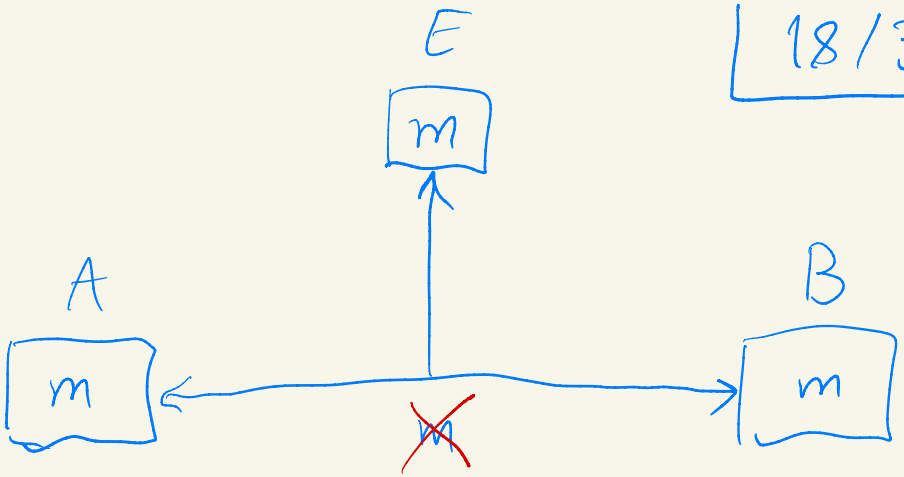
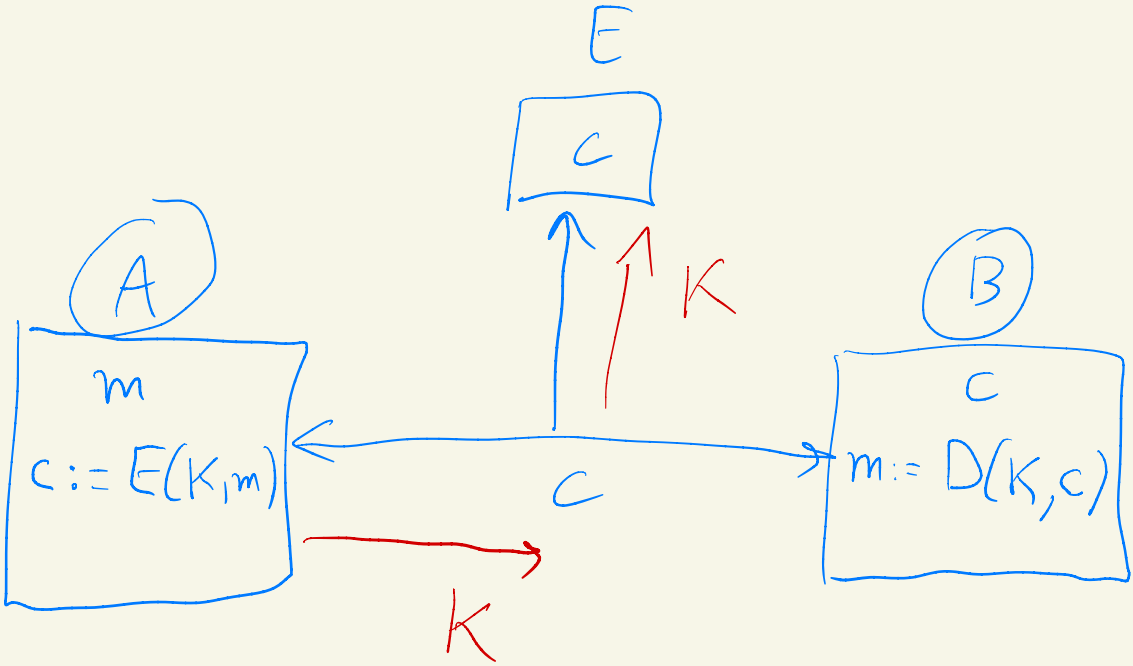
