# Template LRE - EPITA

## Un exemple avec un fichier de style séparé




**Loïc Rouquette**
**EPITA - Laboratoire de Recherche de l'EPITA (LRE)**
**28 octobre 2026**

Template LRE - EPITA © 2026 Loïc Rouquette is licensed under CC BY 4.0.
To view a copy of this license, visit https ://creativecommons.org/licenses/by/4.0/.

# Qu'est-ce que c'est ?

Une fonction de condensation (ou fonction de hachage) est une fonction :

$$H : \{0,1\}^* \rightarrow \{0,1\}^n$$

qui, à partir d'une chaîne de bits quelconque $m$, produit un haché (condensat ou empreinte) $h = H(m)$ de taille fixe ($n$ bits).


licensed under CC BY 4.0

# À quoi ça sert ? — Table de hachage

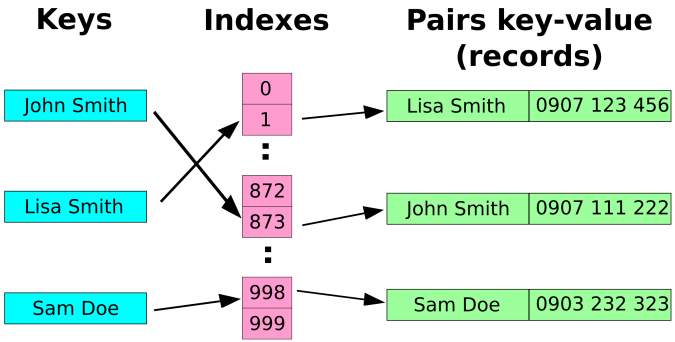



**Figure 1 :** Un annuaire représenté comme une table de hachage. La fonction de hachage transforme les clés (en bleu) en valeurs de hachage (en rouge) indexant les éléments de la table (alvéoles) composés de paires clé–valeur (en vert). (source : Wikipédia)

# À quoi ça sert ? — Intégrité des fichiers

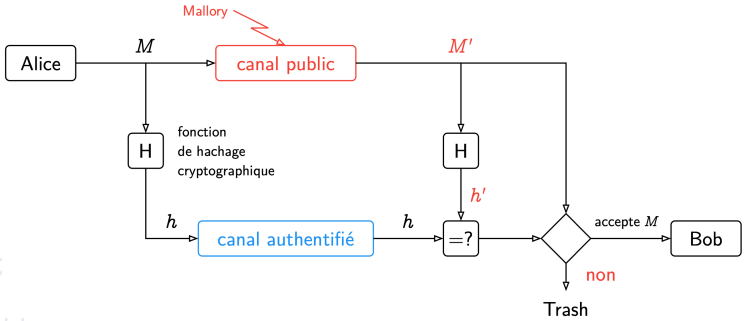



**Figure 2 :** Vérification de l'intégrité d'un fichier. L'empreinte du fichier téléchargé est calculée puis comparée avec l'empreinte officielle.

# À quoi ça sert ? — Mots de passe

Enregistrement des mots de passe !


licensed under CC BY 4.0

# Condensats cryptographiques

Une fonction de condensation est dite cryptographique lorsqu'elle vérifie un certain nombre de propriétés :

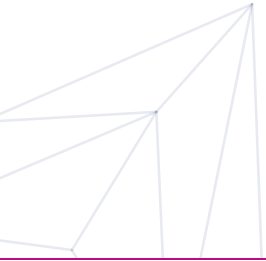



licensed under CC BY 4.0

# Condensats cryptographiques

Une fonction de condensation est dite cryptographique lorsqu'elle vérifie un certain nombre de propriétés :

- **Résistance à la préimage :** pour toute valeur de hachage $h$, il est difficile de trouver un message $m$ tel que $H(m) = h$.




licensed under CC BY 4.0

# Condensats cryptographiques

Une fonction de condensation est dite cryptographique lorsqu'elle vérifie un certain nombre de propriétés :

- **Résistance à la préimage :** pour toute valeur de hachage $h$, il est difficile de trouver un message $m$ tel que $H(m) = h$.
- **Résistance à la seconde préimage :** pour une valeur $m_1$ donnée, il est difficile de trouver un message $m_2$ tel que $H(m_1) = H(m_2)$.


licensed under CC BY 4.0

# Condensats cryptographiques

Une fonction de condensation est dite cryptographique lorsqu'elle vérifie un certain nombre de propriétés :

- **Résistance à la préimage :** pour toute valeur de hachage $h$, il est difficile de trouver un message $m$ tel que $H(m) = h$.
- **Résistance à la seconde préimage :** pour une valeur $m_1$ donnée, il est difficile de trouver un message $m_2$ tel que $H(m_1) = H(m_2)$.
- **Résistance aux collisions :** il est difficile de trouver deux messages différents $m_1$ et $m_2$ tels que $H(m_1) = H(m_2)$. Une telle paire est appelée une collision de hachage cryptographique.


licensed under CC BY 4.0

# À vous !

