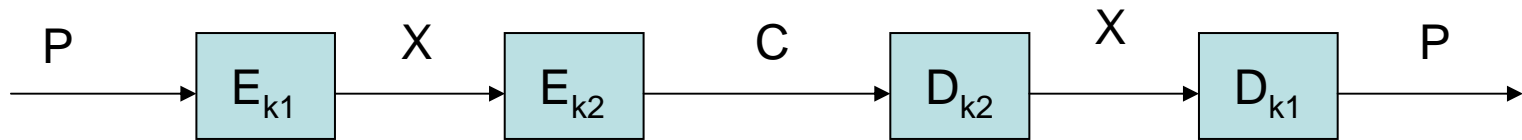


Double DES: Meet in The Middle Attack

Known Plaintext Attack, two pairs: P1;C1 & P2;C2

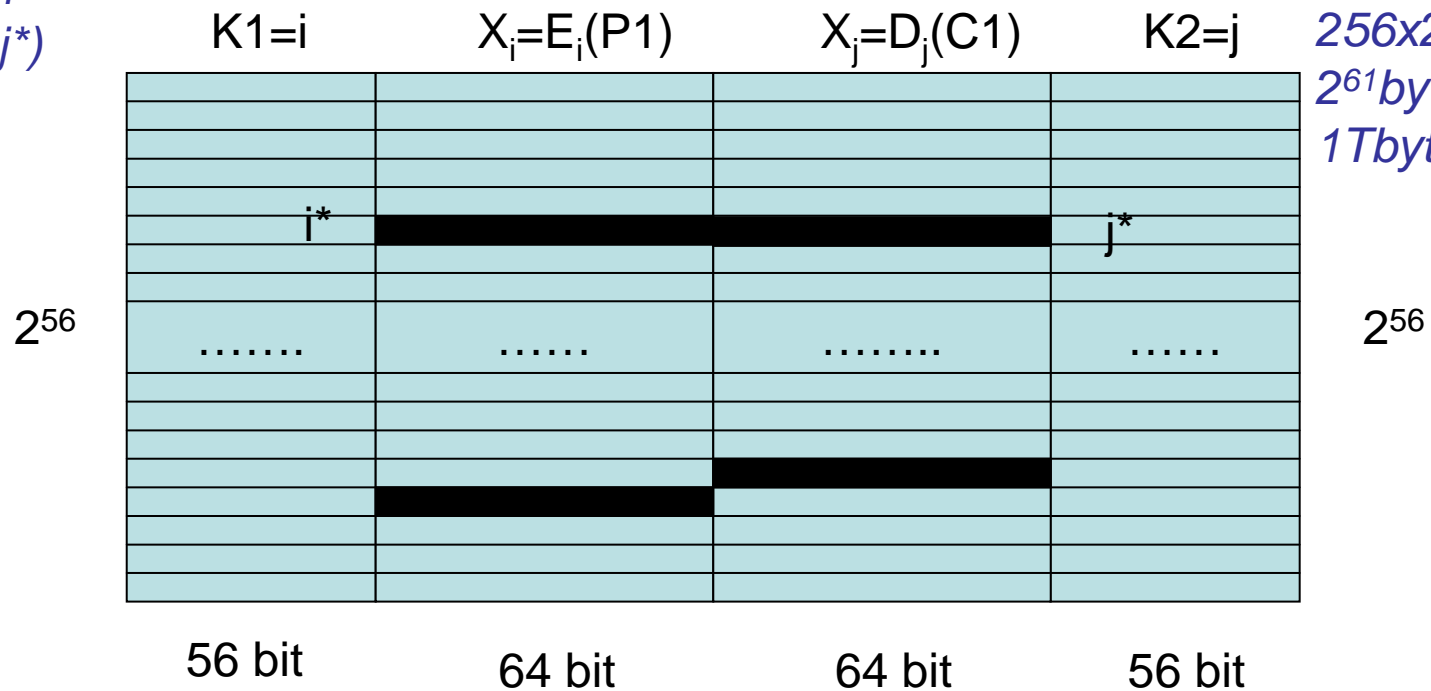


$$X = E_{k_1}(P)$$

$$X = D_{k_2}(C)$$

*First Pair: P1;C1
To find keys (i*;j*)
• $X_{i^*} = X_{j^*}$*

*Total Memory
 $256 \times 2^{56} = 2^{64}$ bit
 2^{61} byte ~ 10^{18} byte
1Tbyte x 10^6 run*



Second Pair: P2;C2

To check keys (i;j*): $P2 = D_{i^*}[D_{j^*}(C2)]$; $C2 = E_{j^*}[E_{i^*}(P2)]$; Average Run # = $2 \times 2^{56} / 2 = 2^{56}$*