Établissement de clé

Définition du problème

- Demande à Alice et Bob d'établir une clé secrète partagée via un canal publique
  - Sans échange / connaissance préalables
  - Sans qu'Eve (qui espionne) ne puisse découvrir le secret
- Applications
  - Chiffrement à clé privée
  - Codes d'authentification de message

Établissement de clé classique

RSA et DH