



Defeat replay attack with a nonce  
(not fully secured)











A





**Reply at a later response!**

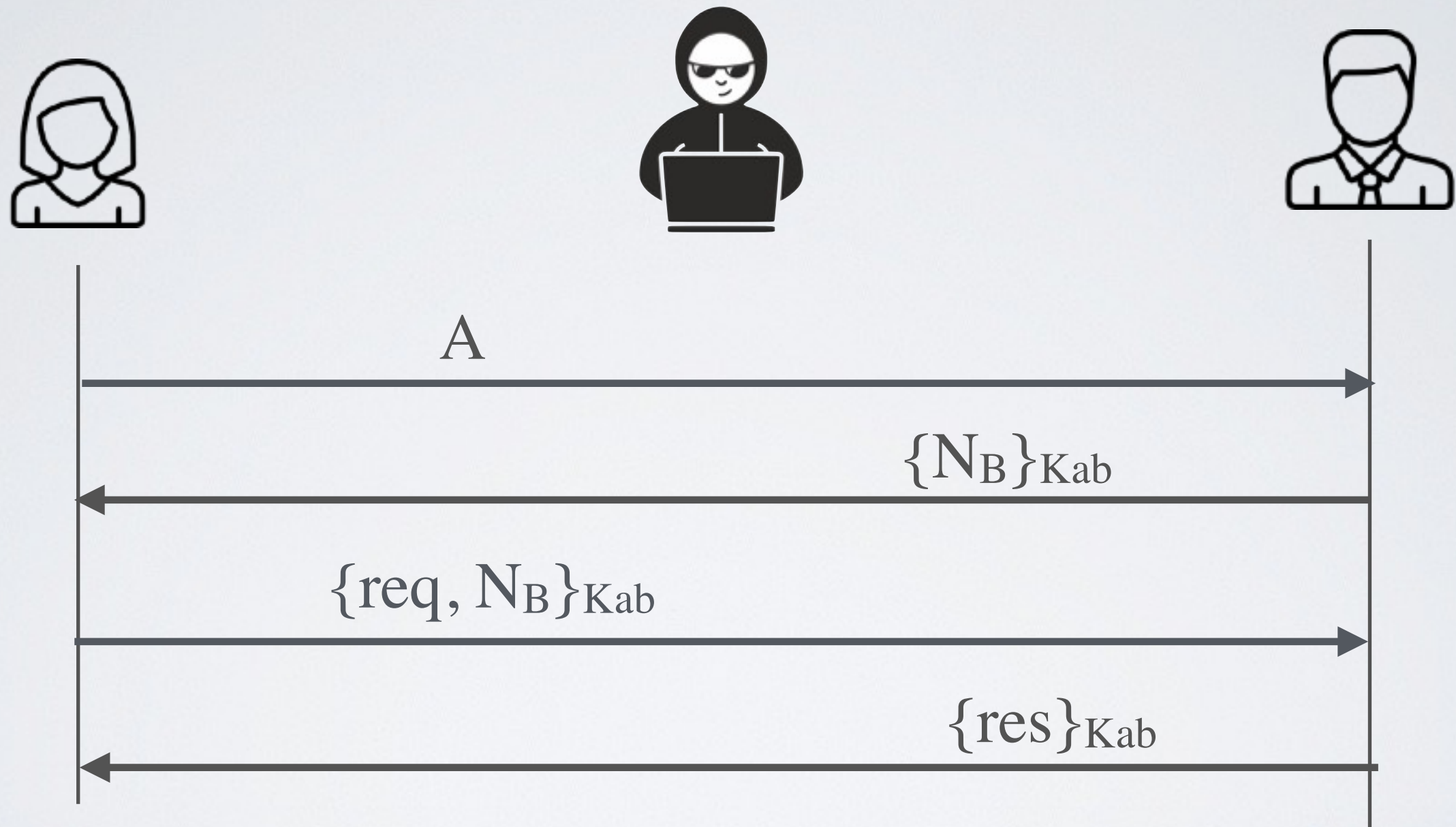
$$\{\text{req}, N_B\}_{K_{ab}}$$


$\{\text{res}\}_{Kab}$




$$\{N_B\} K_{ab}$$

# Defeat replay attack with a nonce (not fully secured)



**Replay attack on the response!**

# Defeat replay attack with a double nonce

