Établissement de clé classique

Diffie-Hellman

- Soit un groupe cyclique de générateur g et d'ordre n
- Alice et Bob choisissent respectivement $a, b \in \mathbb{Z}_n$ aléatoirement en secret
- Ils calculent et échangent publiquement les éléments de groupe $A = g^a$ et $B = g^b$
- Ils peuvent chacun calculer le secret partagé $A^b = g^{ab} = B^a$

Exponentiation rapide vs logarithme discret présumé lent

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 $s = A^b \mod p = 4^3 \mod 23 = 18$