# Authentification de messages

## Détection d'erreur de transmission

- On peut utiliser une fonction de hachage cryptographique $h$ pour faire la détection d'erreur
- On envoie un message $m$ ainsi qu'une empreinte $h(m)$

$$m || h(m)$$

# Authentification de messages

## Détection d'erreur de transmission

- On peut utiliser une fonction de hachage cryptographique $h$ pour faire la détection d'erreur
- On envoie un message $m$ ainsi qu'une empreinte $h(m)$

$$m||h(m)$$

- Si la communication fait défaut et que le message reçu est $m' \neq m$

$$m'||h(m)$$