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

Informatique quantique

Algorithme de Shor

- Solution efficace au logarithme discret et à la factorisation entière
- Les schémas présentés ne sont plus sûrs face à un ordinateur quantique
- Il faut de nouveaux schémas, basés sur d’autres problèmes