

Defeat replay attack with a double nonce











A



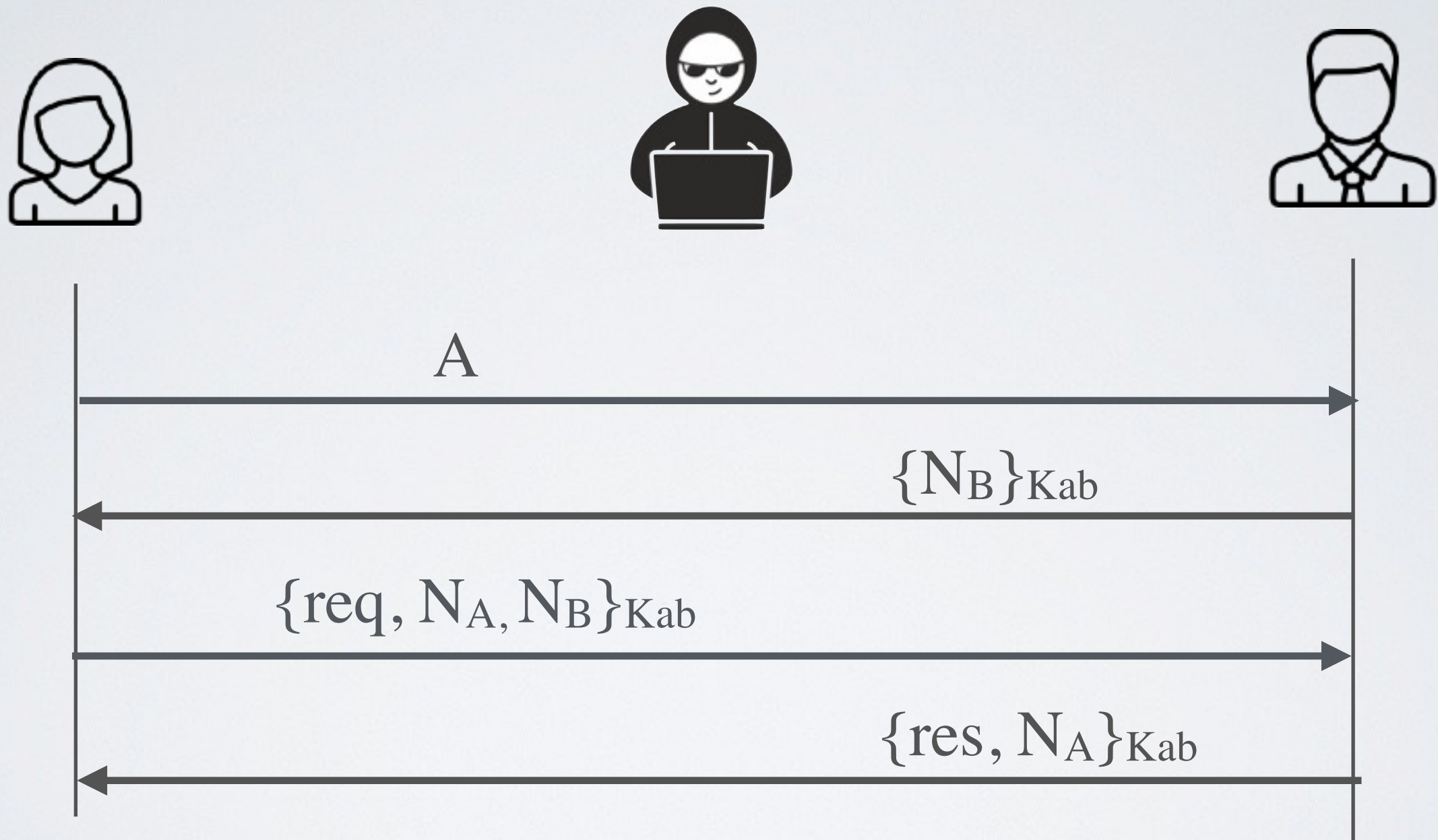
$$\{\text{req}, N_A, N_B\}_{K_{ab}}$$




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


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

Defeat replay attack with a double nonce



The challenge of key exchange