FORMATIO | RESSOURCE INFORMATIQUE BUREAUTIQUE

CHIFFREMENT DES DONNÉES

1. CHIFFREMENT VS HACHAGE (HASH)
2. DIFFÉRENT TYPE DE HACHAGE
3. EXEMPLE DE HACHAGE (LOGICIEL)
4. EXEMPLE DE CHIFFREMENT (LOGICIEL)

Chiffrement vs Hachage (hash)

Le Chiffrement : Le Coffre-Fort (Réversible)

Le but du chiffrement est de cacher un message pour que seule une personne possédant la clé puisse le lire. C'est un processus bidirectionnel.

- ✓Processus : Texte clair + Clé = Texte chiffré.
- ✓Action inverse : Texte chiffré + Clé = Texte clair.
- ✓Usage : Envoyer un courriel confidentiel, protéger tes fichiers sur ton disque dur, ou sécuriser une transaction bancaire.

Le Hachage : L'Empreinte Digitale (Irréversible)

Le but du hachage n'est pas de cacher la donnée, mais de créer un identifiant unique pour vérifier que la donnée n'a pas été modifiée. C'est un processus unidirectionnel. Pour l'intégrité et l'authenticité

- ✓Processus : Donnée → Fonction de hachage → Hash.
- ✓Action inverse : Impossible. Tu ne peux pas retrouver le texte original à partir du hash, peu importe la puissance de ton ordinateur.
- ✓Usage : Vérifier l'intégrité d'un logiciel téléchargé ou stocker des mots de passe en sécurité.

Chiffrement vs Hachage (hash) - suite

Comparaison directe

Caractéristique	Chiffrement (Encryption)	Hachage (Hashing)
Objectif	Confidentialité (Cacher l'info)	Intégrité (Vérifier l'info)
Réversibilité	Oui (avec une clé)	Non (jamais)
Entrée / Sortie	La sortie change de taille selon l'entrée	La sortie a toujours la même taille fixe
Clé	Nécessite une clé (symétrique ou non)	Ne nécessite pas de clé

Différent type de hachage

Nom	Taille du résultat	Statut de sécurité
MD5	128 bits	**Obsolète / Dangereux**
SHA-1	160 bits	**Obsolète / Non sécuritaire**
SHA-256	256 bits	**Standard actuel sécurisé**

Il y a en d'autre (SHA-512, SHA3, Keccak etc.), voir diapo sources (Online Tools pour les autres)

Sources

- File Hash Online Calculator
  https://md5file.com/calculator
- Online Tools
https://emn178.github.io/online-tools/
- Compare Hash Tool
  https://onlinehashtool.com/compare-hash/
- Swisstransfert
  https://www.swisstransfer.com/fr
- Privote
  https://privnote.com/
- KPASTE
  https://kpaste.infomaniak.com/new
- FlowCrypt
  https://flowcrypt.com/