Établissement de clé classique

Exemple: Finite Field Diffie-Hellman

- On prend le groupe multiplicatif de $\mathbb{F}_p$ pour $p = 23$ avec comme générateur $g = 5$
- Alice choisi l'entier secret $a = 4$ et envoie à Bob $A = g^a \mod p = 5^4 \mod 23 = 4$
- Bob choisi l'entier secret $b = 3$ et envoie à Alice $B = g^b \mod p = 5^3 \mod 23 = 10$
- Alice calcule le secret partagé $s = B^a \mod p = 10^4 \mod 23 = 18$
- Bob calcule le secret partagé $s = A^b \mod p = 4^3 \mod 23 = 18$

Établissement de clé classique

État des lieux

- TLS 1.3 publié en 2018 (RFC 8446)
  - Utilisé par les navigateurs et serveurs web partout dans le monde
- L’une des premières étapes du protocole est un établissement de clé
- Les seules méthodes autorisées sont celles basées sur RSA ou DH