



Defeat replay attack with a double nonce











A





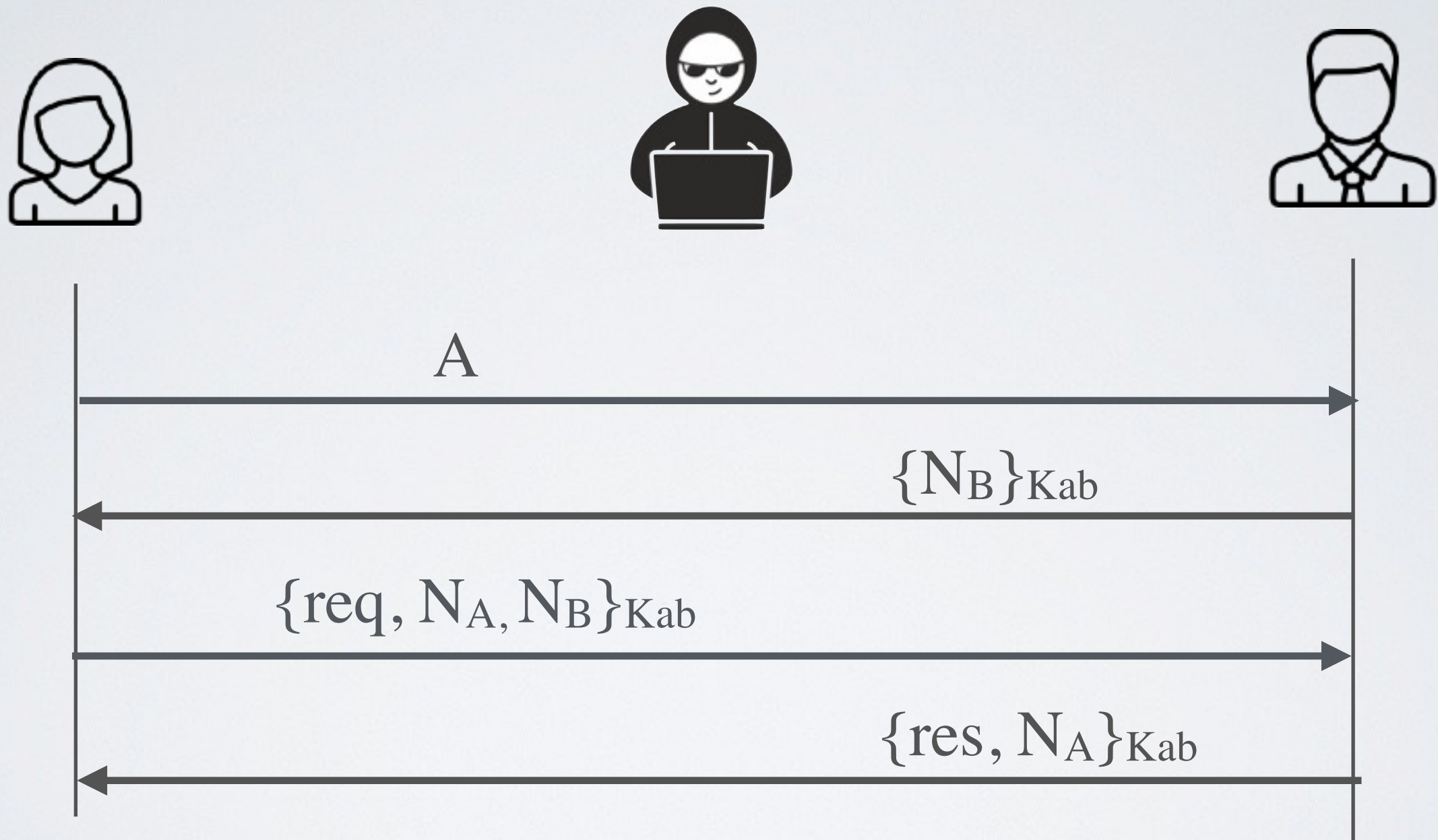
$$\{\text{req}, N_A, N_B\}_{K_{ab}}$$




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


$$\{N_B\}_{Kab}$$

# Defeat replay attack with a double nonce



# The challenge of key exchange