The vulnerable version (1978)

A, B

{Kpb, B}Kss


$\{N_A, A\}_{Kpb}$

$\{N_A, N_B\}_{Kpa}$

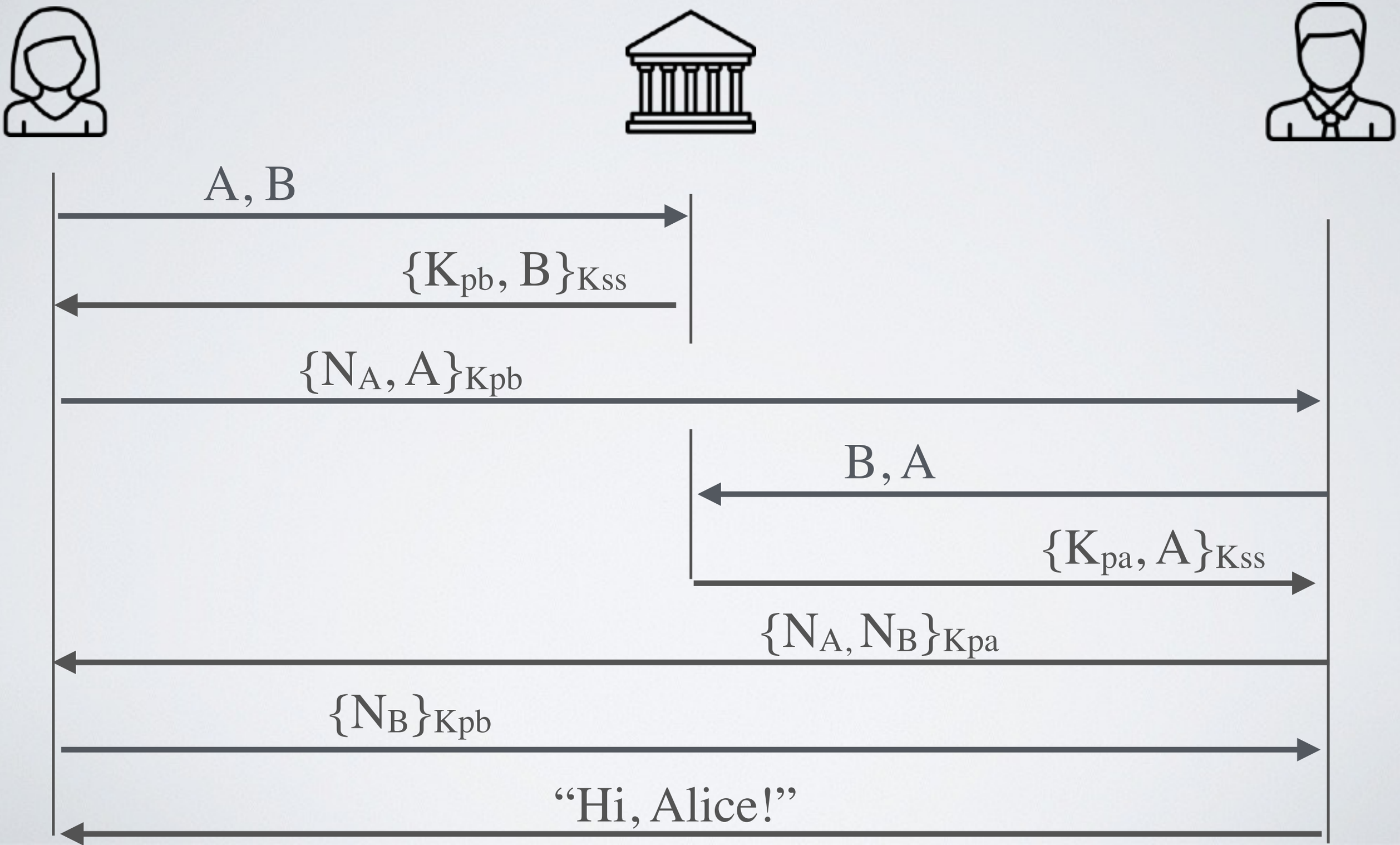

$\{N_B\}_{Kpb}$


B, A

{Kpa, A}Kss

“Hi, Alice!”

The vulnerable version (1978)



Simplified (but still vulnerable) version (1978)