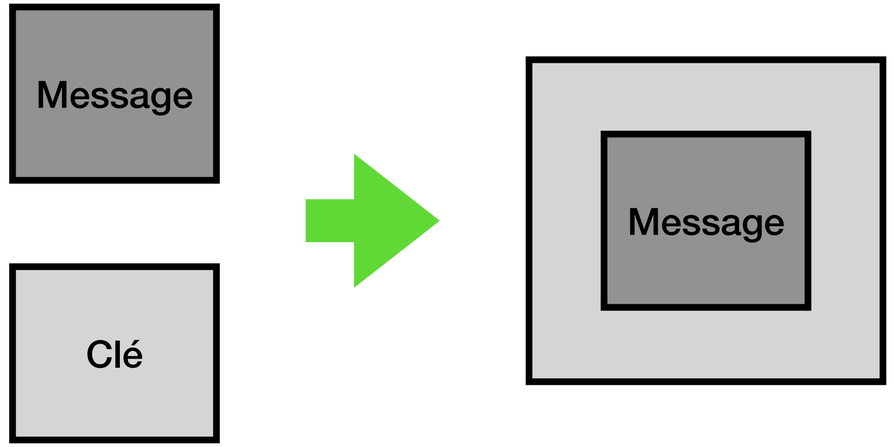
Bootstrapping - Opérations requises

Chiffrement aveugle

- Étant donné:
  - Le chiffré $[m]$ d'un message m
  - Le chiffré $[k]$ d'une clé k
- On peut calculer le chiffré du chiffré $[[m]]$
  - Avec un bruit faible



Bootstrapping - Opérations requises

Déchiffrement aveugle

- Étant donné:
  - Un message doublement chiffré $[[m]]$
  - Le chiffré $[k]$ d'une clé k
- On peut retrouver le chiffré $[m]$
  - Avec un bruit encore faible