Établissement de clé classique

Solutions

- Schéma d'échange de clé basé sur le logarithme discret [DH76]
  - Diffie-Hellman key exchange
- Chiffre basé sur le problème de factorisation [RSA78]
  - RSA cryptosystem

! Basé sur la difficulté de calcul de certains problèmes (incertain même en classique)

! Algorithme efficace quantique pour résoudre DLOG et RSA [S94]

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