

Alice	Eve	Bob
	intercept $k_e^B \leftarrow$	generate keys: public k_e^B , private k_d^B publish k_e^B
download k_e^E	generate keys: public k_e^E , private k_d^E $\leftarrow k_e^E$, spoof origin	
message $m \in \mathcal{M}$ compute $c_A = e_{k_e^E}(m)$ transmit c_A	$\rightarrow c_A$, intercept	
	extract the cleartext $m = d_{k_d^E}(c_A)$ change to m' if desired compute $c_E = e_{k_e^B}(m')$ spoof origin $c_E \rightarrow$	receive c_E
		read the message $m' = d_{k_d^B}(c_E)$