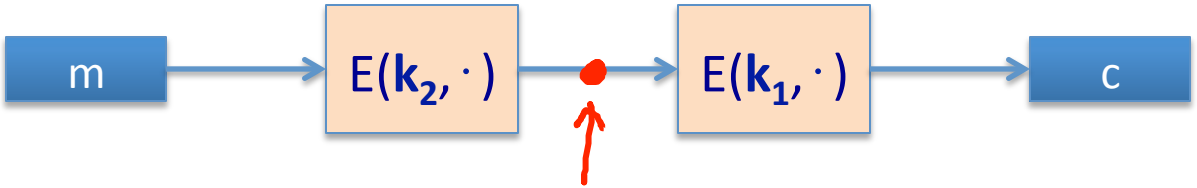
Meet in the middle attack



$k^0 = 00\ldots00$	$E(k^0, M)$
$k^1 = 00\ldots01$	$E(k^1, M)$
$k^2 = 00\ldots10$	$E(k^2, M)$
⋮	⋮
$k^N = 11\ldots11$	$E(k^N, M)$

Attack: $M = (m_1,\ldots, m_{10})$, $C = (c_1,\ldots,c_{10})$

- step 1: build table.
- Step 2: for all $k \in \{0,1\}^{56}$ do:

  test if $D(k, C)$ is in 2nd column.

if so then $E(k^i,M) = D(k,C) \Rightarrow (k^i,k) = (k_2,k_1)$