# Établissement de clé classique

## Via un chiffre à clé publique (exemple: RSA)

- Alice dispose d'une paire de clé privée/publique
- Alice envoie sa clé publique à Bob
- Bob chiffre une chaine aléatoire avec la clé publique d'Alice et lui envoie
- Alice déchiffre la chaine aléatoire, leur secret partagé

# 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