Échange de clé Diffie-Hellman

Protocole

- Soit $\mathbb{G} = \langle g \rangle$ un groupe cyclique fini d'ordre q
- Alice et Bob:
  - Choisissent un nombre secret chaque $a, b \in \mathbb{Z}_q$
  - Calculent respectivement $A = g^a$ et $B = g^b$
  - Échangent A et B
  - Calculent le secret partagé $k = A^b = B^a = g^{ab}$

Échange de clé Diffie-Hellman

Sécurité

- La sécurité du système repose sur la difficulté présumée du problème CDH
  - C’est-à-dire calculer g^{ab} étant donné g^a et g^b
- Une manière de faire est de calculer le logarithme discret
  - Permet de retrouver a et b, et donc calculer g^{ab}
  - On pense que c’est la meilleure manière
- Considéré comme difficile pour certains groupes