Authentification de messages

Prouver son identité et l'intégrité du message

- La méthode présentée (envoyer $m||h(m)$) n'est pas authentifiante
  - N'importe qui peut calculer $h(m)$ et se faire passer pour l'envoyeur

Authentification de messages

Prouver son identité et l'intégrité du message

- La méthode présentée (envoyer $m \,||\, h(m)$) n'est pas authentifiante
  - N'importe qui peut calculer $h(m)$ et se faire passer pour l'envoyeur
  - Un attaquant peut remplacer le message par m' et l'empreinte par $h(m')$ sans être détecté