

The fix (1987)









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





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





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


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

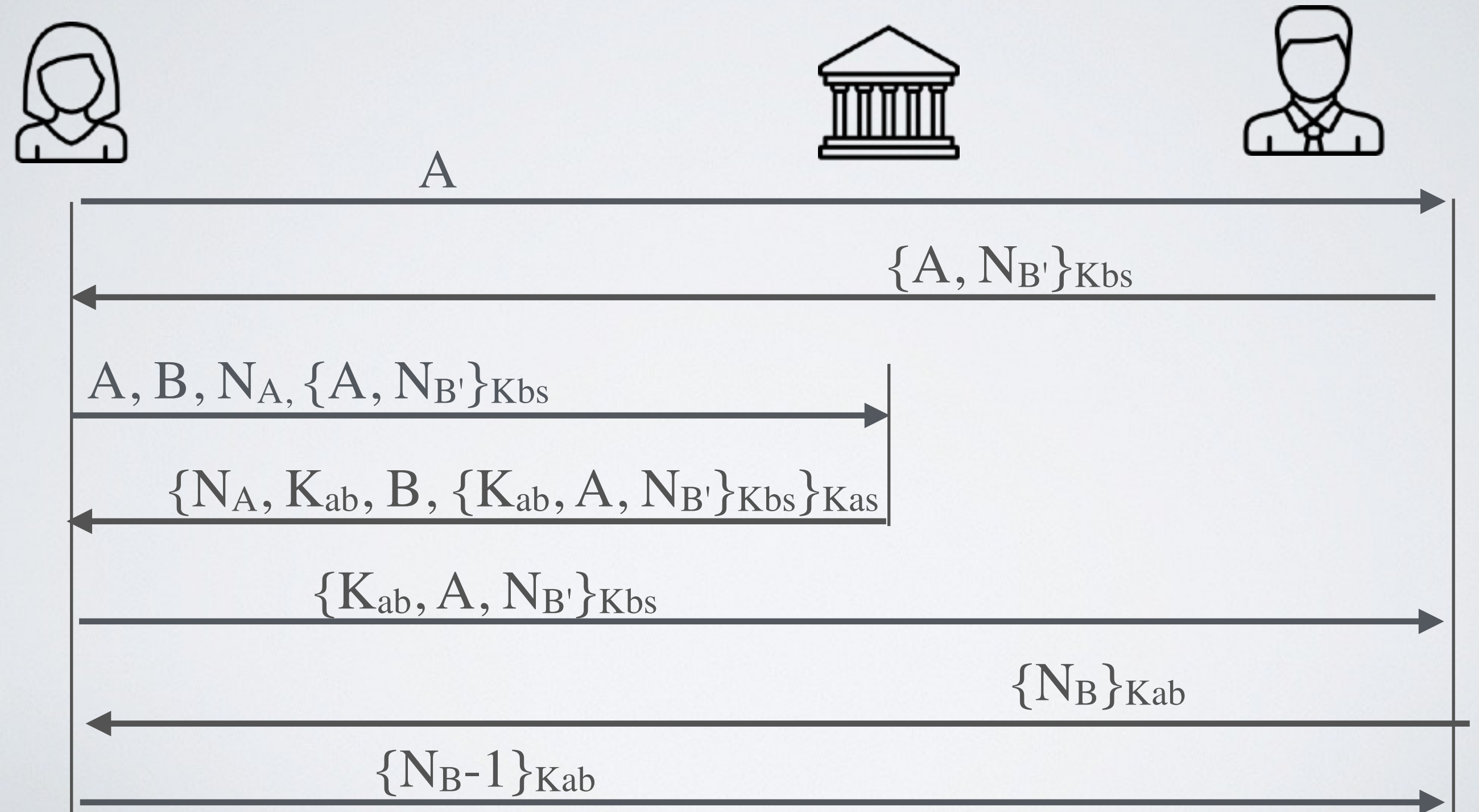
A




$$\{N_B\}_{K_{ab}}$$



The fix (1987)



Limitations of using a key distribution centre

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

- The attacker could record the key exchange and the encrypted session, if one day either **K_{as}** or **K_{bs}** is broken, the attacker can decrypt the session
- ➔ Having a KDC does not offer "Perfect Forward Secrecy"