Replay attack

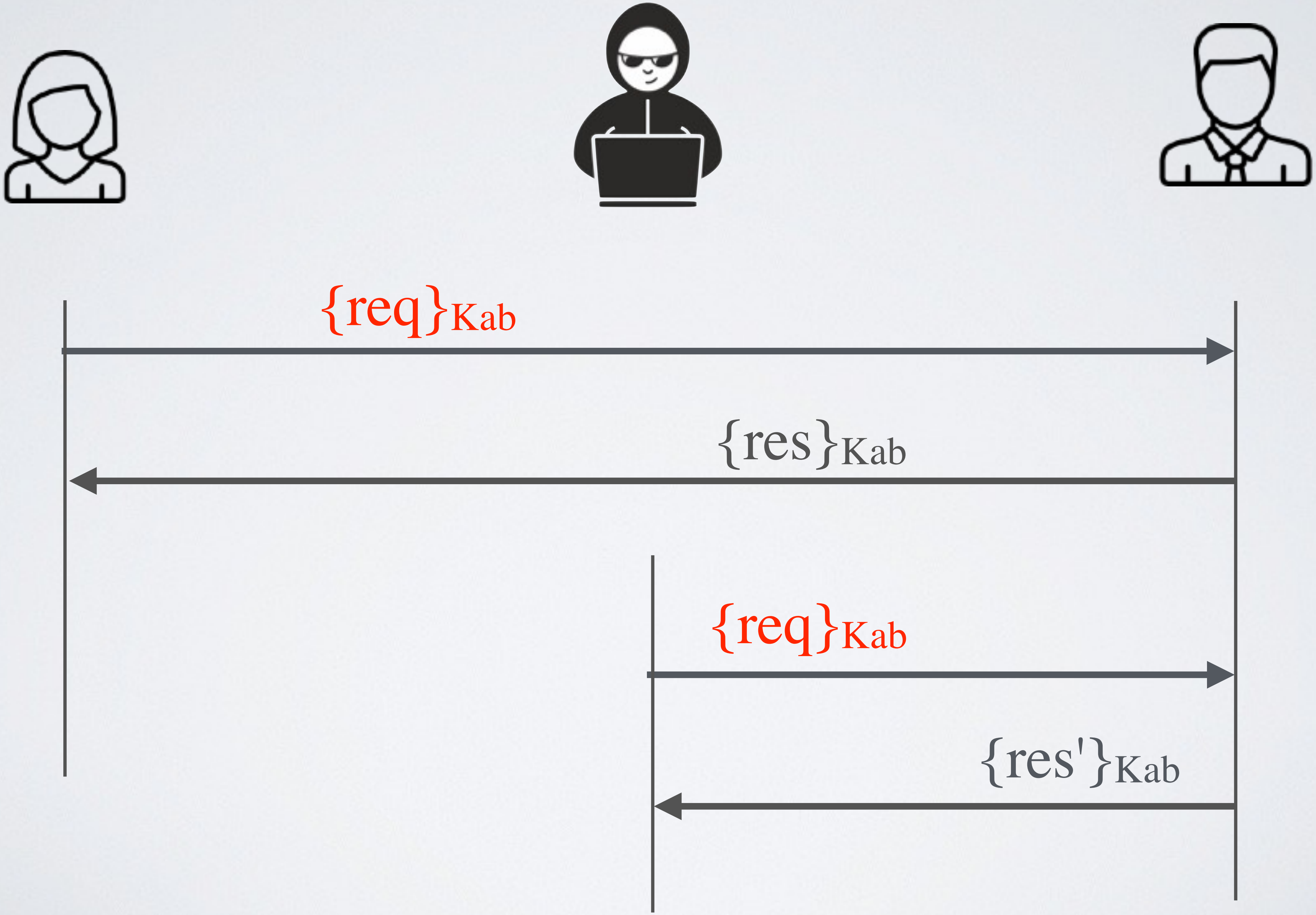
{req}Kab


$\{req\}_{Kab}$

$\{res'\}_{Kab}$

{res}Kab

Replay attack



$\{req\}_{Kab}$

$\{res\}_{Kab}$

$\{req\}_{Kab}$

$\{res'\}_{Kab}$

Counter replay attacks

Several solutions:

- **use a nonce (random number)**
- use sequence numbers
- use timestamps
- have fresh key for every transaction (key exchange problem)