The fix (1987)

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

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

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

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

$$\longrightarrow$$

A

$$\longleftarrow \{N_B\}Kab$$

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

The fix (1987)

A

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

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

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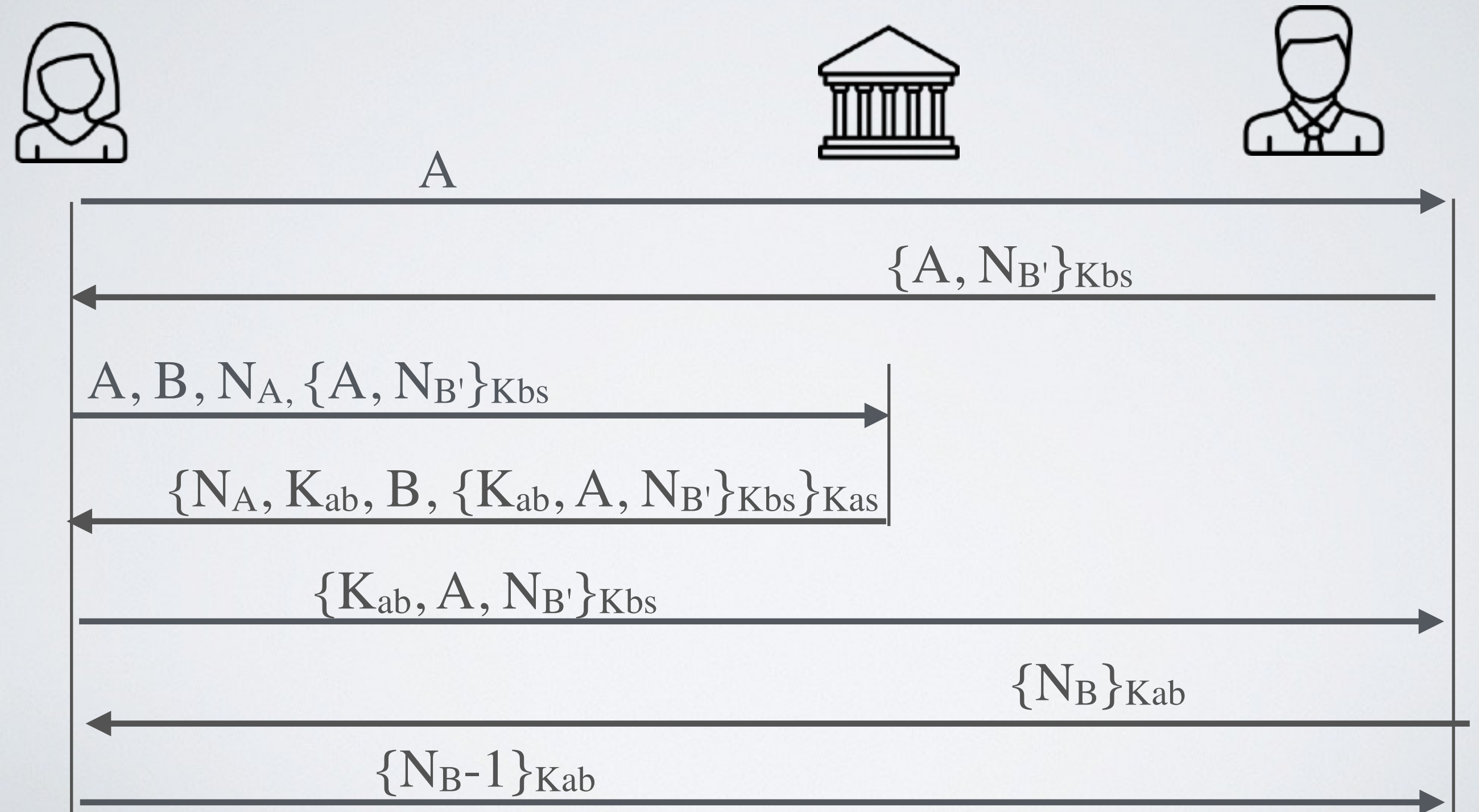
$\{K_{ab}, A, N_{B'}\}_{Kbs}$

$\{N_B\}_{Kab}$

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

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 **Kas** or **Kbs** is broken, the attacker can decrypt the session

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