

Authentification 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 $h(x) \in \mathbb{B}^k$
 - Difficile de trouver différents $x_0, x_1 \in \mathbb{B}^*$ tels que $h(x_0) = h(x_1)$
 - Exemple (plus considéré sûr):

`md5("hello world") = 2aae6c35c94fcfb415dbe95f408b9ce91ee846ed`

Authentification de messages

Détection d'erreur de transmission

- On peut utiliser une fonction de hachage cryptographique h pour faire la détection d'erreur