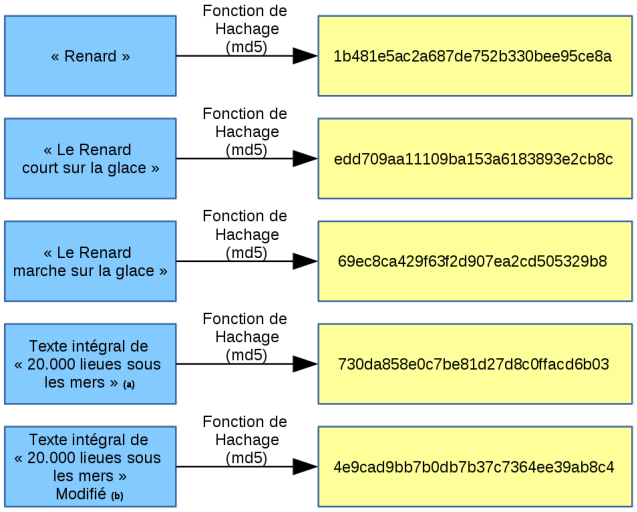
Python : crack mot de passe (mini projet):

Fonction de hachage:

On nomme fonction de hachage, de l'anglais hash function (hash: pagaille, désordre, recouper et mélanger) par analogie avec la cuisine, une fonction particulière qui, à partir d'une donnée fournie en entrée, calcule une empreinte numérique servant à identifier rapidement la donnée initiale, au même titre qu'une signature pour identifier une personne. Les fonctions de hachage sont utilisées en informatique et en cryptographie notamment pour reconnaître rapidement des fichiers ou des mots de passe.



En python, la bibliothèque hashlib permet d'utiliser différentes fonctions de hachage. Tester le code suivant et donner le résultat de la fonction de hachage (md5) pour les mots "hello", "Hello", "salut" et "slatu".

```python
import hashlib

"""
Test de hash:
"""
mystring = "ttkd1fe"
# Assumes the default UTF-8
hash_object = hashlib.md5(mystring.encode())
print(hash_object.hexdigest())
```

hash.py

Hachage d'un mot de passe:

Le hachage de mot de passe est l'une des pratiques de sécurité les plus basiques qui doit être effectuée. Sans cela, chaque mot de passe stocké peut être volé si le support de stockage (typiquement une base de données) est compromis. Ce mot de passe peut alors être immédiatement utilisé pour accèder frauduleusement non seulement à votre application mais aussi sur d'autres applications si l'utilisateur utilise le même mot de passe ailleurs.

Sur une base de donnée, nous avons récupéré les hashs de trois personnes:

1. Chloé: 89d5083995286b663d66f3e563b44267
2. Stéphane: 4d34712de64dd235040d3dc9af937aac
3. Léa: 873a3eea54db92ef25232f9737905604

Nous avons deplus les informations suivantes:

- le mot de passe de Chloé provient d'un dictionnaire en français,
- le mot de passe de Stéphane est composé uniquement de 5 lettres minuscules,
- le mot de passe de Léa est composé 6 lettres minuscules et d'un chiffre.
- l'algorithme de hachage utilisé pour ces mots de passe est MD5.

Trouver les différents mots de passe. Que dire du mot de passe de Léa? Quels conseils donner à un utilisateur pour choisir un mot de passe fort?

NB: Les algorithmes de hashage comme MD5, SHA1 et SHA256 sont destinés à être rapides et efficaces. Avec les équipements informatiques modernes, il est devenu facile d'attaquer par force brute la sortie de ces algorithmes pour retrouver la chaîne originale.

C'est la raison pour laquelle de nombreux experts en sécurité considèrent ces algorithmes comme faibles et les déconseillent fortement pour hasher un mot de passe utilisateur.