

Reply attack (1981)











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



$\{N_B\} Kab$

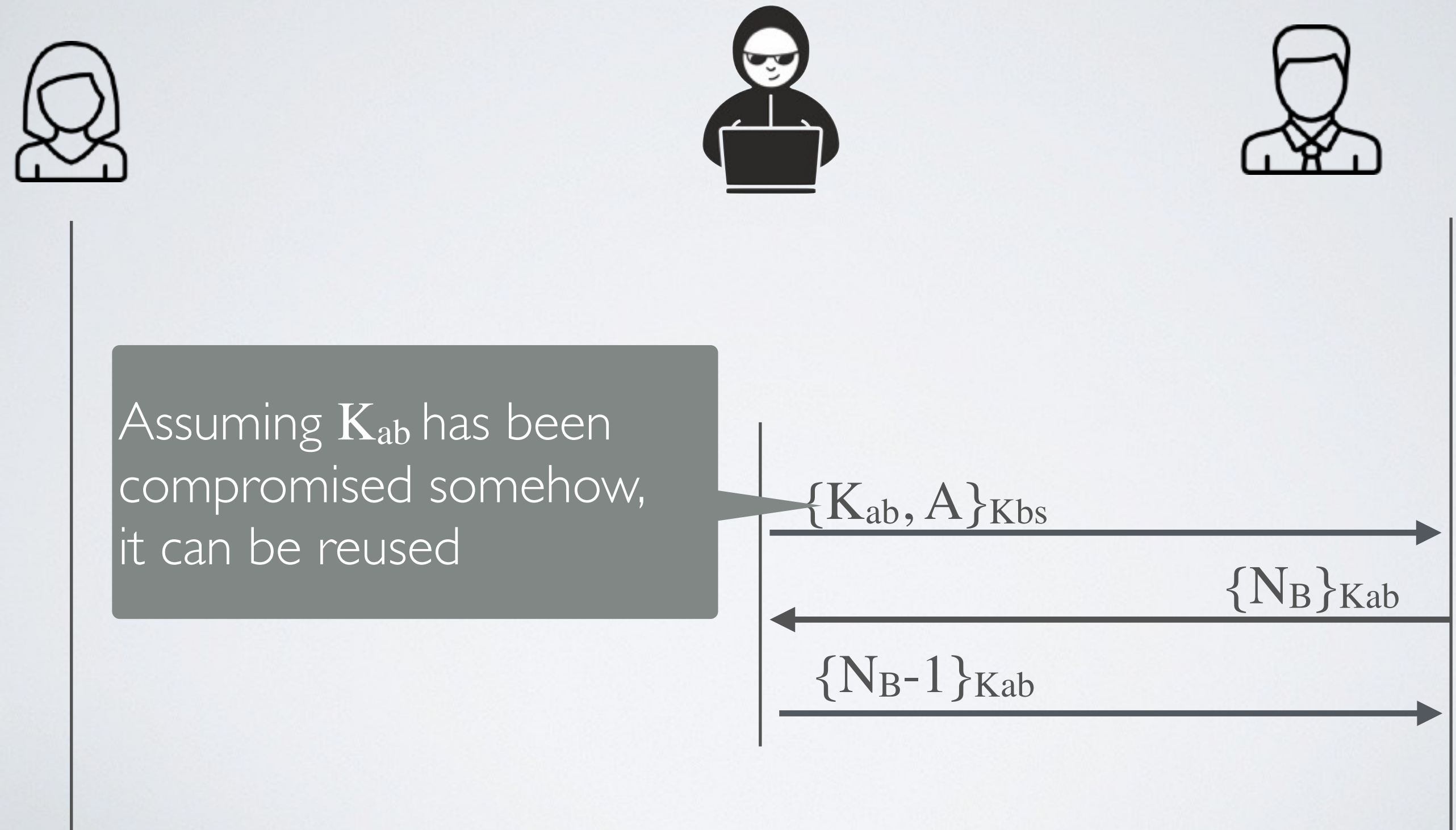
$\{N_B-1\}K_{ab}$





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

Replay attack (1981)



The fix (1987)

