

private communication		
Alice	$\longleftrightarrow$ of shared key $k \in \mathcal{K}$ $\longleftrightarrow$	Bob
	on public network	
message $m_A \in \mathcal{M}$ compute $c_A = e_k(m_A)$ transmit c_A	$\rightarrow$ ciphertext c_A $\rightarrow$	receive c_A compute $m_A = d_k(c_A)$
receive c_B compute $m_B = d_k(c_B)$	$\leftarrow$ ciphertext c_B $\leftarrow$	message $m_B \in \mathcal{M}$ compute $c_B = e_k(m_B)$ transmit c_B
etc....		