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

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