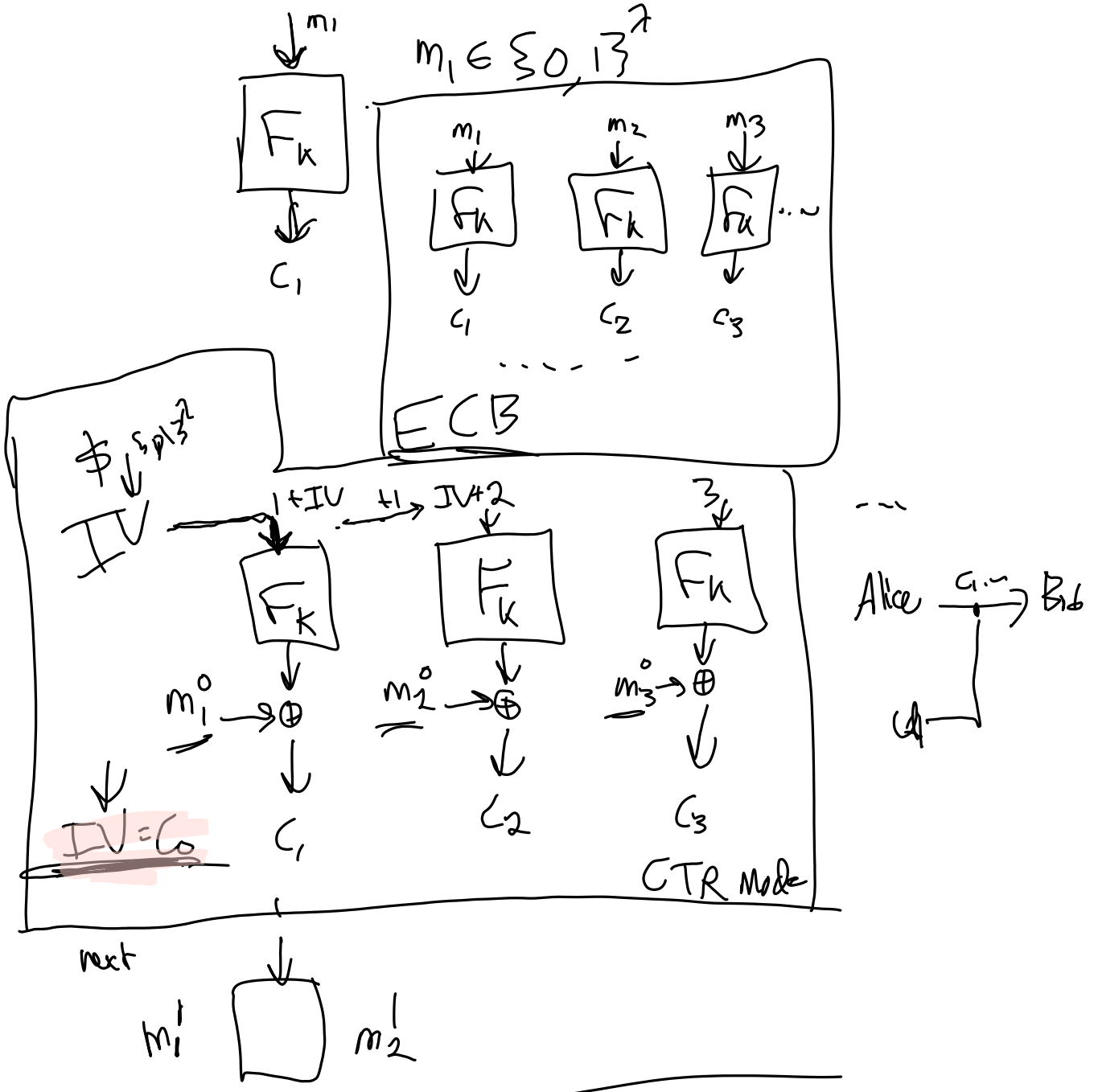
Block Cipher Modes of Operation

Monday, September 13, 2021 3:56 PM

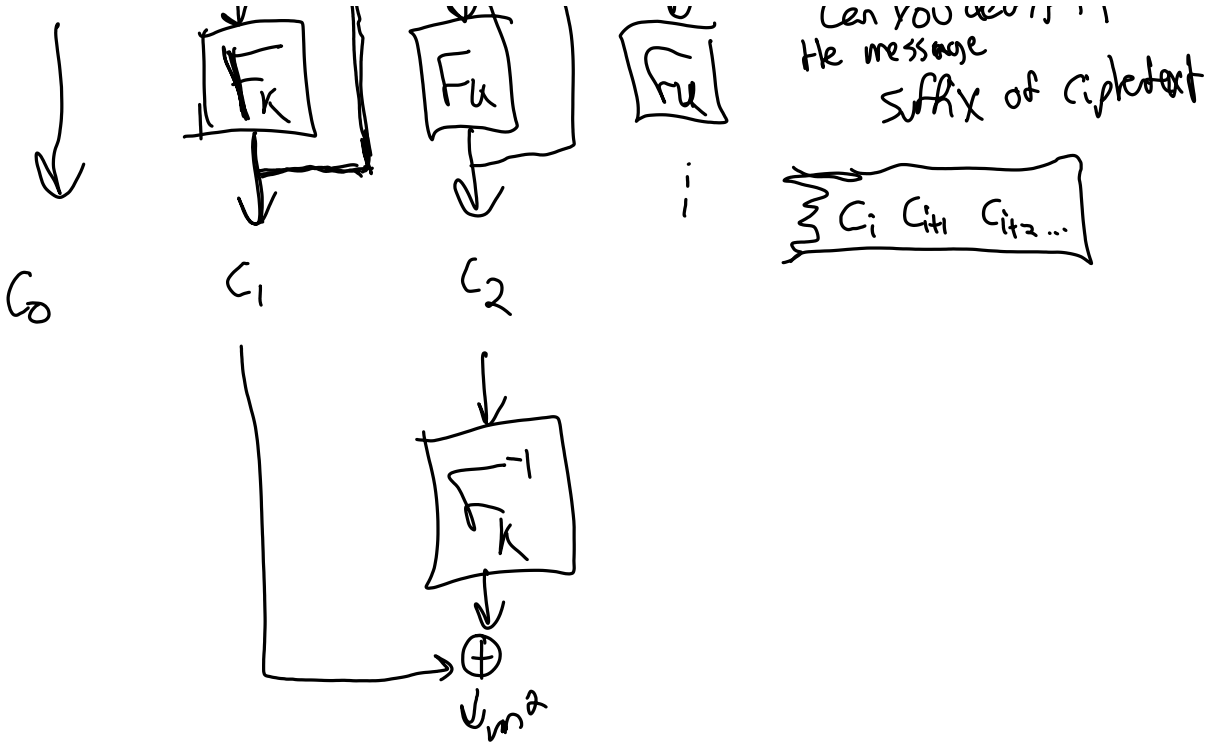
# Block Cipher Modes

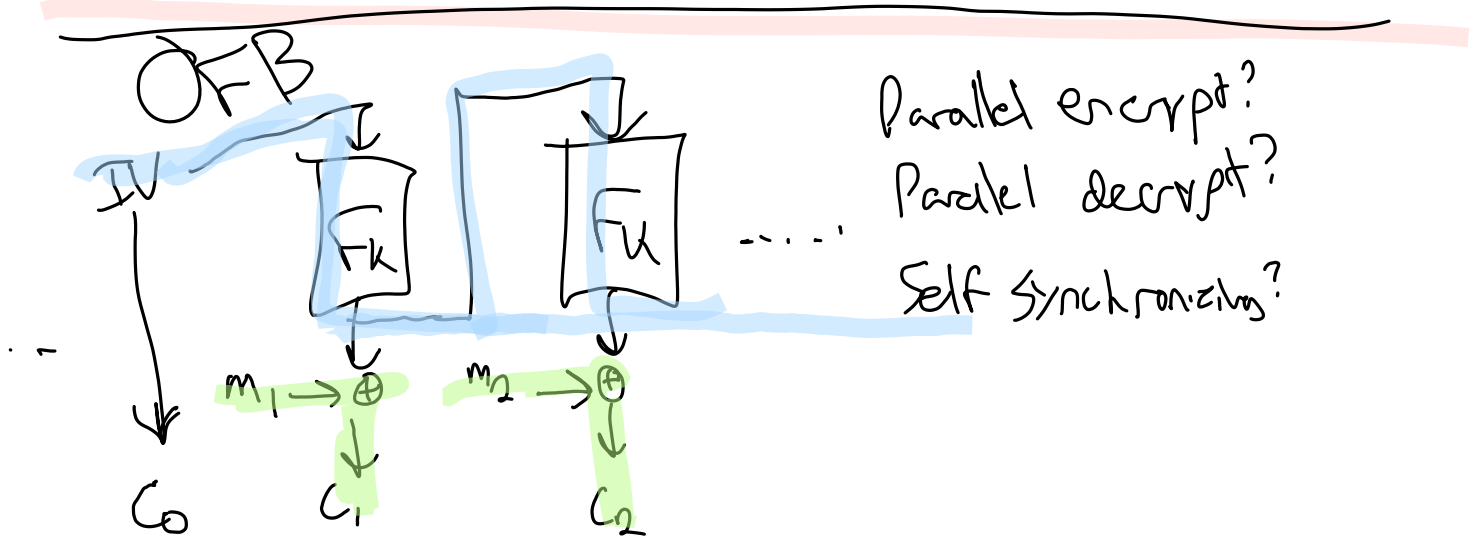
Goals: "use a long term key to encrypt arbitrarily many messages, each of arbitrary length"




## CFB: Ciphertext feedback (for $F_k$ a PRP)


... part of


Can you decrypt the message
suffix of ciphertext
$C_i$ $C_{i+1}$ $C_{i+2}$ ...
$F_K$
$F_K$
$F_K$
i
$C_0$
$C_1$
$C_2$
$F_K^{-1}$
$m_2$


OFB
IV
$F_K$
$F_K$
$m_1$
$m_2$
$C_0$
$C_1$
$C_2$
Parallel encrypt?
Parallel decrypt?
Self synchronizing?