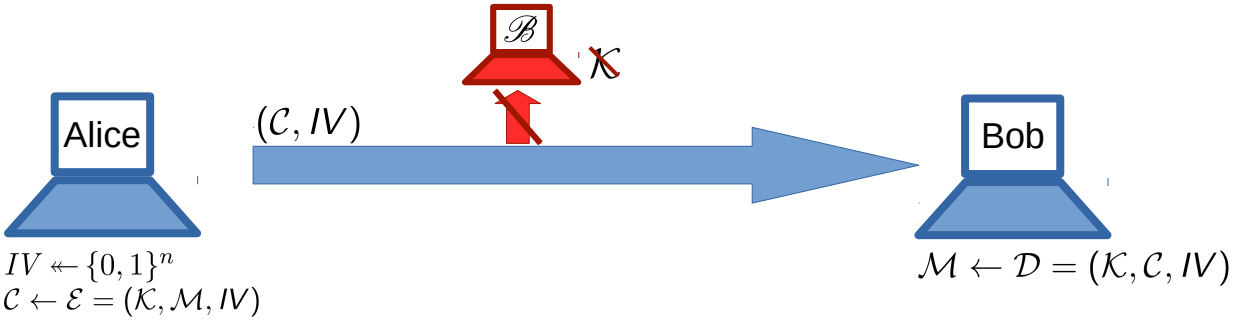
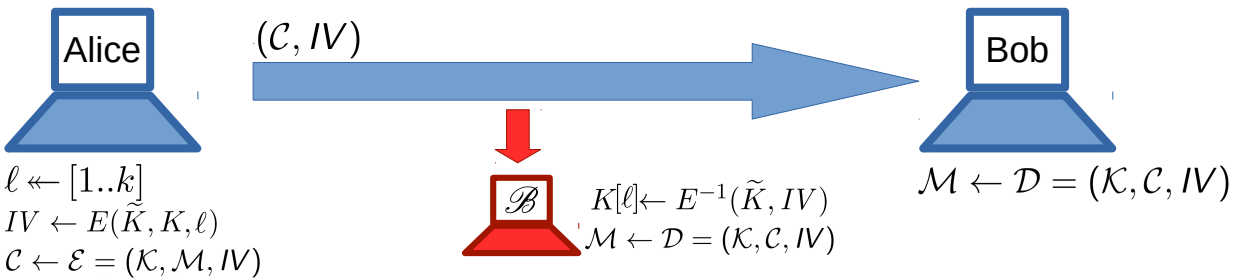

$\mathscr{B}$
$\mathcal{K}$
Alice
$(\mathcal{C}, IV)$
Bob
$IV \twoheadleftarrow \{0,1\}^n$
$\mathcal{C} \leftarrow \mathcal{E} = (\mathcal{K}, \mathcal{M}, IV)$
$\mathcal{M} \leftarrow \mathcal{D} = (\mathcal{K}, \mathcal{C}, IV)$


Alice
$(\mathcal{C}, IV)$
Bob
$\mathscr{B}$
$\ell \twoheadleftarrow [1..k]$
$IV \leftarrow E(\widetilde{K}, K, \ell)$
$\mathcal{C} \leftarrow \mathcal{E} = (\mathcal{K}, \mathcal{M}, IV)$
$K[\ell] \leftarrow E^{-1}(\widetilde{K}, IV)$
$\mathcal{M} \leftarrow \mathcal{D} = (\mathcal{K}, \mathcal{C}, IV)$
$\mathcal{M} \leftarrow \mathcal{D} = (\mathcal{K}, \mathcal{C}, IV)$