Signature cryptographique

Arthur Garnier

Utiliser la crypto asymétrique pour signer des choses.

Problème : Signer un document de sorte que tout le monde puisse vérifier que **vous** l'avez signé. C'est une défense contre Man in the middle.

RSA =

- Publique : N, e
- Privée = p, q, d
- Chiffrer = $s = m^e \ mod \ N$
- Déchiffrer = $s^d = m \ mod \ N$
- Signer = $H(m)^d \ mod \ N$ (vous êtes le seul à pouvoir signer)
- Vérifier la signature = $s^e \ mod \ N$ (tout le monde peut vérifier)

$H(m)$ car : C'est plus petit donc c'est plus rapide et ça protège mieux

- Envoyer un message à Bob = Chiffrer avec **sa** clé publique
- Hacher
- Signer le hash avec **ma** clé privée