

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







$\{N_A, A\} K_{pm}$

“Hi, Alice!”




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









$\{N_A, A\}_{K_{pb}}$



$\{N_B\}_{K_{pb}}$

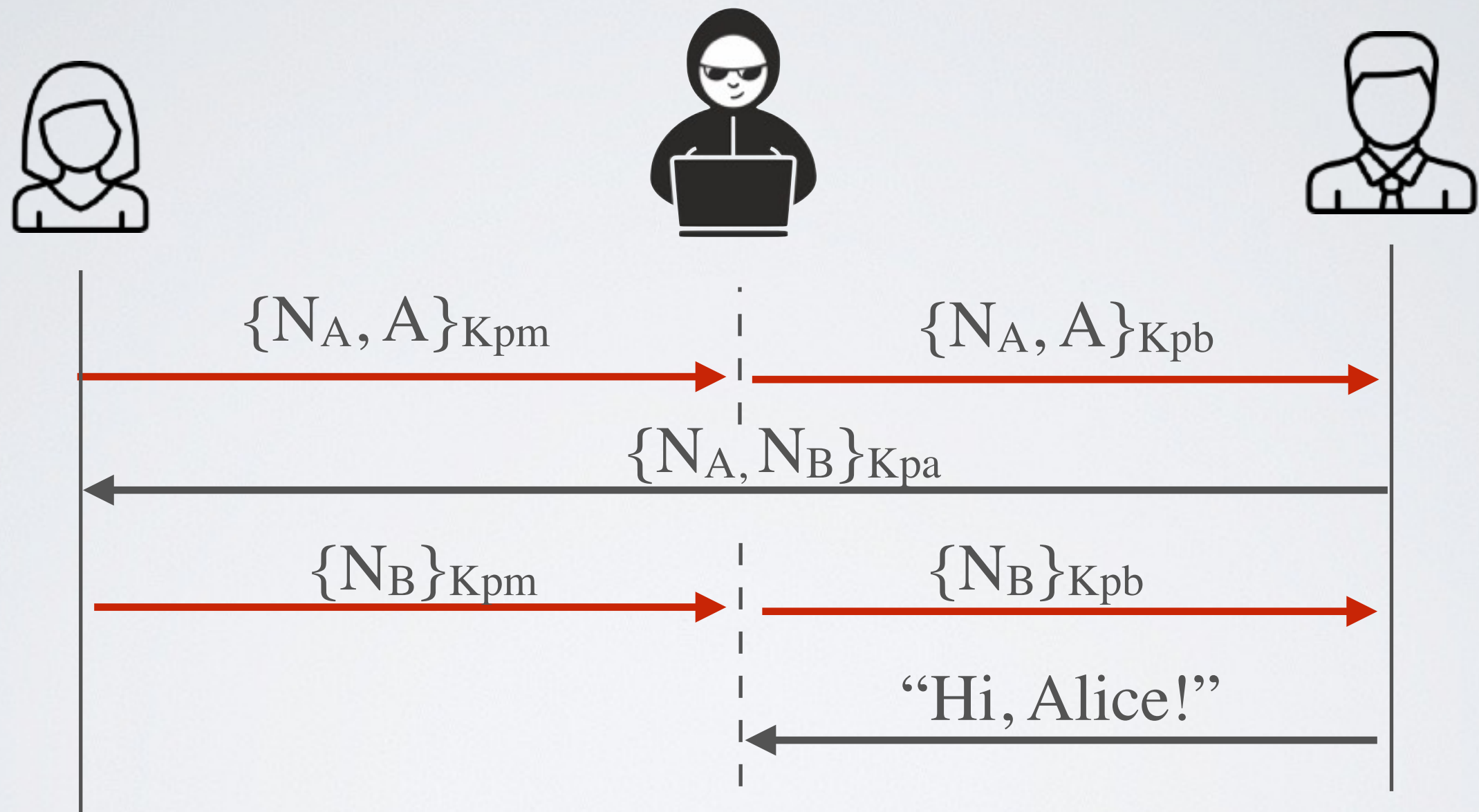


$\{N_B\}_{K_{pm}}$





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



Lowe's fix (1995)

