The fix (1987)

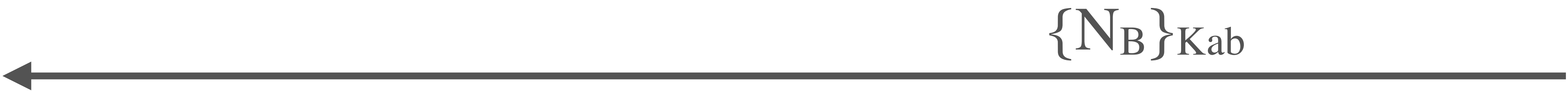
$$\xrightarrow{A, B, N_A, \{A, N_{B'}\}_{Kbs}}$$

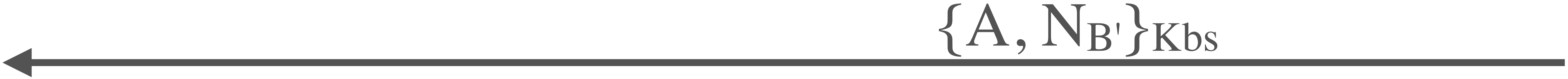
$$\xleftarrow{\{N_A, K_{ab}, B, \{K_{ab}, A, N_{B'}\}_{Kbs}\}_{Kas}}$$

$$\xrightarrow{\{K_{ab}, A, N_{B'}\}_{Kbs}}$$

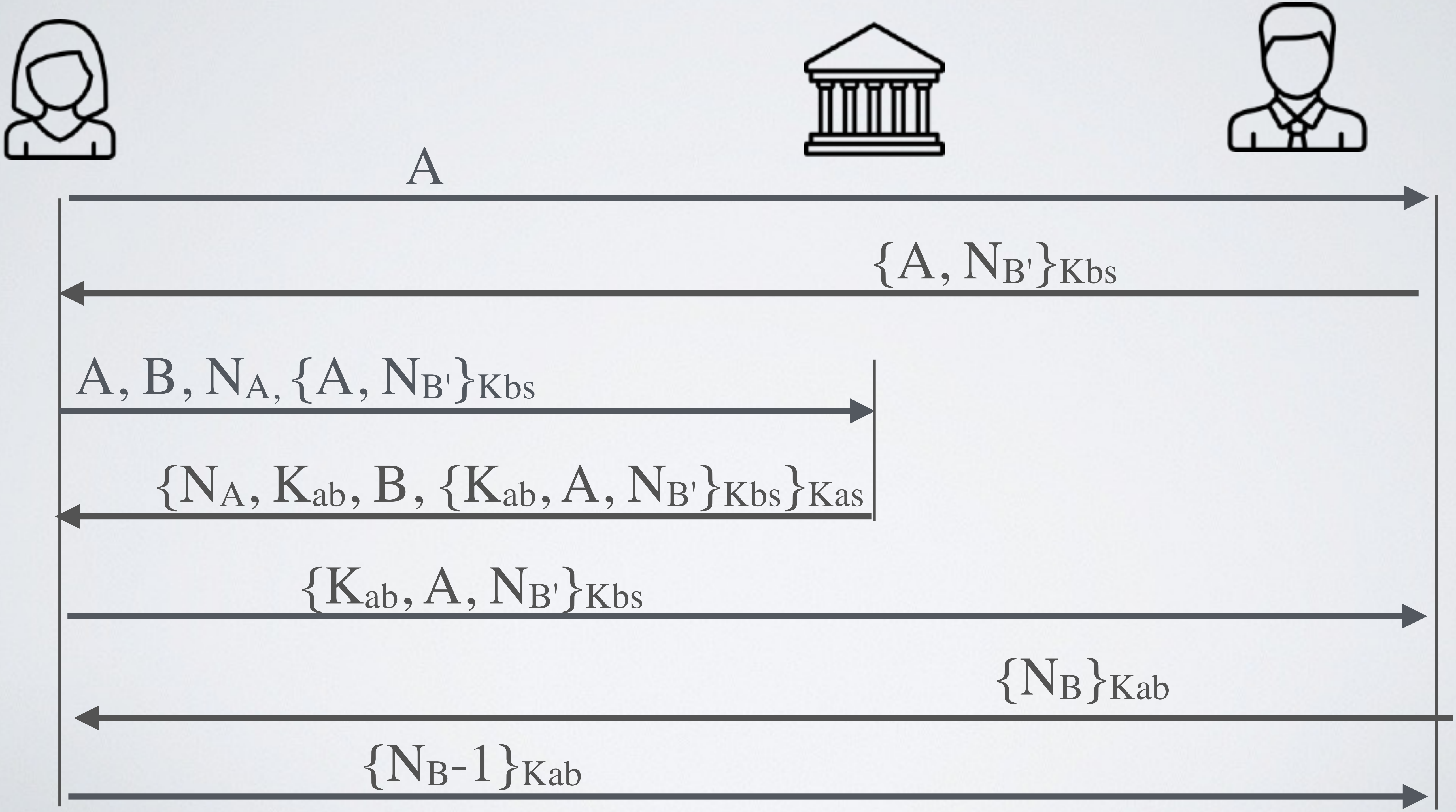
$$\xrightarrow{\{N_B-1\}_{Kab}}$$

A


$\{N_B\}_{Kab}$


$\{A, N_{B'}\}_{Kbs}$

The fix (1987)



A

$\{A, N_{B'}\}_{Kbs}$

$A, B, N_{A,} \{A, N_{B'}\}_{Kbs}$

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

$\{K_{ab}, A, N_{B'}\}_{Kbs}$

$\{N_B\}_{Kab}$

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

Kerberos

The Needham-Shroeder symmetric protocol is the basis for **the Kerberos Protocol**

➡ Use by Microsoft Windows for key exchange between machines on the same domain manage by the Active Directory