

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
 - Un attaquant peut remplacer le message par m' et l'empreinte par $h(m')$ sans être détecté
- Une manière de résoudre ce problème est d'échanger au préalable un secret s
 - Puis de l'ajouter à l'empreinte comme par exemple $m \parallel h(m) \parallel s$

