ECB

ex2 -msg 10111110011001 -key 1110101 -op enc -mode ECB

m1=1011111
m2= 0011001

E_k(m1):
1 0 1 1 1 1 1
xor 1 1 1 0 1 0 1
c1= 0 1 0 1 0 1 0

E_k(m2):
0 0 1 1 0 0 1
xor 1 1 1 0 1 0 1
c2= 1 1 0 1 1 0 0

ECB

ex2 -msg 1101111 1000001 -key 0110101 -op dec -mode ECB

c1=1101111
c2= 1000001

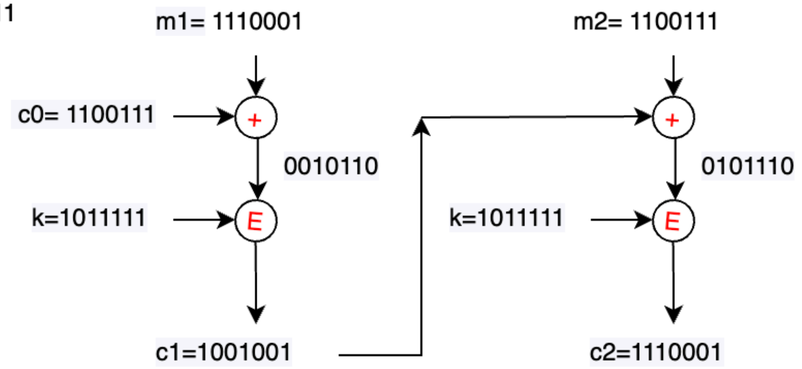
D_k(c1):
1 1 0 1 1 1 1
xor 0 1 1 0 1 0 1
m1= 1 0 1 1 0 1 0

D_k(c2):
1 0 0 0 0 0 1
xor 0 1 1 0 1 0 1
m2= 1 1 1 0 1 0 0

CBC

ex2 -msg 1110001 1100111 -key 1011111 -op enc -mode CBC -iv 1100111

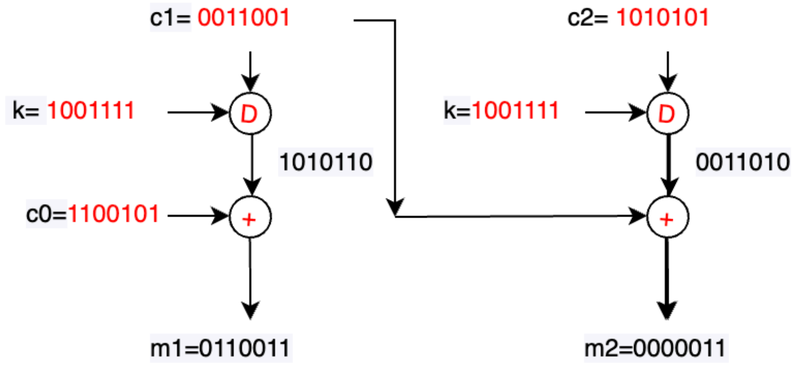
m1= 1110001
m2= 1100111
c0=iv=1100111



Résultat = c0 c1 c2 = 1100111 1001001 1110001

CBC

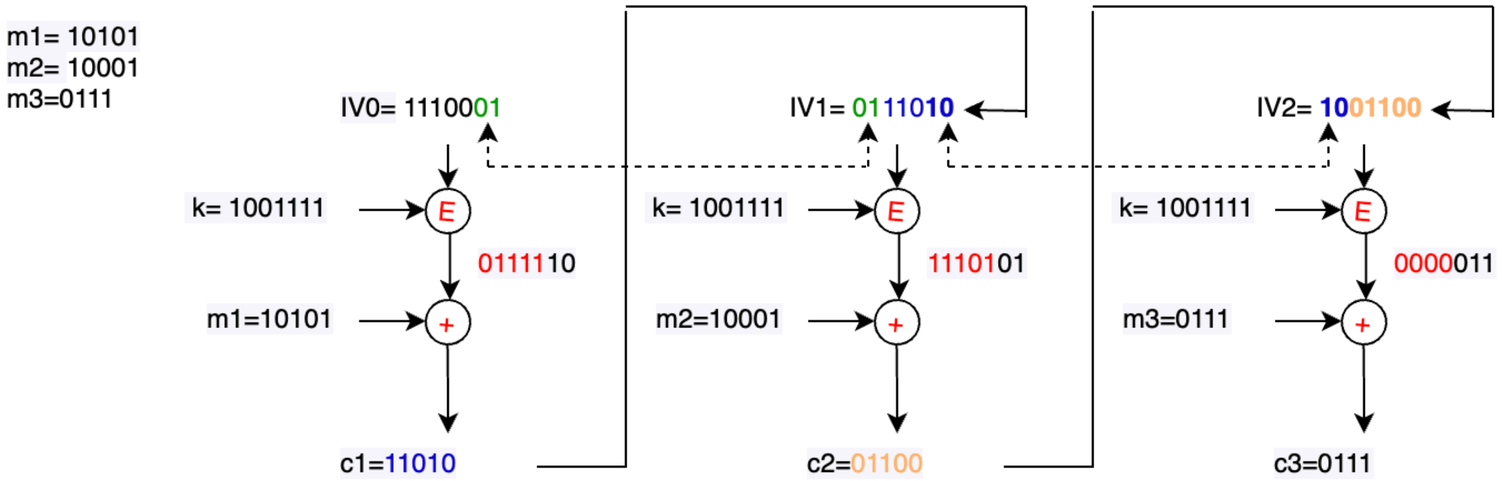
ex2 -msg 1100101 0011001 1010101 -key 1001111 -op dec -mode CBC



