Notes:

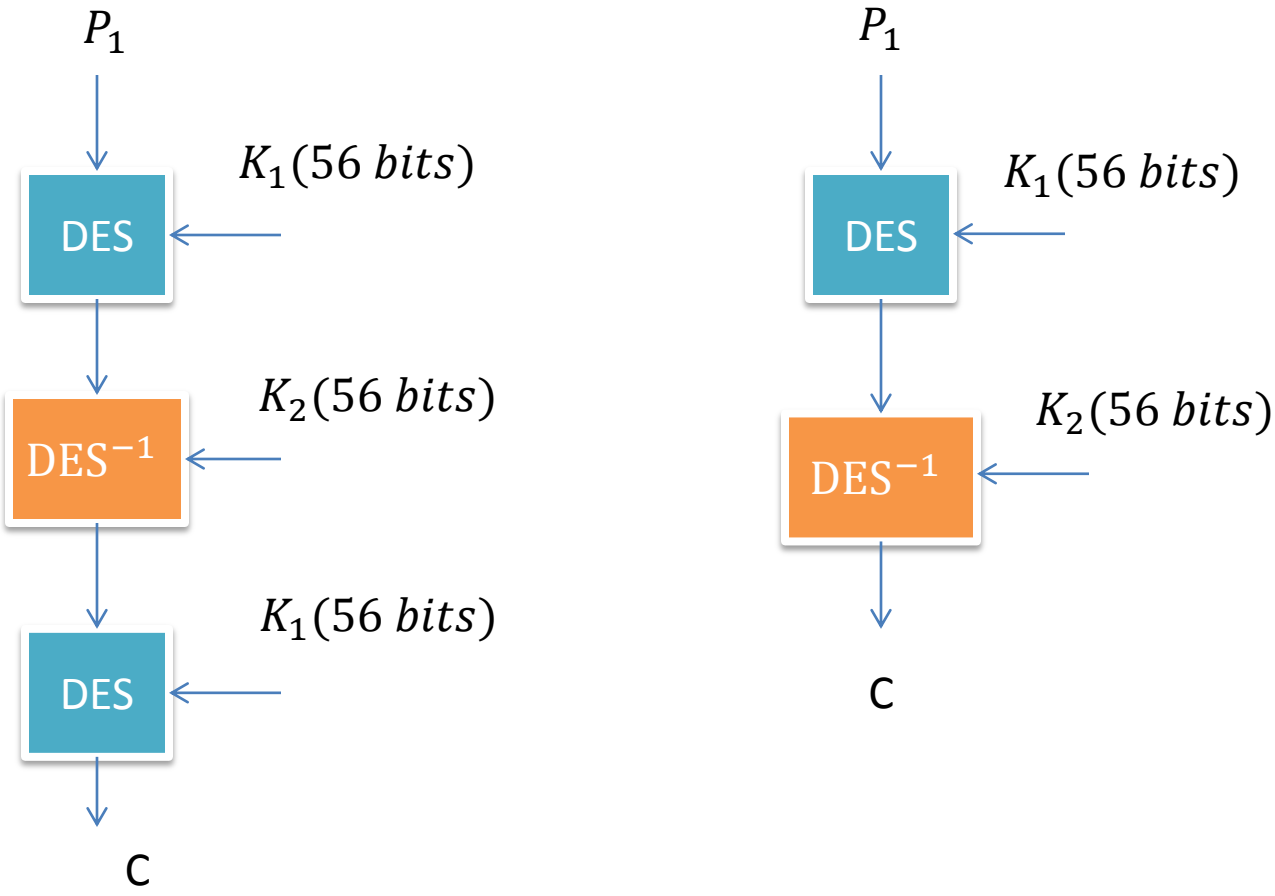
- Lab 1 is due tomorrow!!!
- Homework 1 is out!!! – Due May 1st, 5pm
- Office hours are today at 3:30 in CSE 002

Crypto Exercises

- Given Alice and Bob wish to communicate over a secure channel, what are possible means through which they could exchange the private key, if they plan to use a symmetric encryption scheme?

- Why would you not use the Random IV CBC mode?

3DES


P_1
$K_1(56\ bits)$
DES
$K_2(56\ bits)$
DES^{-1}
$K_1(56\ bits)$
DES
C
P_1
$K_1(56\ bits)$
DES
$K_2(56\ bits)$
DES^{-1}
C

Hashes

- What are some properties of a good hash function?

- What are the weaknesses of hash functions?