Meet-in-the-middle Attack against Double DES
Double DES

\[ m \rightarrow \text{DES} \rightarrow \text{DES} \rightarrow C \]
Given plaintext-ciphertext pairs

\((m_1, c_1)\)

\((m_2, c_2)\)

\(\vdots\)

\((m_n, c_n)\),

find \(K_1\) and \(K_2\).
Naive algo:

try all possible \((k_1, k_2)\) and check if \(E_{k_2} E_{k_1}(m_i) = c_i\) \(\forall i = 1, n\)

Time complexity \(O(2^{1/2})\)
However, the meet-in-the-middle algorithm takes:

- **Time:** $2 \times O(2^{56})$
- **Space:** $O(2^{64})$
4 steps: Given \((m_1, c_1)\),

1. create \(2^{64}\) cells with addresses from \(0^{64}\) to \(1^{64}\).

2. calculate \(E_{k_i}(m_1)\)'s with all possible \(2^{66}\) \(k_i\)'s and save \(k_i\) in the cell of address \(E_{k_i}(m_1)\).
e.g., \[ k_1 = 0^{56} \left( \begin{array}{l} \overbrace{0 \cdots 0}^{56 \text{ bits}} \end{array} \right) \]

\[ E_{0^{56}}(m_1) = (01)^{32} \left( \begin{array}{l} \overbrace{0101 \cdots 01}^{64 \text{ bits}} \end{array} \right) \]

\[ \Rightarrow \] cell 0 \cdots 0

\begin{array}{l}
\text{cell} 0 \cdots 01 \\
\vdots \\
\text{cell} 0101 \cdots 01 \\
\vdots \\
\text{cell} \cdots 1
\end{array}
3. Calculate $E^{-1}_{k_2}(c_{c_1})$ with all possible $2^{56}$ $k_2$'s and check if there is some $k_1$ in the cell of address $E^{-1}_{k_2}(c_{c_1})$. If so, $(k_1, k_2)$ may be the true keys of the double DES. See 4 for the further check.
4. Use this $(k_1, k_2)$ to test the rest $(m_i, c_i)$ to see if $E_{k_1}(m_i) = E_{k_2}^{-1}(c_i)$.
   
   a. If yes, we got it.
   
   b. If some $i$ with $E_{k_1}(m_i) \neq E_{k_2}^{-1}(c_i)$

   $\Rightarrow$ Keep searching!
This is a known plaintext attack model.

Time: $2 \times \mathcal{O}(2^{56})$

Space: $\mathcal{O}(2^{64})$