# The vulnerable version of the protocol (1978)

A, B, NA

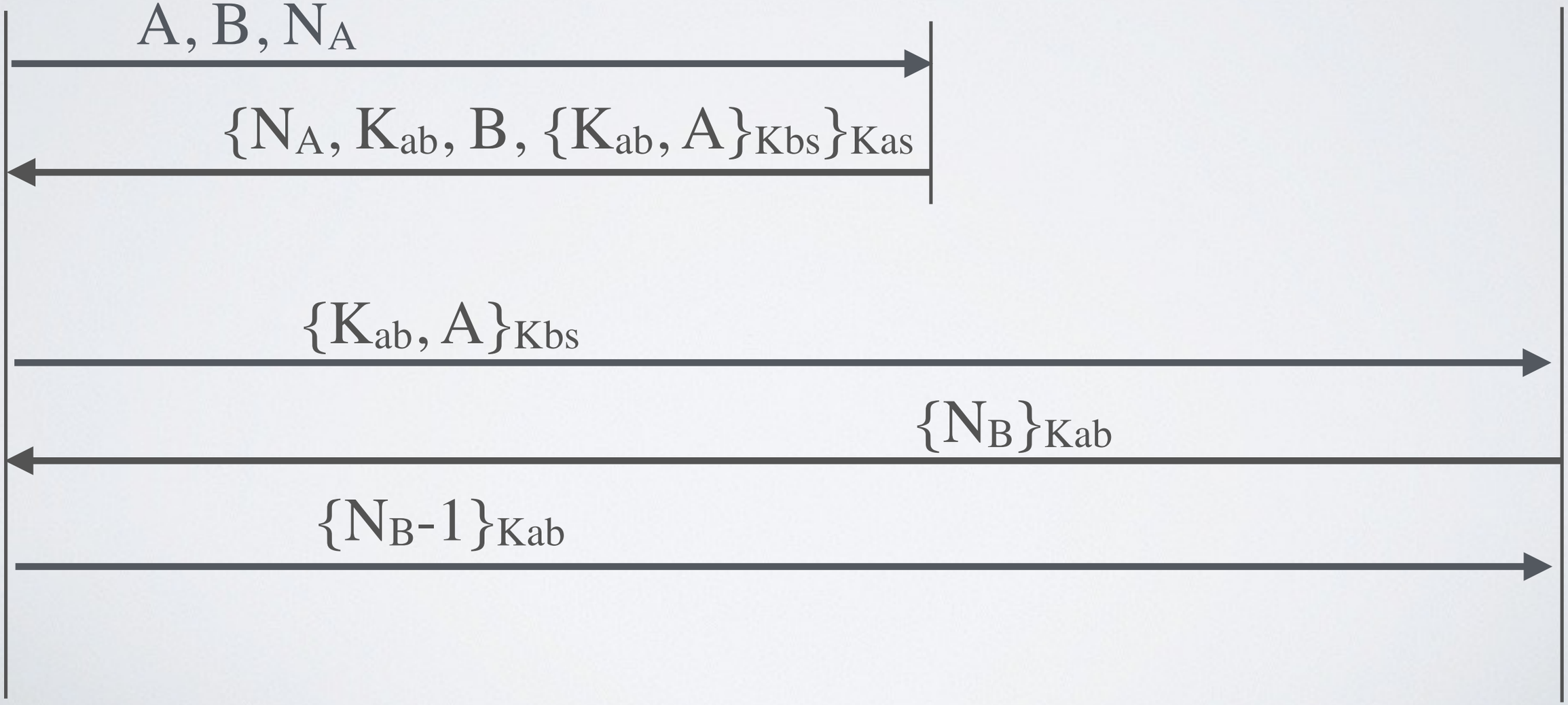
$\{N_A, K_{ab}, B, \{K_{ab}, A\}_{Kbs}\}_{Kas}$

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

$\{N_B\}_{Kab}$


{NB-1}Kab

# The vulnerable version of the protocol (1978)



# Replay attack (1981)

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