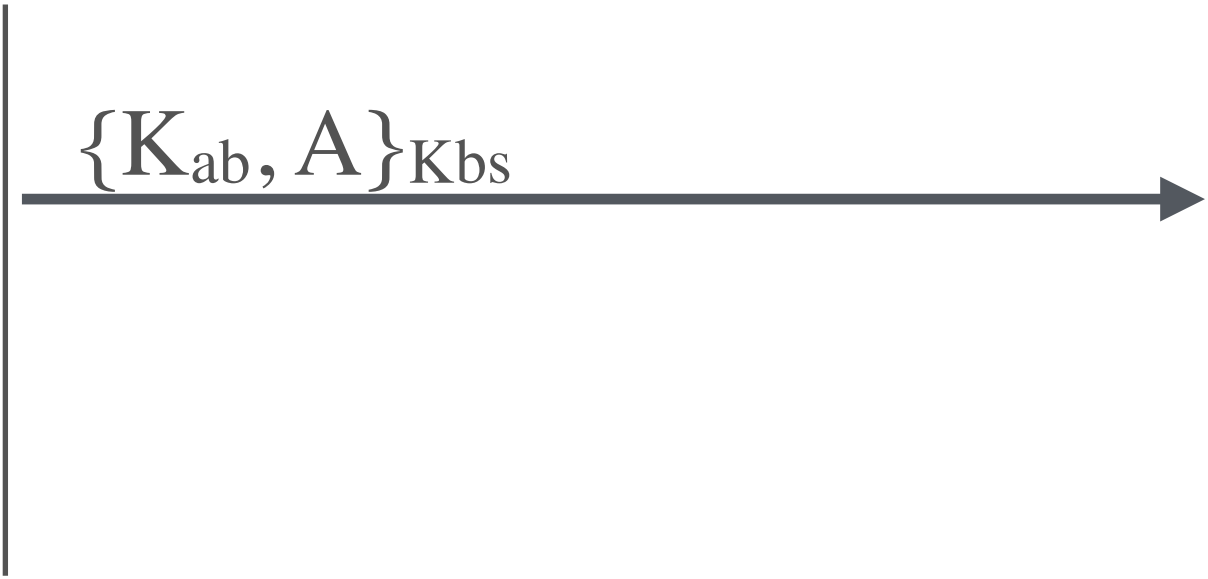
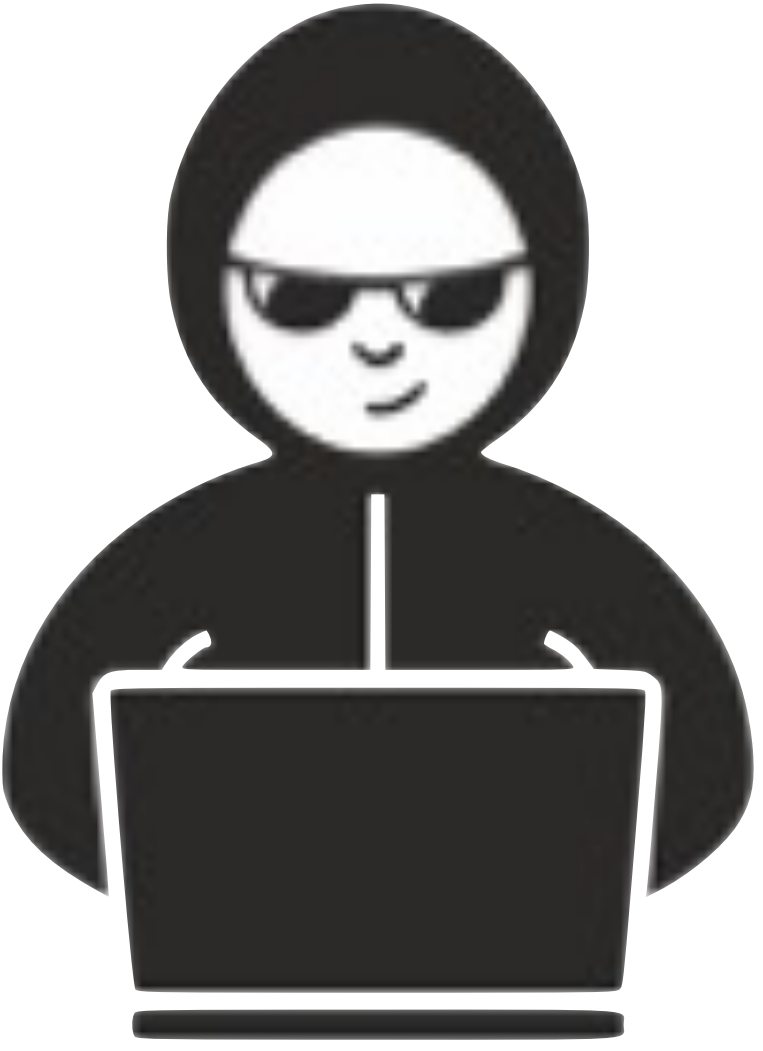
Replay attack (1981)


$\{K_{ab}, A\}_{Kbs}$

{N_B}Kab

{NB-1}Kab



Assuming $\mathbf{K_{ab}}$ has been compromised somehow, it can be reused

Replay attack (1981)

Assuming K_{ab} has been compromised somehow, it can be reused

$\{K_{ab}, A\}_{Kbs}$

$\{N_B\}_{Kab}$

$\{N_B\text{-}1\}_{Kab}$

The fix (1987)