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

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

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