(Trace écrite)

THÈME : MODÉLISATION ET LA SIMULATION DES OBJETS ET SYSTÈMES TECHNIQUES	
Connaissance : MSOST.1.5.1 Outils de description d'un fonctionnement, d'une structure et d'un comportement.	*Compétence :* Décrire, en utilisant les outils et langages de descriptions adaptés, le fonctionnement, la structure et le comportement des objets.

Problématique :
- Comment transmettre de l'information sur les réseaux en toute sécurité ?

Hypothèse :
En utilisant un code secret, en cachant les informations, ...

Expérimentation :
- Exercices d'application sur le hachage et de chiffrage.
- Entraînement sur les concours al-Kindi.

Synthèse :

C'est quoi le hachage ?

Le hachage est une technique mathématique utilisée en informatique qui permet de stocker *"l'empreinte d'une information"*. Il n'est pas possible de retrouver l'information qu'à partir de son empreinte car le hachage ne fonctionne que dans un sens. Cependant certaines fonctions de hachage peuvent devenir obsolètes face aux nouvelles puissances de calcul des nouveaux processeurs…
Le hachage ne doit pas être confondu avec le cryptage (ou codage) de l'information.
Cette technique permet de vérifier la validité d'une information (Ex:Mot de passe, code secret, …)

Il existe plusieurs méthodes connues : MD5, SHA-1, SHA-256/ SHA-512.

C'est quoi le cryptage ?

Le cryptage est une technique mathématique utilisée en informatique qui permet de transmettre une information en toute confidentialité. Son utilisation est très ancienne car elle apporte un intérêt stratégique militaire. Même si son utilisation est désormais intensive sur le web, cette technique est classée dans de nombreux pays, dans la catégorie juridique des armes !

Un système de chiffrement est dit :

- chiffrement symétrique quand il utilise la même clé pour chiffrer et déchiffrer.
- chiffrement asymétrique quand il utilise des clés différentes : une paire composée d'une clé publique, servant au chiffrement, et d'une clé privée, servant à déchiffrer.

Quelques méthodes de chiffrement connues : Code de César, Code de Vigenère, Code Morse.

Le code César, une des premières formes de substitution

Le code César doit son nom a Jules César qui l'utilisa abondamment dans ses correspondances

C'est un principe de substitution mono-alphabétique. L'idée est de décaler les lettres de l'alphabet d'une valeur clé.
César utilisait régulièrement le chiffre 3 transformant les **a** en **d**... et les **z** en **c**.

Les substitutions alphabétiques sont à l'origine de très nombreuses méthodes de chiffrement. Ce type de code est particulièrement faible car le chiffrement n'affecte pas les fréquences de d'apparition des lettres dans un texte.
Al Kindi mettra en évidence cette faiblesse par une méthode d'analyse des fréquences dès le IX^{ème} siècle.