Résultat = m1 m2 = 0110011 0000011

CFB

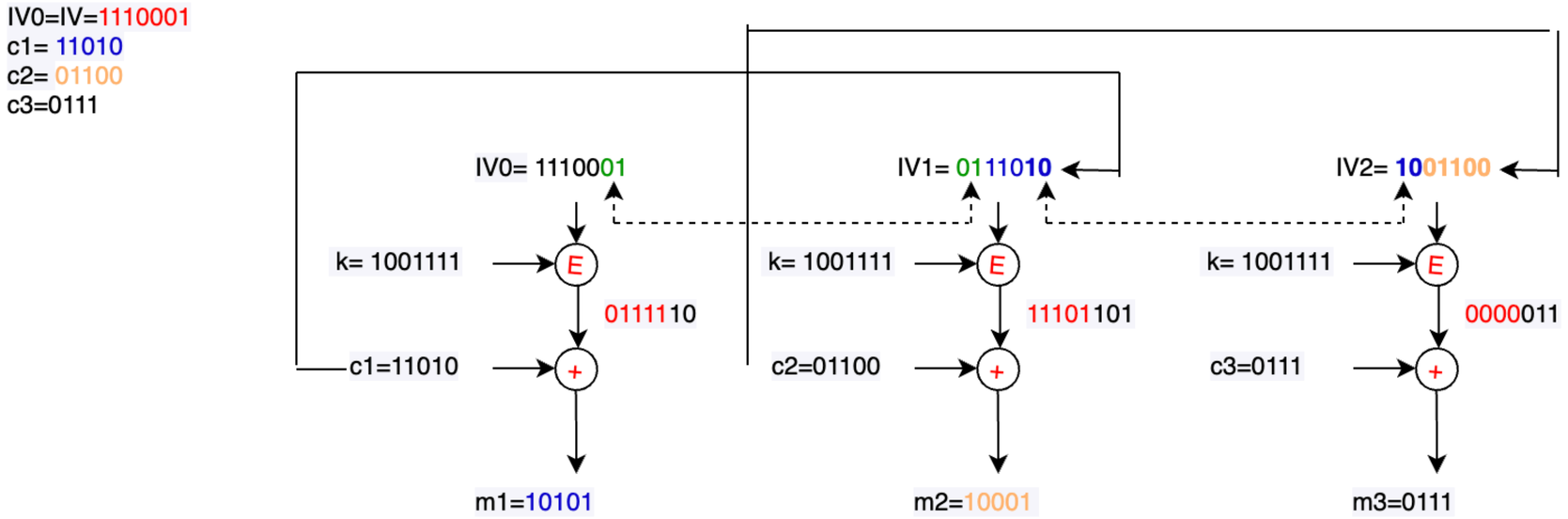
ex2 -msg 101011 00010111 -key 1001111 -op enc -mode CFB -iv 1110001 -r 5



