

# Authentication de messages

## Fonction de hachage cryptographique

- On dit que  $h : \mathbb{B}^* \rightarrow \mathbb{B}^k$  est une **fonction de hachage cryptographique** si il est
  - Facile de calculer  $h(x)$  étant donné  $x \in \mathbb{B}^*$

# Authentication de messages

## Fonction de hachage cryptographique

- On dit que  $h : \mathbb{B}^* \rightarrow \mathbb{B}^k$  est une **fonction de hachage cryptographique** si il est
  - Facile de calculer  $h(x)$  étant donné  $x \in \mathbb{B}^*$
  - Difficile de calculer  $x$  étant donné  $h(x) \in \mathbb{B}^k$