

The vulnerable version of the protocol (1978)









A, B, N_A



$$\{N_A, K_{ab}, B, \{K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$$







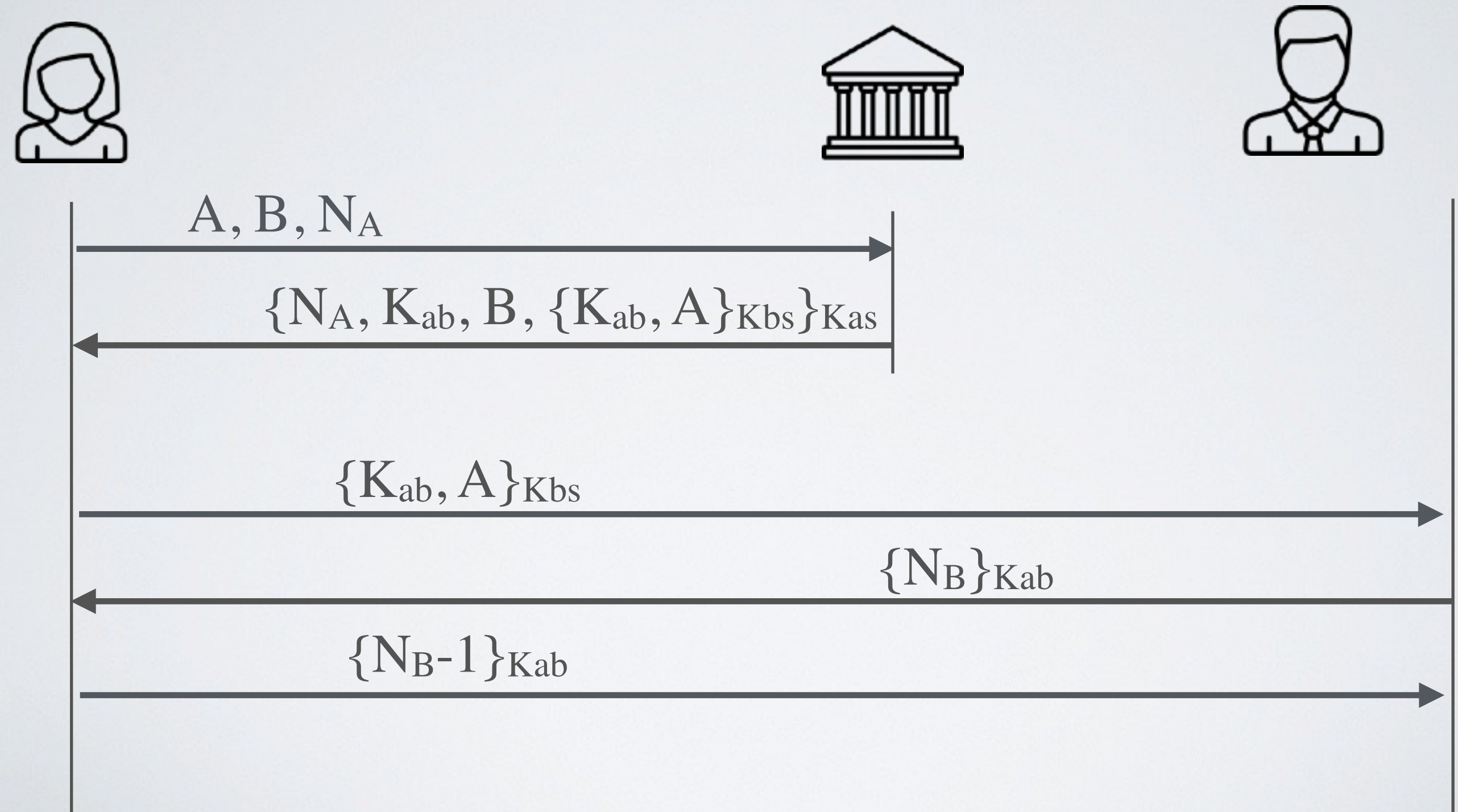
$$\{K_{ab}, A\}_{Kbs}$$




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

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


The vulnerable version of the protocol (1978)



Replay attack (1981)



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