Résultat = iv c1 c2 c3 = 1110001 11010 01100 0111

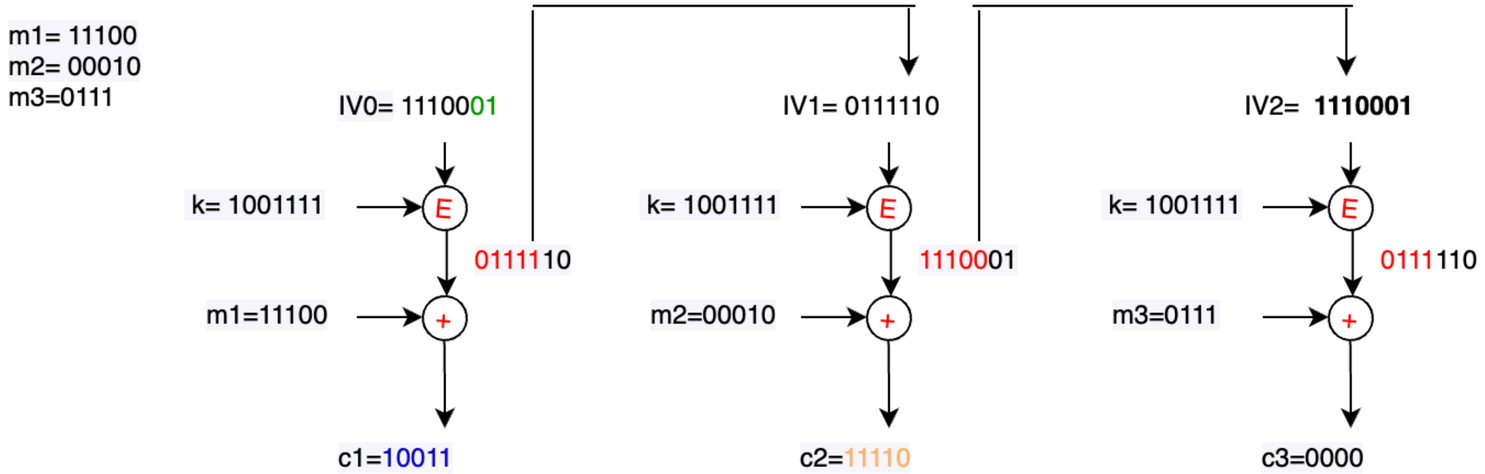
CFB

ex2 -msg 1110001 11010 01100 0111 -key 1001111 -op dec -mode CFB -r 5



OFB

ex2 -msg 11100 00010 0111 -key 1001111 -op enc -mode OFB -iv 1110001 -r 5

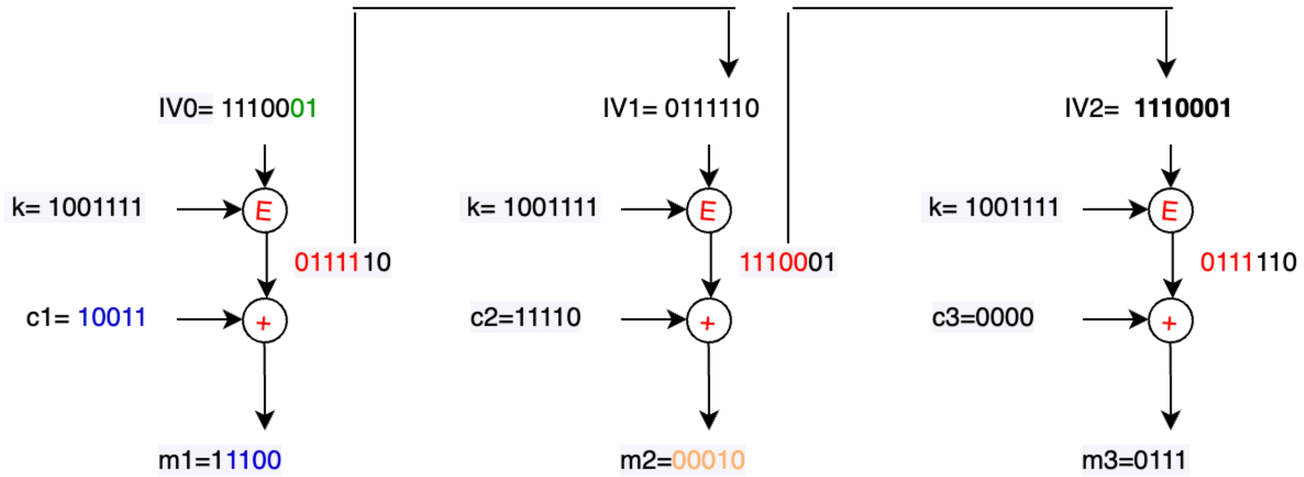


Résultat = iv c1 c2 c3 = 1011001 10011 11110 0000

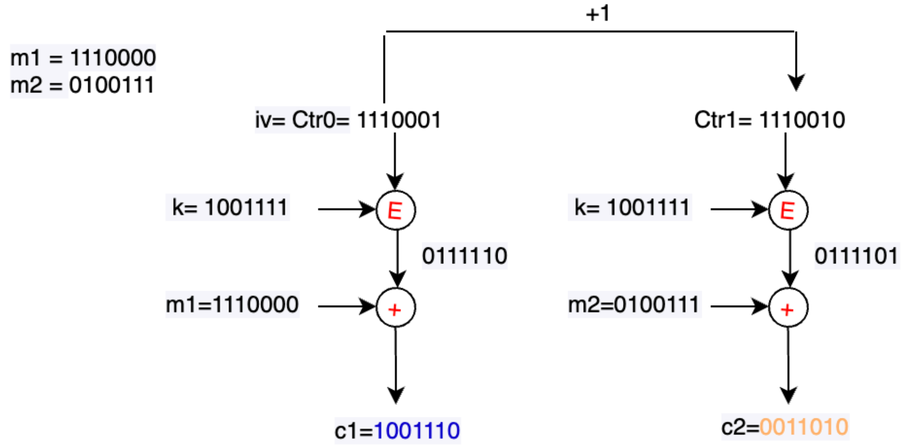
OFB

ex2 -msg 1110001 10011 11110 0000 -key 1001111 -op dec -mode OFB -r 5

IV0=IV=1110001
c1= 10011
c2= 11110
c3=0000



CTR ex2 -msg 1110000 0100111 -key 1001111 -op enc -mode CTR -iv 1110001



Résultat = iv c1 c2 = 11110001 1001110 0011010

CTR ex2 -msg 1110001 1001110 0011010 -key 1001111 - op dec -mode CTR