

Problem: replay attack













A, $E_k(n)$



$A, E_k(m)$

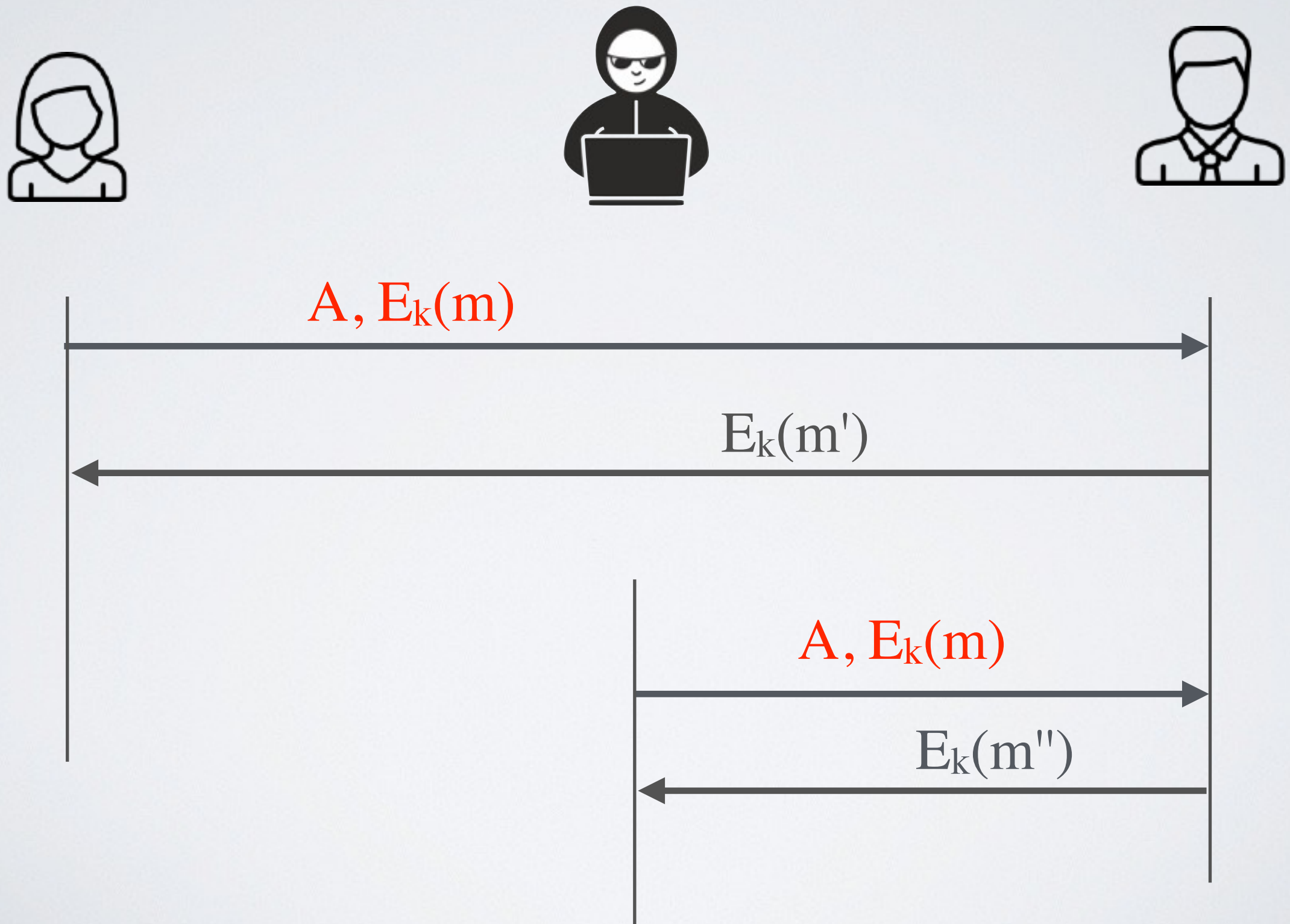
A diagram consisting of a horizontal axis with a dark gray arrow pointing to the right, and a vertical line segment on the left. The text $A, E_k(m)$ is written in red above the horizontal axis.

$E_k(m')$



$E_k(n')$

Problem : replay attack



Counter replay attacks

- ✓ **Storage-based solution**

Store the message entirely (log), or ID or encryption nonce or timestamp and check whether the same message has been replayed

- ✓ **Protocol-based solution**

Add a nonce in the interaction and verify that the nonce is sent back