

Reply attack













$\{req\}Kab$





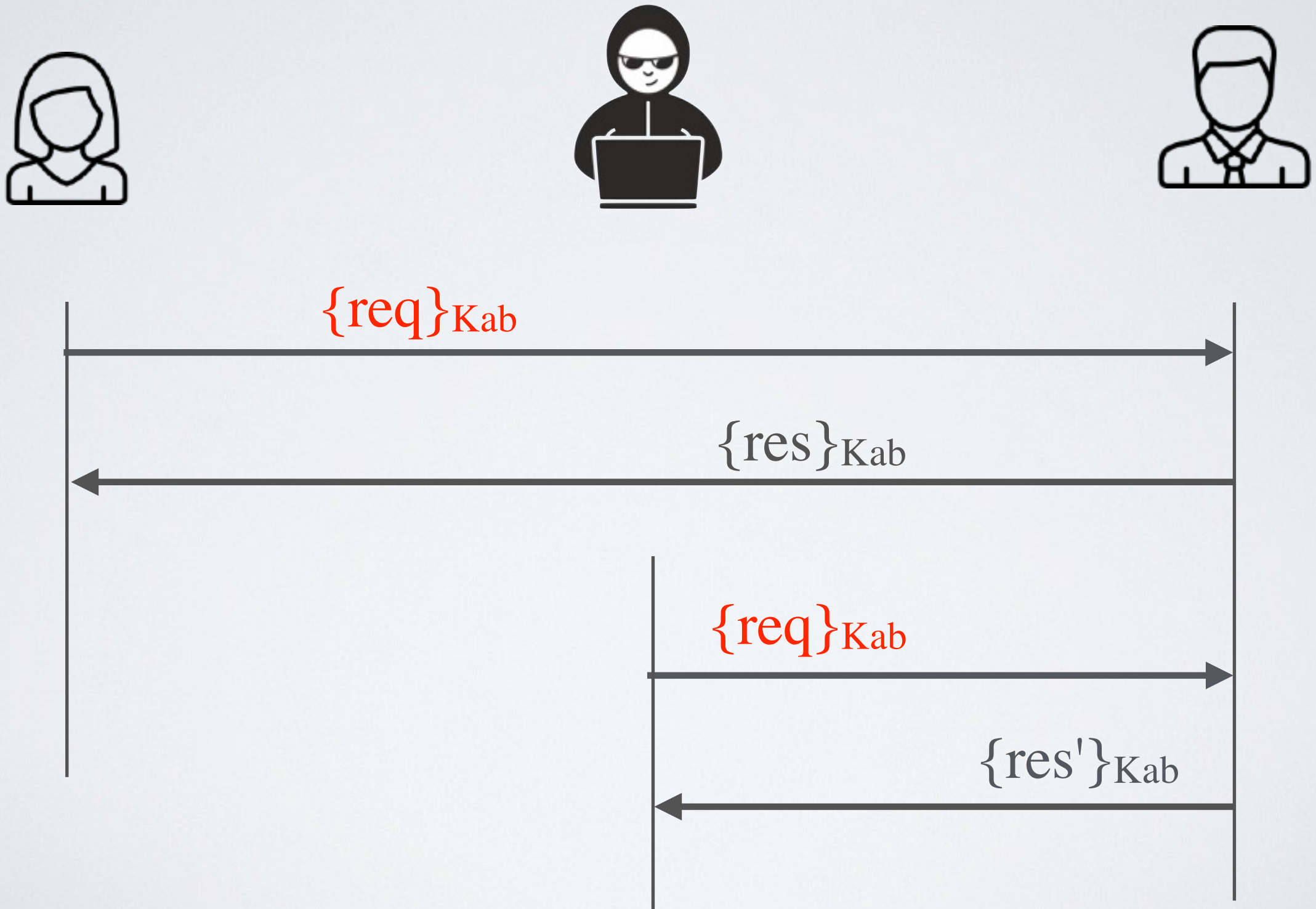
$\{\text{req}\}_{K_{ab}}$

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



$\{res\}Kab$

Replay attack



Counter replay attacks

Several solutions:

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