ECE 471/571 Modes of Encryption

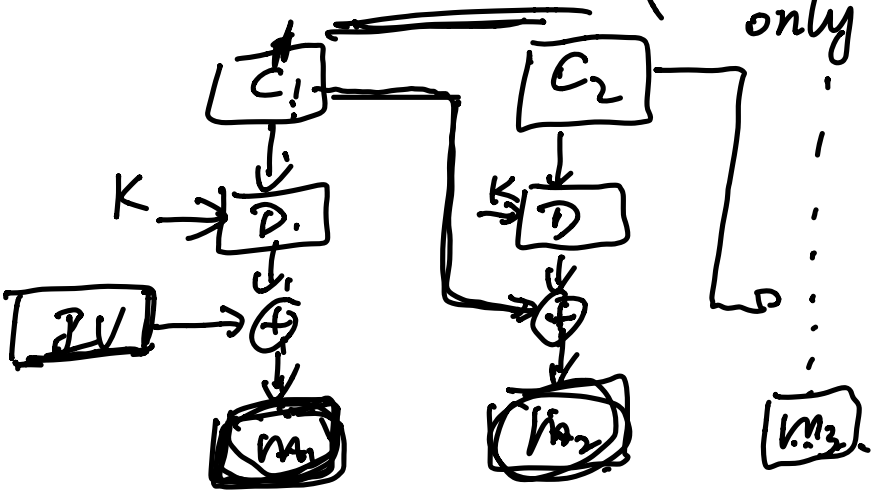
- CBC Mode

different IV for each msg

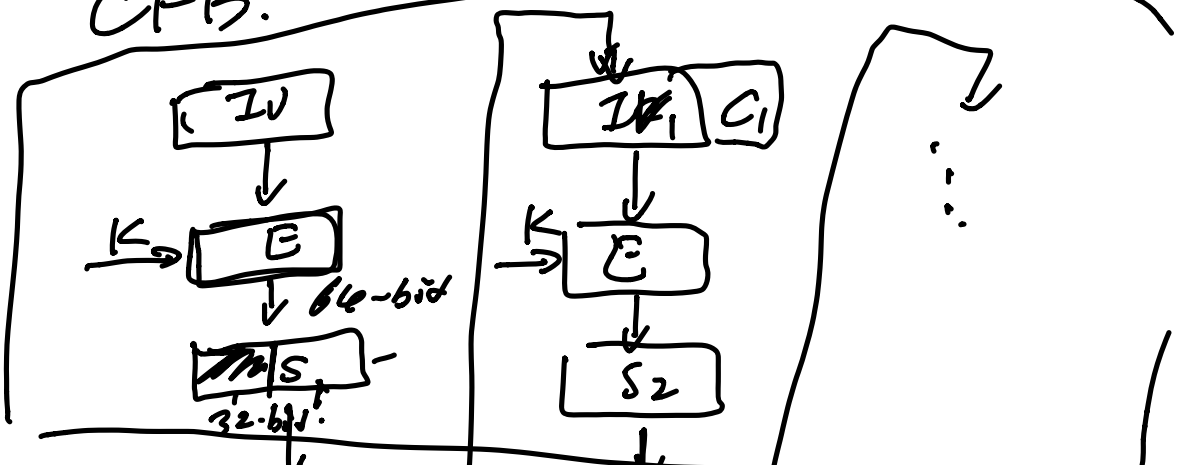
→ different cipher (even for same plaintext)

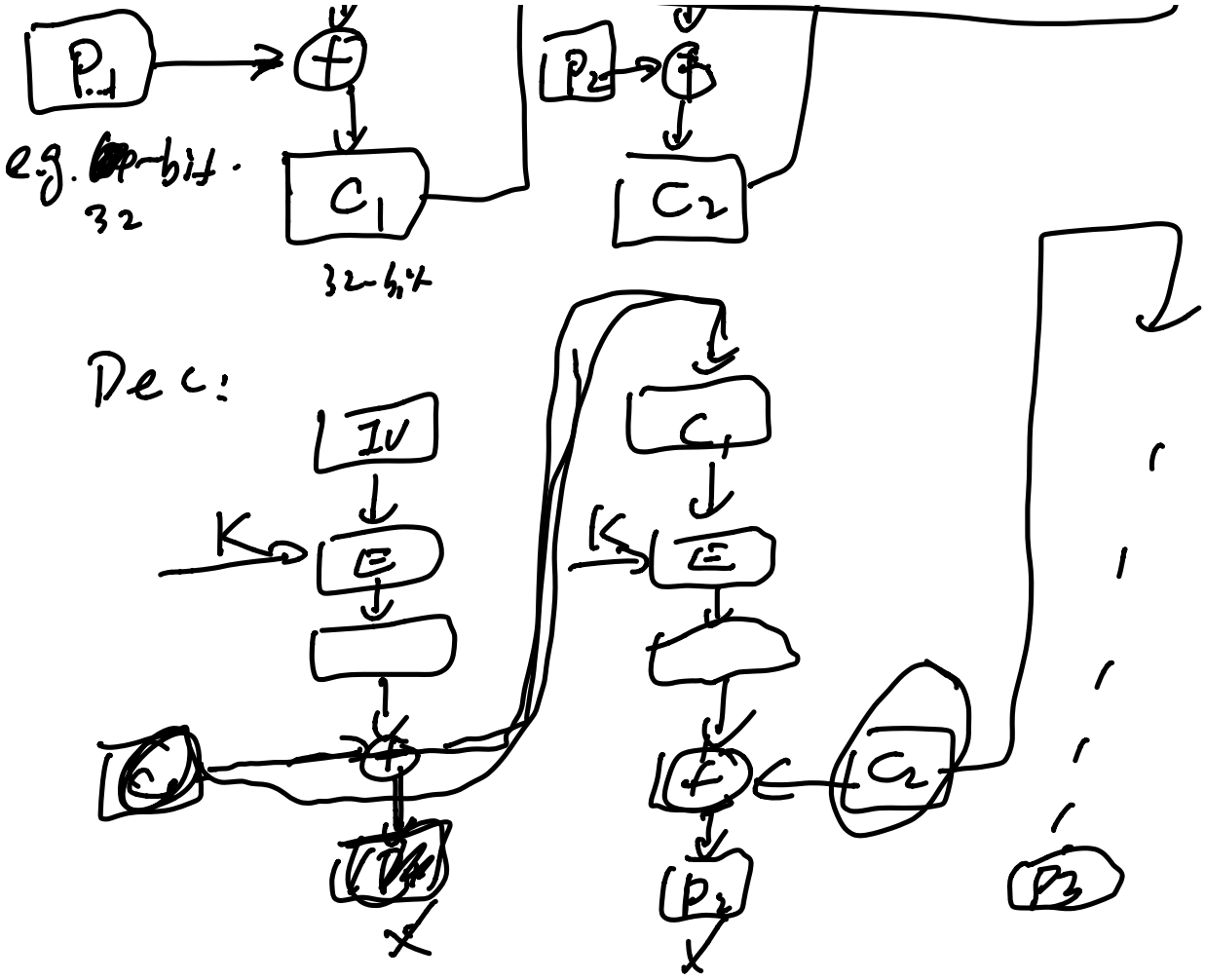
IV is public.

is nonce. (number used only once)



CFB.




$P_{...1}$
eg. bit.
32
C_1
32-bit
P_2
C_2
Dec:
IV
K
E
C_1
E
C_2
P_2