# PROJET AGORA

## Mise en place d'un mécanisme d'authentification

## Mission 2

## Authentification

Dans le contexte Agora l'identité numérique est stockée dans la base de données. Un formulaire d'authentification permet aux utilisateurs de saisir leurs données d'identification pour accéder à l'application.

Dans cette mission, nous transmettons le hash ou empreinte du mot de passe, en utilisant l'algorithme de hachage SHA512 qui produit un hash de 512 bits soit 128 caractères hexadécimaux. Ce n'est donc pas le mot de passe en clair qui transitera via le réseau mais son empreinte numérique.

### Méthodes de sécurisation des mots de passe :

- Fonction de hachage (SHA256, SHA512, bcrypt, …)

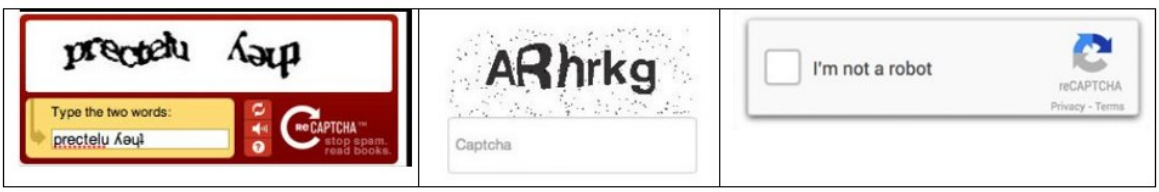
Une fonction de hachage convertit un texte en une suite de caractères assez courte nommé l'empreinte (hash) (ou condensé, haché, message digest).
Il est impossible de déchiffrer l'empreinte pour revenir au texte d'origine

- Technique du (grain de) sel

Il s'agit de compliquer le piratage en concaténant des caractères supplémentaires (le grain de sel, de préférence une longue chaine de caractères) au mot de passe à hacher.
Le grain de sel peut lui-même être haché, aléatoire, regénéré …
Dans le cadre d'une authentification, il est recommandé d'utiliser un grain de sel propre à chaque utilisateur et stocké dans la base de données.
Tests de grain de sel en PHP : http://info.crypto.free.fr/graindesel.php

- Captcha

Le captcha est un système couramment utilisé sur les sites Web pour vérifier qu'un humain est bien ce qu'il prétend être, et non une machine. Il peut ainsi arrêter les attaques par force brute en cours.



## *Principales étapes de la mise en œuvre de l'authentification*

- Création d'un utilisateur avec des droits restreints sur la base
- Adaptation de la base de données
- Développement du modèle (MVC)
- Développement de la vue : le formulaire d'authentification
- Hachez le mot de passe
- Développement du contrôleur
- Transmission de données via les sessions
- Adaptation du contrôleur principal : index.php
- Création du contrôleur secondaire : c_connexion.php
- Adaptation des vues v_header et v_accueil
- Déconnexion
- Test

### *Formulaire d'authentification créé*