Defeat replay attack with a double nonce

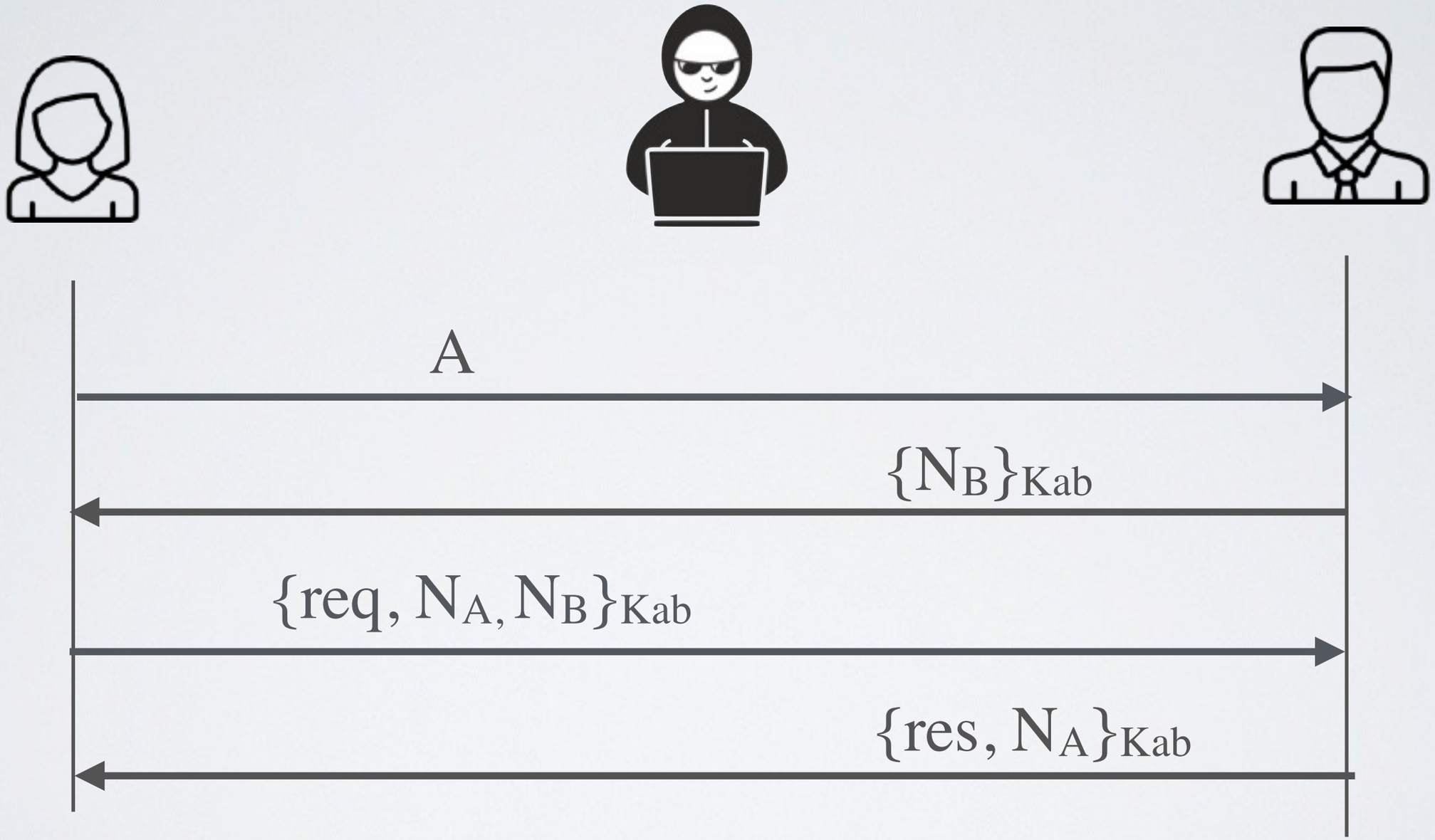

A

{req, N_A, N_B}Kab

{res, NA}Kab

$\{N_B\}_{Kab}$

Defeat replay attack with a double nonce



The challenge of key exchange