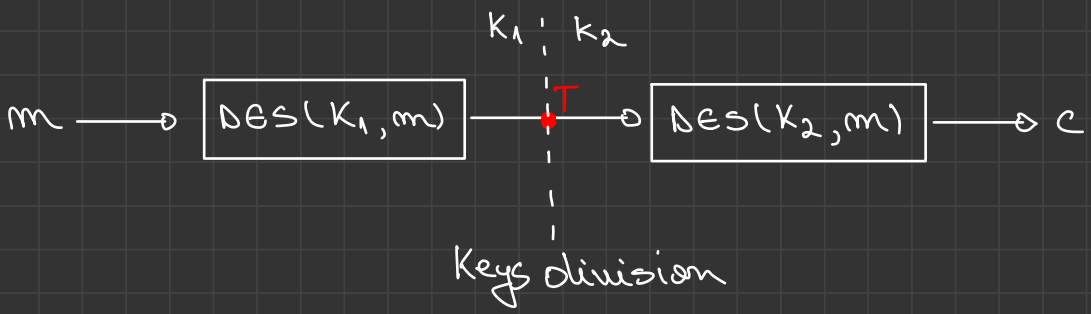
Meet in the Middle Attack - 2DES

- Enc: 2DES(k1, k2, m) = DES(k2, DES(k1, m)) → 2^{112} op
- Dec: $2DES^{-1}$(k1, k2, m) = DES^{-1}(k1, DES^{-1}(k2, m))



① Build a table:

- try all values for K_2;
- $T_i = E(K_i, m)$;
- 2^{56} ops;

	K_2	$T = E(K_2, m)$
1	0...00	T_0
2	0...01	T_1
⋮	⋮	⋮
2^{56}	1...11	$T_{2^{56}-1}$

② Sort by T values the table

- $2^{56} \log 2^{56} \approx 2^{62}$ ops;

③ Binary search:

→ for all possible K_1 keys:

- $T' = Dec^{-1}(K_1, C)$;
- binary search for T' in the table;
- if we find $T' = T_i$ → return (K_1, K_2)
- $2^{56} \log 2^{56} \approx 2^{62}$ ops;

∴ Attack complexity: $< 2^{63} << 2^{112}$