Établissement de clé

Attaque de l'homme du milieu

g: générateur fixé d'un groupe cyclique

$s_1 = C^a = g^{ac}$ $\quad$ $s_1 = A^c = g^{ac}$ $\quad$ $s_2 = C^b = g^{bc}$

$Enc_{s_1}(m)$ $\quad$ $s_2 = B^c = g^{bc}$ $\quad$ $Enc_{s_2}(m)$

(c, C): clé de session de l'attaquant

(a, A): clé de session du client

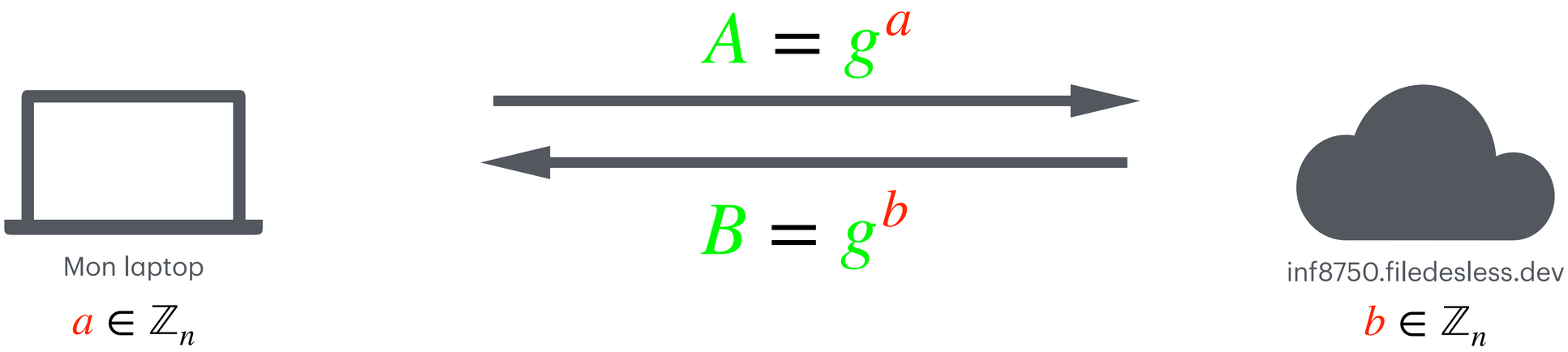
(b, B): clé de session du serveur

s_1, s_2: clés de session partagée

Établissement de clé

Certification des clés éphémères

g: générateur fixé d'un groupe cyclique



- On voudrait signer B avec une clé privée (RSA ou DSA) du serveur
- Problème: comment transmettre la clé publique correspondante au client?
- Solution: Introduction d'une tierce personne de confiance