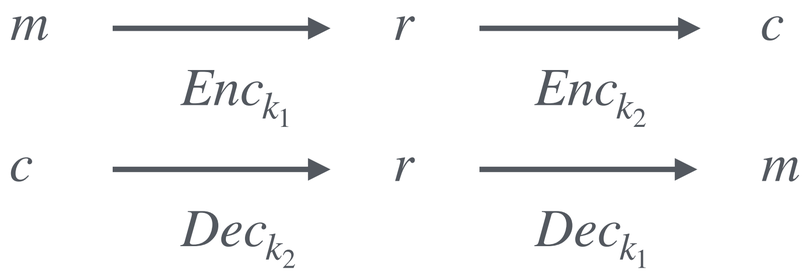
Rencontre par le milieu

Mise en situation

- On a (m, c) tels que $c = Enc_{k_2}(Enc_{k_1}(m))$ pour Enc une fonction de chiffrement 56 bits
- On veut retrouver k_1 et k_2 de manière (beaucoup) plus efficace que par fouille exhaustive
- On note r le résultat de chiffrement intermédiaire



Rencontre par le milieu

Attaque par fouille exhaustive

- Pour chaque k_2 on calcule $r \leftarrow Dec_{k_2}(c)$ (2^{56} étapes)
  - Pour chaque (r, k_1) on calcule $m' \leftarrow Dec_{k_1}(r)$ (2^{56} étapes)
    - On retourne la paire (k_1, k_2) quand on trouve $m' = m$
- Total: $2^{56} \times 2^{56} = 2^{112}$ étapes de calcul

$$c \xrightarrow[Dec_{k_2}]{} r \xrightarrow[Dec_{k_1}]{} m$$