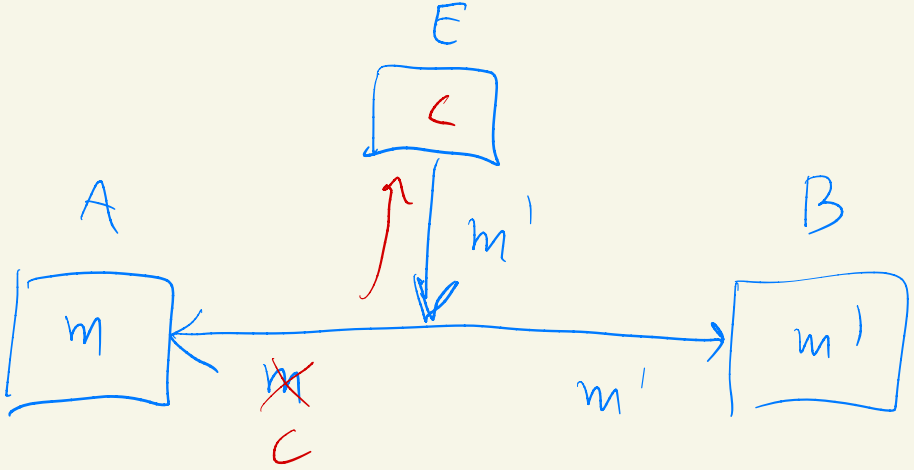
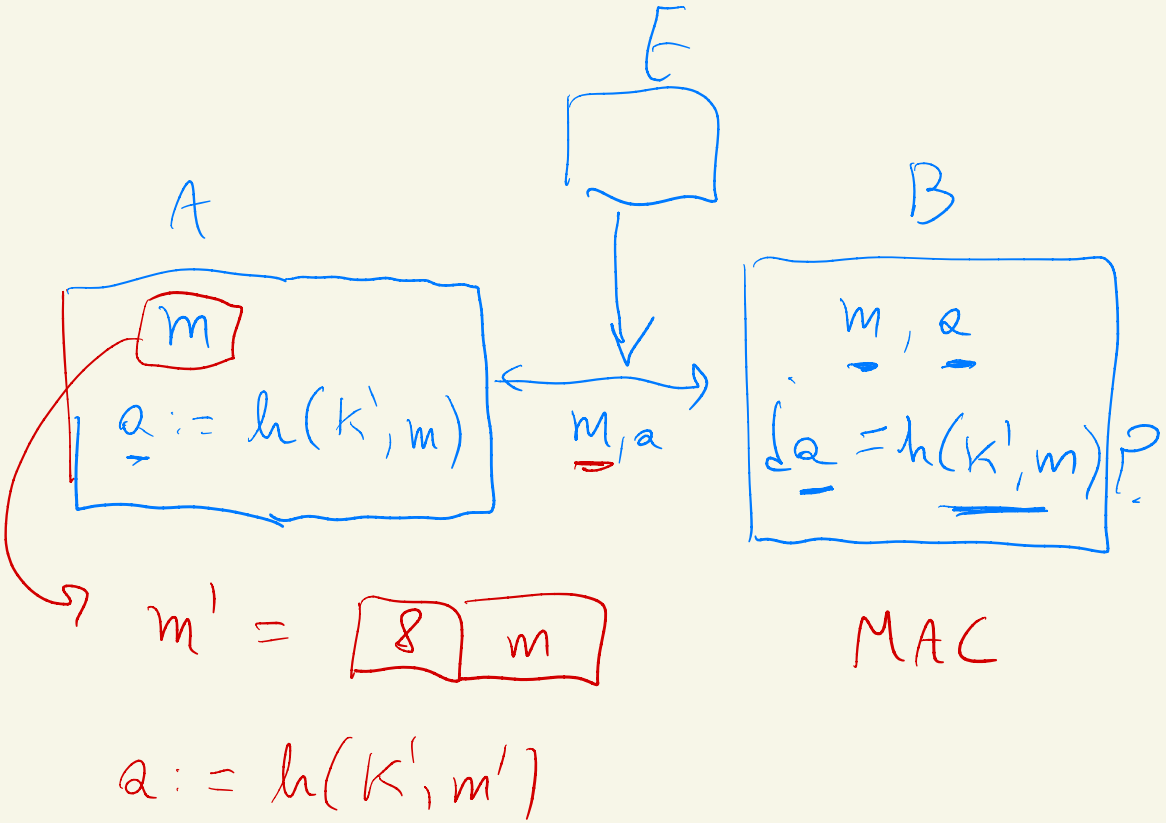
18/3/21

