d'horodatage va ensuite décrypter le document avec la clé publique de Bob, et ajouter un time stamp, que nous pouvons vérifier dans "bob_document.txt.enc.dec".

La société va ensuite encrypter/signer ce document avec sa clé privé, dans "bob_document.txt.enc.dec.society.enc", on ne peut plus accéder au contenu.

Finalement Alice va pouvoir découvrir le document crypté, en le décryptant avec la clé public de la société, que l'on peut consulter dans "bob_document.txt.enc.dec.verified".

Techniquement nous n'aurions pas besoin de décrypter le document à l'étape où la société reçoit le document, et Alice pourrait simplement utiliser les clés de Bob et de la société pour décrypter, mais j'ai trouvé plus facile de montrer chaque étape comme cela.

Ci-dessous le résultat final :

```
bob_document.txt ×
bob_document.txt
1 This is Bob's document content.

bob_document.txt.enc ×
bob_document.txt.enc
The file is not displayed in the text editor because it is either binary or
uses an unsupported text encoding.
Open Anyway

bob_document.txt.enc.dec ×
bob_document.txt.enc.dec
1 This is Bob's document content.
2 Timestamp: 2023-10-01 12:00:00

bob_document.txt.enc.dec.society.enc ×
bob_document.txt.enc.dec.society.enc
The file is not displayed in the text editor because it is either binary or
uses an unsupported text encoding.
Open Anyway

bob_document.txt.enc.dec.verified ×
bob_document.txt.enc.dec.verified
1 This is Bob's document content.
2 Timestamp: 2023-10-01 12:00:00
```