

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 $h(m)$

$$m \parallel h(m)$$

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

$$m' \parallel h(m)$$

- Le récepteur calcule $h(m') \neq h(m)$ et constate qu'il y a eu erreur

Authentification de messages

Prouver son identité et l'intégrité du message

- La méthode présentée (envoyer $m \parallel h(m)$) n'est pas authentifiante