Simplified (but still vulnerable) version (1978)

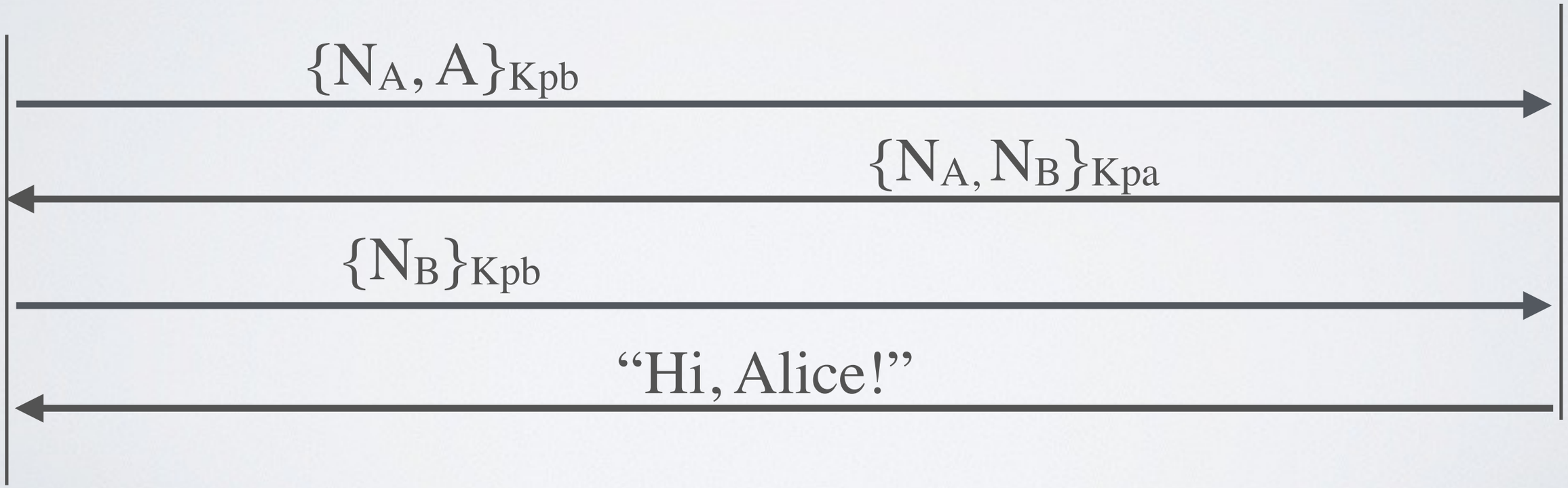

$\{N_A, A\}_{Kpb}$

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


$\{N_B\}_{Kpb}$

“Hi, Alice!”

Simplified (but still vulnerable) version (1978)



Man-in-the-middle attack (Lowe's 1995)