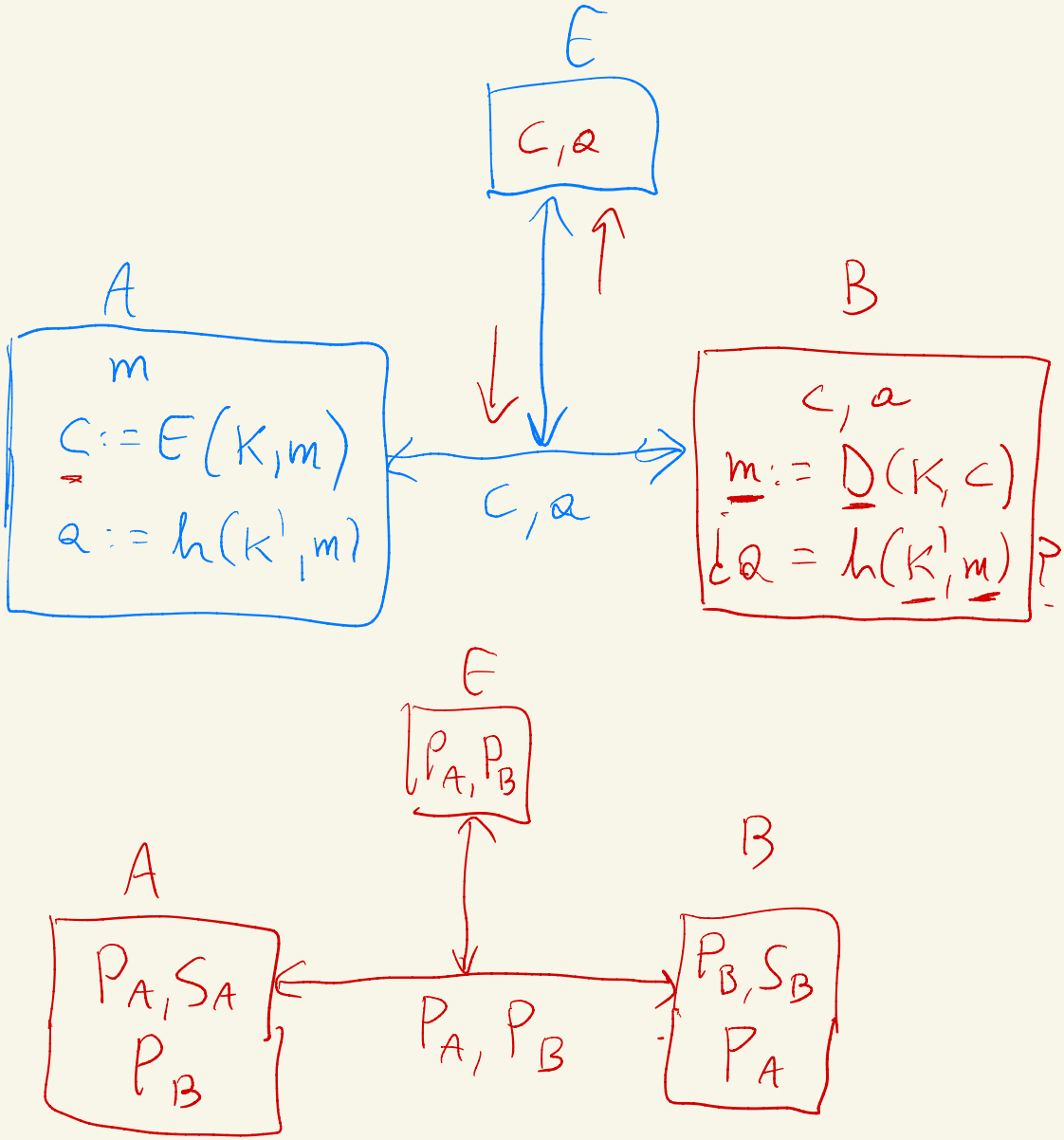


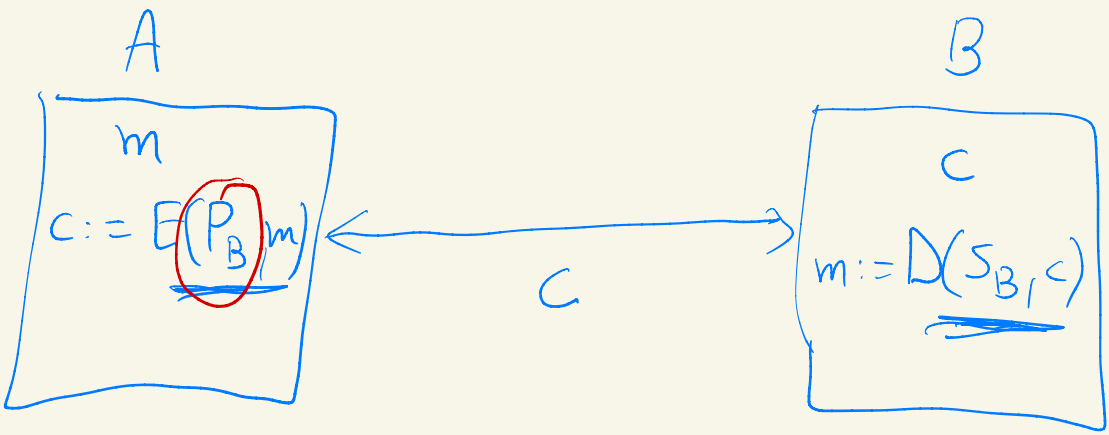


$$D(k, E(K, m)) = m$$


E
C
A
B
m
m'
m
m'
m'
C


E
A
B
m
a := h(k', m)
m, a
m, a
a = h(k', m) ?
m' = 8 m
MAC
a := h(k', m')


E
c, a
A
m
c := E(K, m)
a := h(k', m)
B
c, a
m := D(K, c)
a = h(k', m) ?
c, a
E
P_A, P_B
A
P_A, S_A
P_B
B
P_B, S_B
P_A
P_A, P_B



