Première année

Cours 5: La fonction de hachage

ASCII

1er encodage historique – > **ASCII** (American Standard Code for Information Interchange): **norme américaine**, standardisée en **1963**. (*Son but est d'organiser l'univers informatique à l'échelle nationale*)

A l'époque les caractères considérés comme essentiels à une communication – > **127 caractères**

- les **10 chiffres**
- les **26 lettres minuscules ET majuscules**
- **32 symboles** (@,<,>,espace,etc...)
- **33 symboles de mise en page** (passage à la ligne, saut de page, etc...)

On code donc sur 1 octet (8 bits), **le premier étant toujours 0** et sert au contrôle de parité (pour éviter les erreurs).

128	64	32	16	8	4	2	1

- Les caractères de **numéro 0 à 31** correspondent à des **commandes de contrôle de terminal informatique**.
- Le caractère **numéro 127 est la commande pour effacer**.
- Les **chiffres sont codés par les nombres de 48 à 57**.
- Les **lettres majuscules et les nombres de 65 à 90**.
- Les **minuscules par les nombres de 97 à 122**.

/!\ ce code a rapidement montré ses limites – > pas d'accent, pas de caractère spécial pour les langues latines

ISO 10646 / UNICODE

1990: création de la solution ultime **ISO 10646** – > **Jeu Universel de Caractères** (Universal Character Set) **Crée pour pouvoir accueillir n'importe quel caractère existant de n'importe quelle langue du monde**.

1991: surcouche **Unicode** – > **Gère les différents sens de lecture**

UTF-8

Il est **codé entièrement en ASCII** et dès qu'on a besoin d'un caractère appartenant à l'Unicode,

on **utilise un caractère spécial indiquant qu'il est en Unicode**.

Il est un des **formats de codage les plus courants** – > la **plupart des navigateurs supportent l'UTF-8** et le détectent automatiquement

Qu'est ce que l'encodage ?

– > **Action de transcrire des données vers un format ou un protocole donné.**

Hachage

– > **Algorithme permettant de modifier un texte (appelé message) en valeur de longueur fixe (appelé hash)**.

Exemples:

- **1991**: **md5** est une fonction de hachage qui retourne toujours 32 caractères
- **1995**: **sha1** est une fonction de hachage qui retourne toujours 40 caractères

Pour contrer l'évolution des logiciels malveillants **les algorithmes de hachage évoluent** aussi

– > 2008: MD5 – > MD6

– > 2015: SHA-1 devient SHA-2 puis SHA-2

On peut **utiliser une fonction de hachage lorsque l'on souhaite comparer une valeur sans pouvoir stocker sa représentation simple** (ex: stocker des mots de passe dans une base de données – > Il est interdit de stocker un MDP sous sa forme brut.)

Différence entre chiffrement et hachage – > **le chiffrement** est par principe **une fonction réversible** alors que le **hachage** n'est par principe **pas réversible**.