1

```python
import hashlib

def generate_hash(path):
    hasher = hashlib.sha256()

    with open(path, "rb") as file:
        for block in iter(lambda: file.read(4096), b""):
            hasher.update(block)

    return hasher.hexdigest()

def save_hash(hashValue, outputFile):
    with open(outputFile, "w") as file:
        file.write(hashValue)

if __name__ == "__main__":
    path = "./protoCrypto/tdpastp1/maxime.lefranc"
    hashValue = generate_hash(path)
    print("Hash:", hashValue)
    outputFile = "./protoCrypto/tdpastp1/maxime.hash"
    save_hash(hashValue, outputFile)

    print("saved in ", outputFile)
```

2

j'ai hash mon fichier (maxime.lefranc) avec la fonction sha 256. le fichier n'a pas de sel. en utilisant sha 256, il est possible de verifier si le fichier a ete modifie. dans ce cas la, le resultat est different. j'ai envoye le hash (ef38f2ce4647dc5ffbaeba507b60b62f3f0f6af7b7d551eda4010b9e1b7f6fb8) a Maxime Lefranc.

3

j'ai recu une empreinte de la part de Maxime Lefranc (en sha 256) (ef20902572f40ef42f66691af17f0529d7dbb8e08af877fb859b0c434a56814c) ainsi que son fichier a verifier (fichier.txt)

> fichier.txt

```
salut mon pote
```

apres verification, j'obteins le meme hash.

j'ai modifie le fichier de Maxime pour l'envoyer a une 3e personne

> fichier.txt

```
je collectionne des cannards vivants
```

celui ci a un hash different :
5a78385a629dbc7117e0fb3b3d2a64d62a3e9dcb0af6715347097f2861070947

4

Une collision est le terme employe pour decrire deux fichiers ayant la meme valeur de hash, pour la meme fonction de hashage.

lien vers les 2 fichiers ayant le meme hash : https://shattered.it/

En 2017, deux chercheurs ont reussi a provoquer une collision entre deux PDF avec SHA1.
L'attaque utilisee est une attaque par chemin choisi.

la premiere etape consistait a generer des PDF distincts mais aux hash similaires.
en ajoutant puis manipulant des blocs de donnees a la fin des fichiers, ils ont pu atteindre la colision

5

la signature permet de verifier l'authenticite du message, mais elle ne resoudra pas le probleme du hash, la cle privee ne signant que le hash.