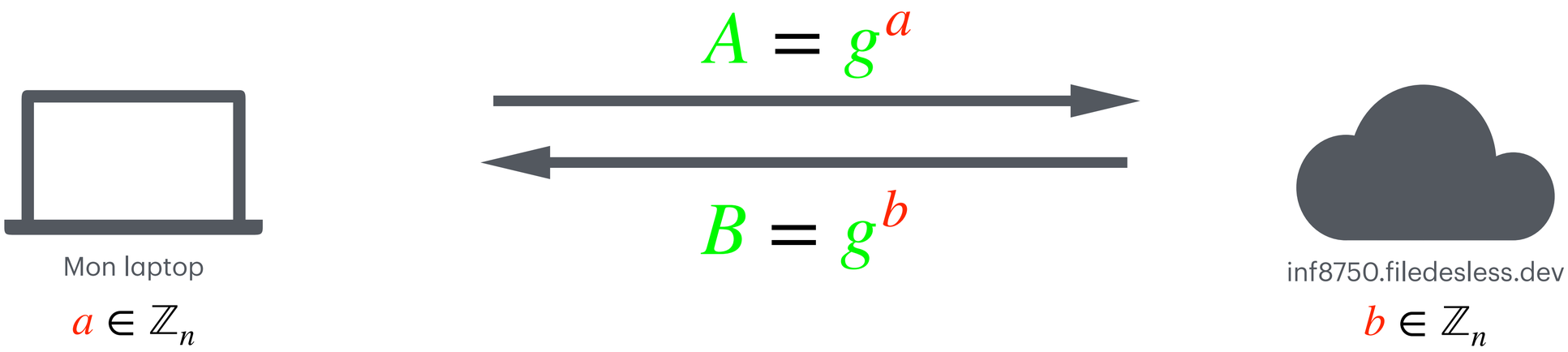
Établissement de clé

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

Établissement de clé

Shoutout to: https://letsencrypt.org/

Certification signée par une autorité de confiance

- L'appareil du client vient pré-installé avec un "magasin de confiance" (trust store) contenant:
  - Nom de l'autorité de confiance
  - Clé publique de l'autorité de confiance
- Le serveur possède un certificat préalablement signé par l'autorité de confiance contenant:
  - Nom du serveur
  - Nom de l'autorité de confiance
  - Clé publique du serveur