Établissement de clé classique

Motivation

- Confidentialité parfaite si on résout l'établissement de clé (One Time Pad) [S49]
- XOR un message avec une clé aussi longue, à usage unique

Aucune hypothèse calculatoire nécéssaire

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]