

Alice	on public network	Bob
download k_e	$\leftarrow$ public key k_e $\leftarrow$	pick $k_d \in \mathcal{K}_d$ compute $k_e = \mathcal{E}(k_d) \in \mathcal{K}_e$ publish k_e
message $m \in \mathcal{M}$ compute $c = e_{k_e}(m)$ transmit c	$\rightarrow$ ciphertext c $\rightarrow$	receive c compute $m = d_{k_d}(c)$