Contexte
La CNIL précise que : Le mot de passe ne doit jamais être stocké en clair. Lorsque l'authentification a lieu sur un serveur distant, et dans les autres cas si cela est techniquement faisable, le mot de passe doit être transformé au moyen d'une fonction cryptographique non réversible et sûre, intégrant l'utilisation d'un sel ou d'une clé. (https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires)
Afin de répondre à cette exigence, une technique assez populaire est d'utilisation de hachage : Pour les applications, avant de stocker un mot de passe (sur un serveur base de données par exemple), on peut le « hacher »

Application
Version1 : Développer une application qui saisit un mot de passe et qui affiche son hachage md5.
Version 2 : Développer une application qui saisit un mot de passe et qui affiche son hachage md5 en faisant un « salage ».
Version 3 : Développer une application qui choisit une fonction de hachage et un mot de passe. L'application affiche le mot de passe haché avec le salage.

Annexe

- **Fonction de hachage**

Définition
La fonction de hachage convertit des séquences de caractères de différentes longueurs en séquences de même longueur. Dans le cadre de ce processus, les données sont donc « **hachées** » par la fonction de hachage avant d'être ramenées à une **longueur uniforme**, quelle que soit la taille de la valeur initiale.

Propriétés
Le même message donne toujours la même valeur de hachage (c'est-à-dire que la fonction est *déterministe*).
La valeur de hachage est calculée rapidement.
Il est impossible d'avoir deux messages avec la même valeur de hachage (appelée «collision»).
Il est impossible de créer intentionnellement un message qui produit une valeur de hachage donnée.
De légères modifications apportées au message doivent modifier considérablement la valeur de hachage résultante, afin qu'elle apparaisse non corrélée avec le hachage d'origine.

- **« Sel »**

Pour remédier aux principaux problèmes des fonctions de hachage dites "simple" (MD5, SHA1, SHA256, SHA512), des techniques ont été inventées. Parmi lequelles, on a la notion de "sel" (salt) qui se veut être une chaîne générée aléatoirement et concaténée au mot de passe (en préfix, en suffixe, ou les deux, etc.).