

Authentication de messages

Détection d'erreur de transmission

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

Authentication 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 $h(m)$

$$m \parallel h(m)$$