Établissement de clé classique

RSA et DH

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