

# Authentification de messages

Prouver son identité et l'intégrité du message

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

# Authentification de messages

Prouver son identité et l'intégrité du message

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