

Larry	on public network	Bob
download k_e	$\leftarrow$ public key k_e $\leftarrow$	pick $k_d \in \mathcal{K}_d$ compute $k_e = \mathcal{E}(k_d)$ publish k_e
receive (m, s)	$\leftarrow$ signed message (m, s) $\leftarrow$	message $m \in \mathcal{M}$ compute $s = d_{k_d}(m)$ transmit (m, s)
if $e_{k_e}(s) = m$ ACCEPT otherwise, REJECT		