



Problem: replay attack















A,  $E_k(n)$



$A, E_k(m)$

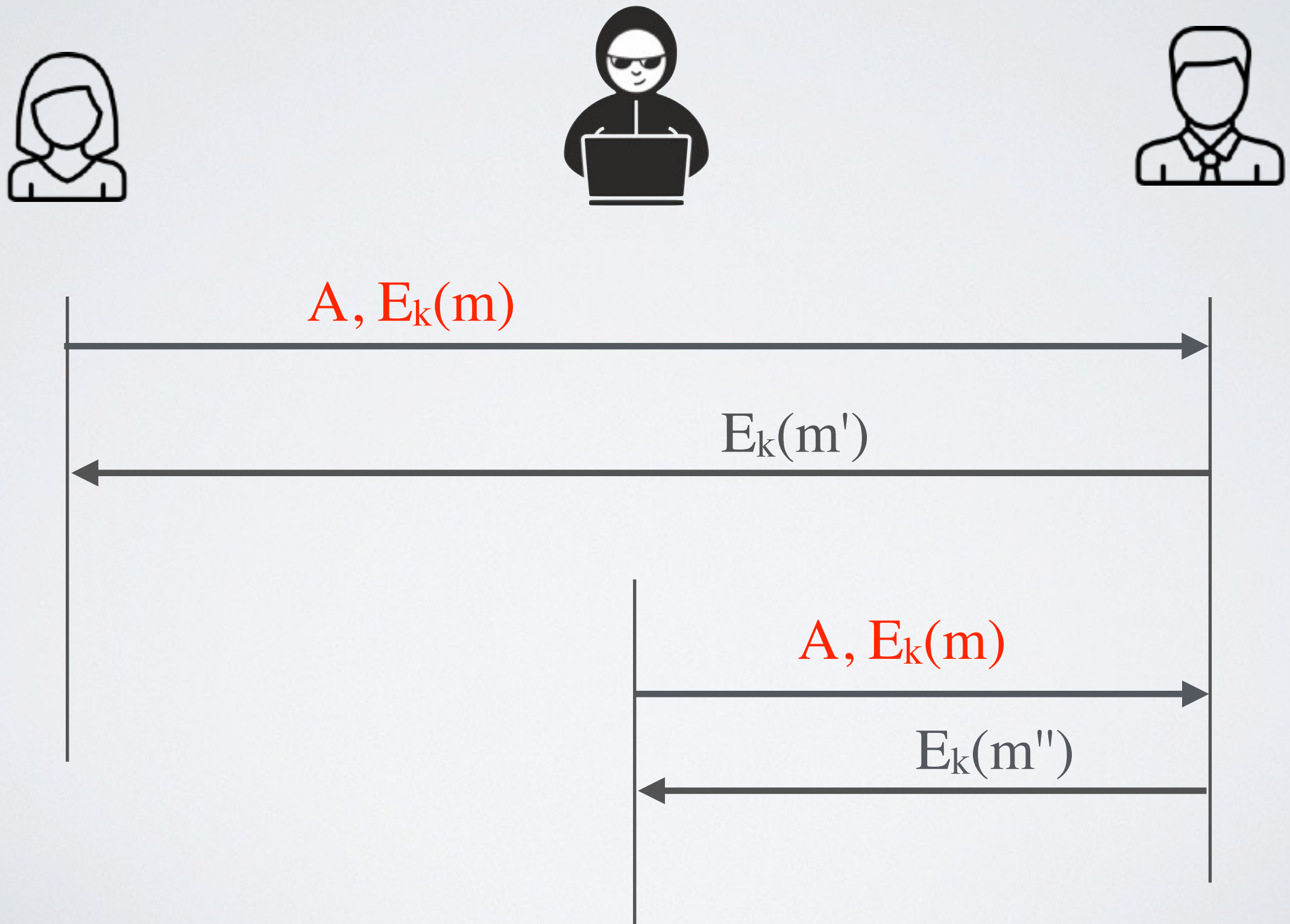
A diagram consisting of a horizontal axis with a dark gray arrow pointing to the right. A vertical line segment is positioned on the left side of the horizontal axis. The text  $A, E_k(m)$  is written in red above the horizontal axis.

$E_k(m')$



$E_k(n')$

# Problem : replay attack



# Counter replay attacks

## ✓ **Storage-based solution**

Store the message entirely (log), or ID or encryption nonce 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 it does not repeat itself over time