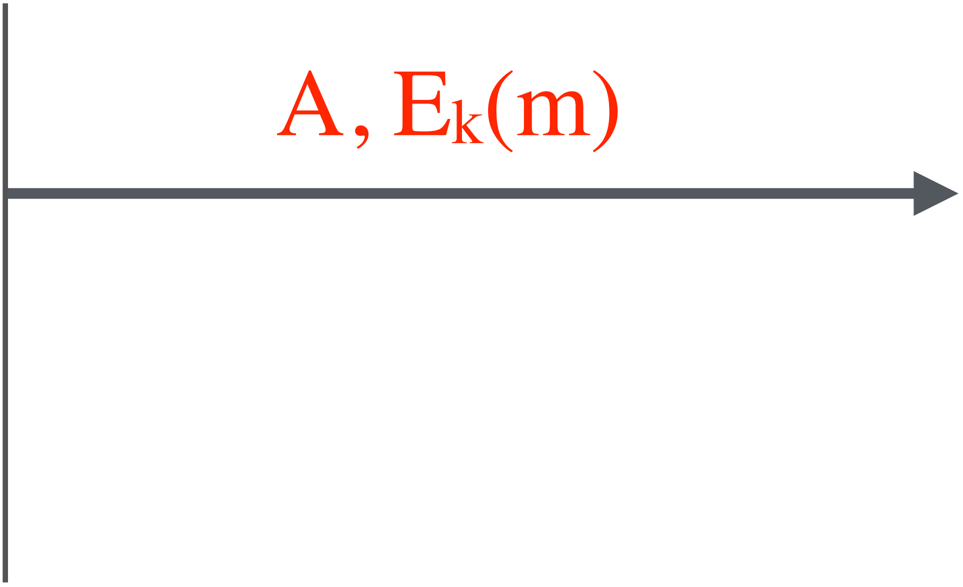
Problem : replay attack

$A, E_k(m)$

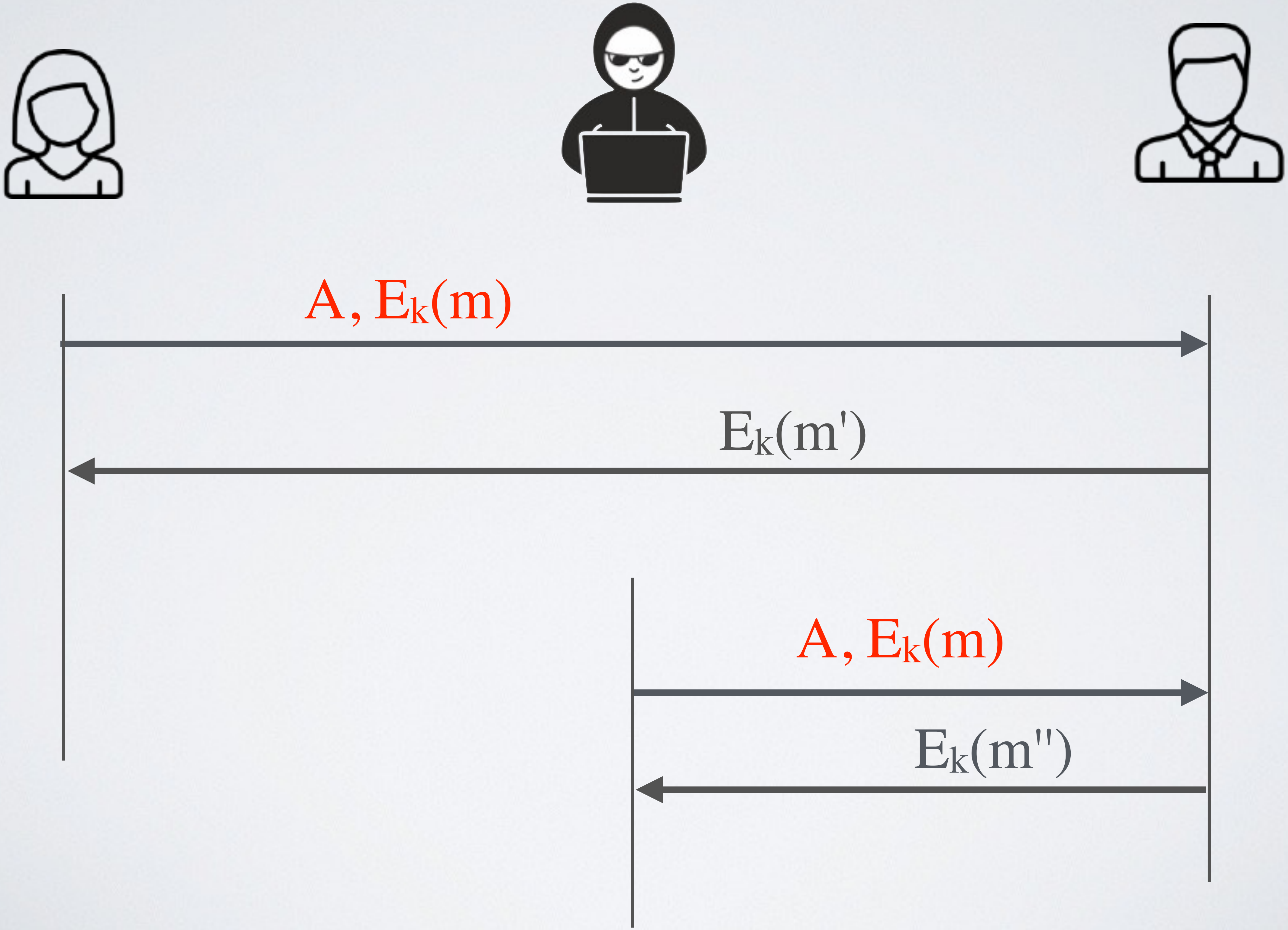


$A, E_k(m)$

$$\xleftarrow{E_k(m'')}$$

$$E_k(m')$$

Problem : replay attack



$A, E_k(m)$

$E_k(m')$

$A, E_k(m)$

$E_k(m'')$

Counter replay attacks

- ✓ **Storage-based solution**
  Store the message entirely (log), or ID or encryption nonce and check whether the same message has been replayed
- ◉ Problem: this solution can be expensive
- ✓ **Protocol-based solution**
  Add a nonce in the interaction and verify that the nonce is sent back
- ➡ The nonce should be random enough that is does not repeat itself over time