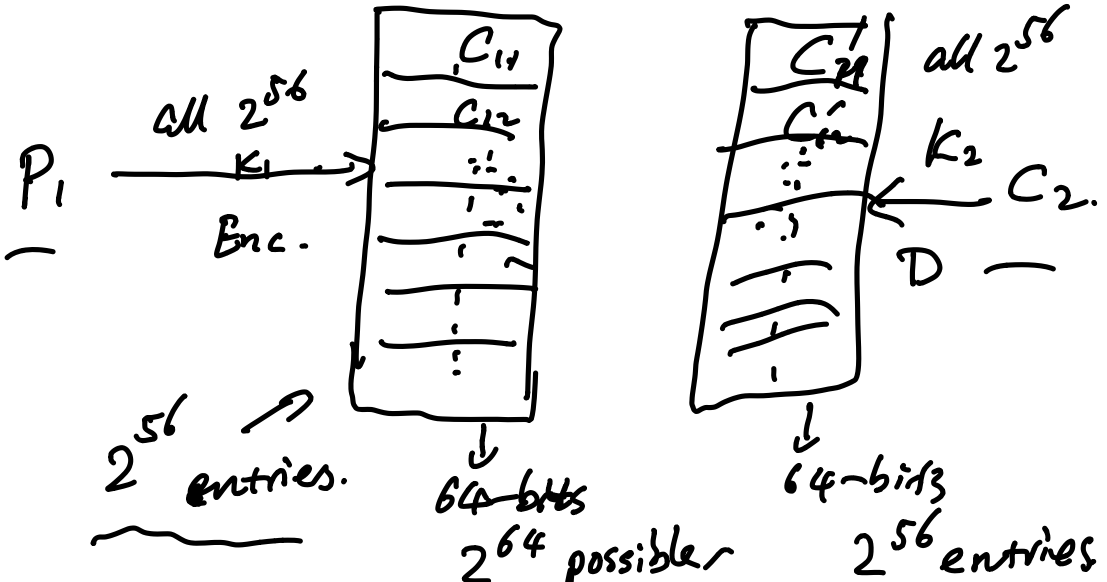
ECE471/571.   3DES & AES

$$P_1 \xrightarrow[E_{K_1}]{} \boxed{C_1} \xrightarrow[E_{K_2}]{} C_2$$

$$(\underset{56}{K_1}, \underset{56 \text{ bits}}{K_2}) \sim 2^{112} \text{ pairs.}$$

Meet-in-the-middle attack.

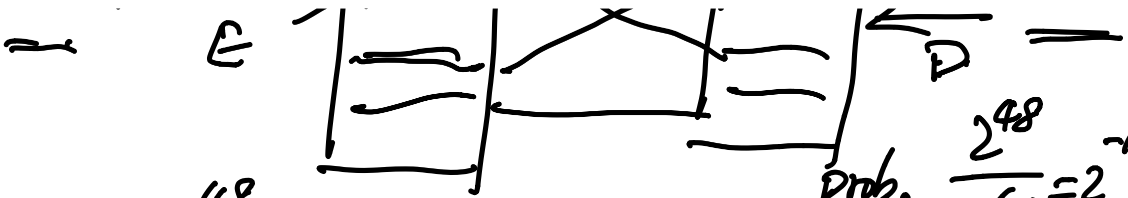


Exp # of same intermediate C_1

$$2^{56} \times \frac{2^{56}}{2^{64}} = 2^{56} \times \frac{1}{2^8} = 2^{48}$$

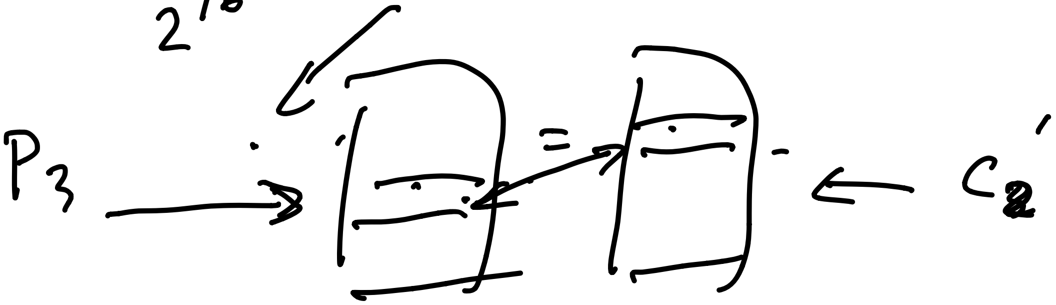
(imposters) (K_{11}, K_{12})

all K_{11}.
P_2
K_{12} C_2'



prob. $\frac{2^{48}}{2^{64}} = 2^{-16}$

$\sim \frac{2^{48}}{2^{16}} = 2^{32}$



storage.

$$2 \times 2^{56} + 2\times 2^{48} + 2 \times 2^{32} \simeq 2^{57}$$

computation

$$\simeq 2^{57}$$

AES.

① not feistel. structure

②. 1 permutation, 2 substitutions in each round

③. simple structure

④. only Add round Key uses the key
$\downarrow$
XOR

⑤. all stages are reversible

Dec. is not the same as Enc.