$$D(S_B, E(P_B, m)) = m$$

$$D(P_B, E(P_B, m)) \neq m$$

c

$$D(P_B, E(P_B, 1)) = 1$$

$x \cdot y \bmod z = 1$

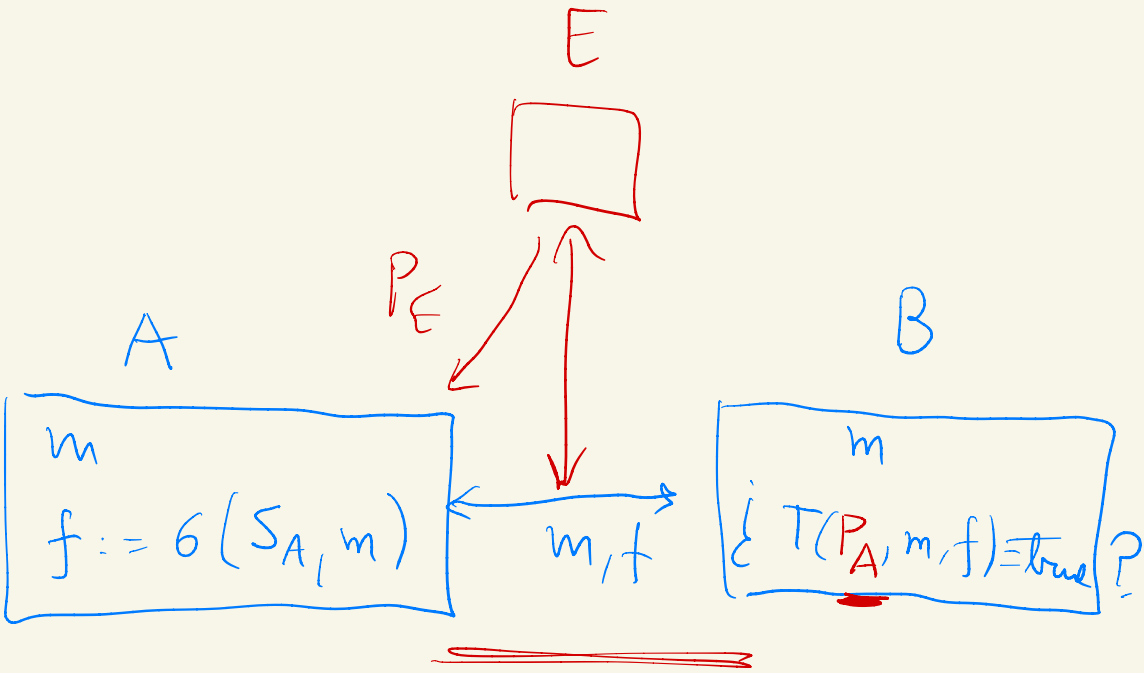
$\phi(N)$

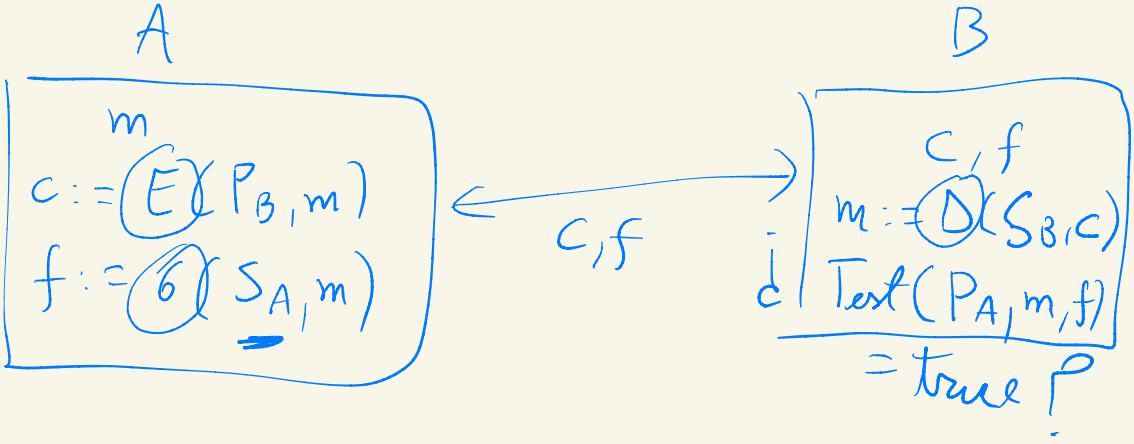
(x, N)

(y, N)

$N = P \cdot Q$

$\phi(N) = (P-1)(Q-1)$




A
B
m
c := E(P_B, m)
f := S(S_A, m)
c, f
m := D(S_B, c)
Test(P_A, m, f)
= true ?