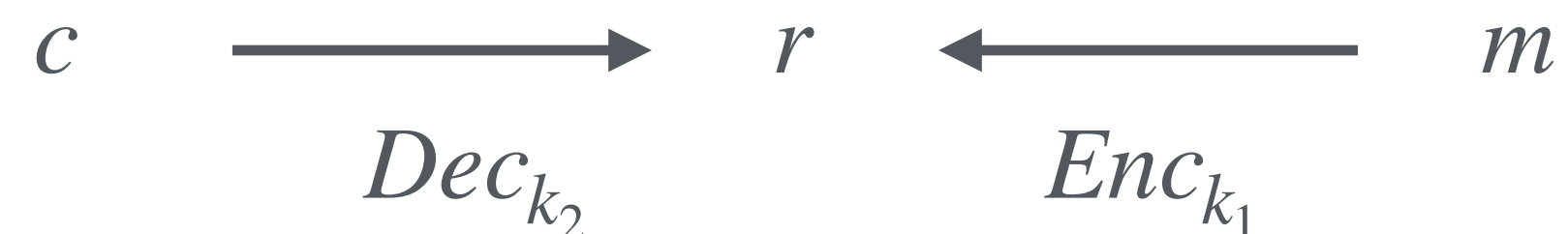


# Rencontre par le milieu

## Attaque “Meet in the Middle”

- Pour chaque  $k_2$  on calcule  $r \leftarrow Dec_{k_2}(c)$  ( $2^{56}$  étapes)
  - On ajoute  $r \mapsto k_2$  dans une table de hachage  $H[r] \leftarrow k_2$
- Pour chaque  $k_1$  on calcule  $r \leftarrow Enc_{k_1}(m)$  ( $2^{56}$  étapes)
  - On retourne la paire  $(k_1, k_2)$  quand on trouve  $k_2 \leftarrow H[r]$
- Total:  $2^{56}$  étapes de calcul



Authentication de messages