The fix (1987)

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


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


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

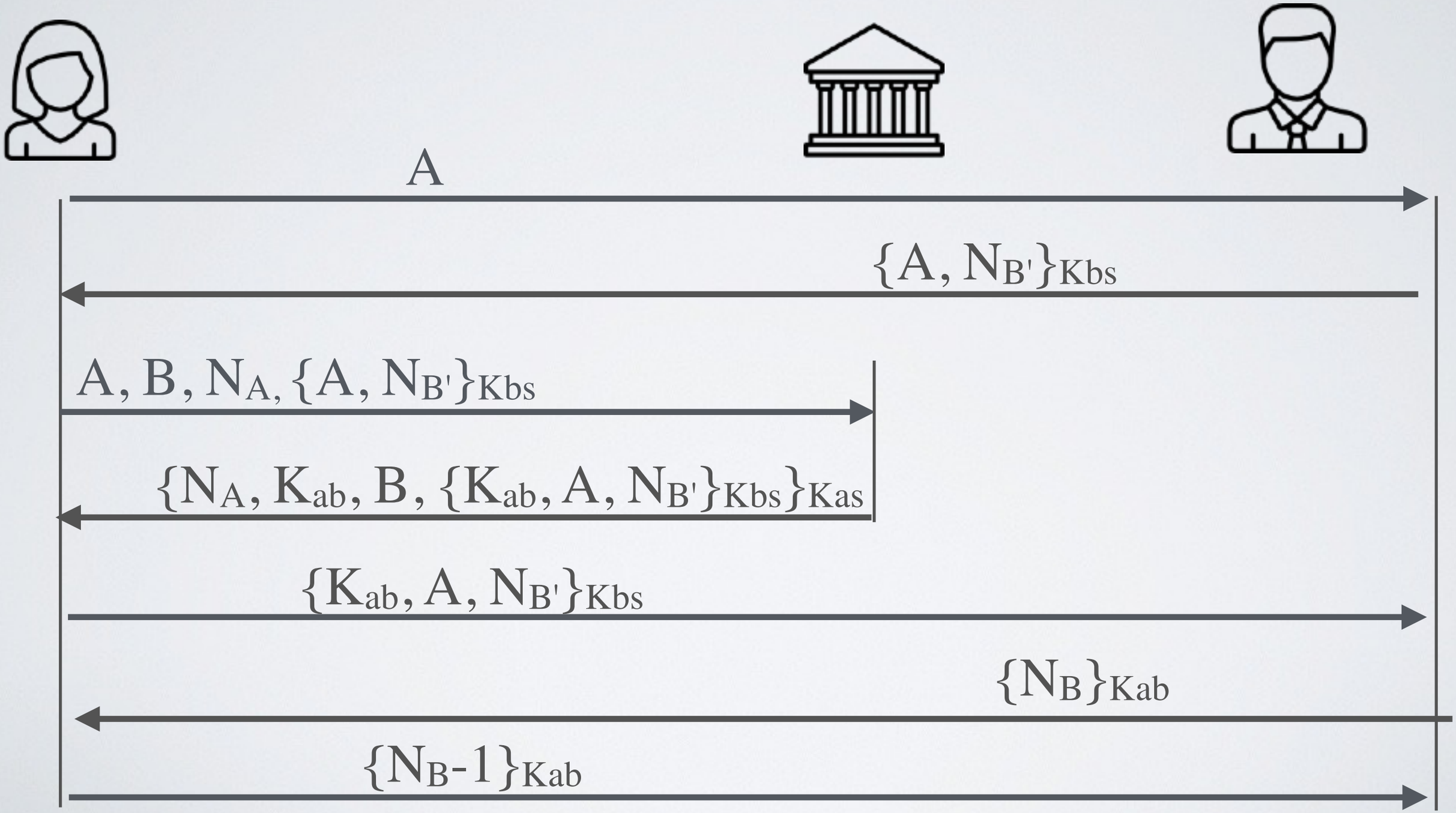
$\{N_B\text{-}1\}_{Kab}$

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-1}Kab

Limitations of using a key distribution centre

The key distribution server is a bootleneck and **weak link**

- The attacker could record the key exchange and the encrypted session, if one day either $\mathbf{Kas}$ or $\mathbf{Kbs}$ is broken, the attacker can decrypt the session

➡ Having a KDC does not offer "Perfect Forward Secrecy"