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


{NA, A}Kpm


“Hi, Alice!”

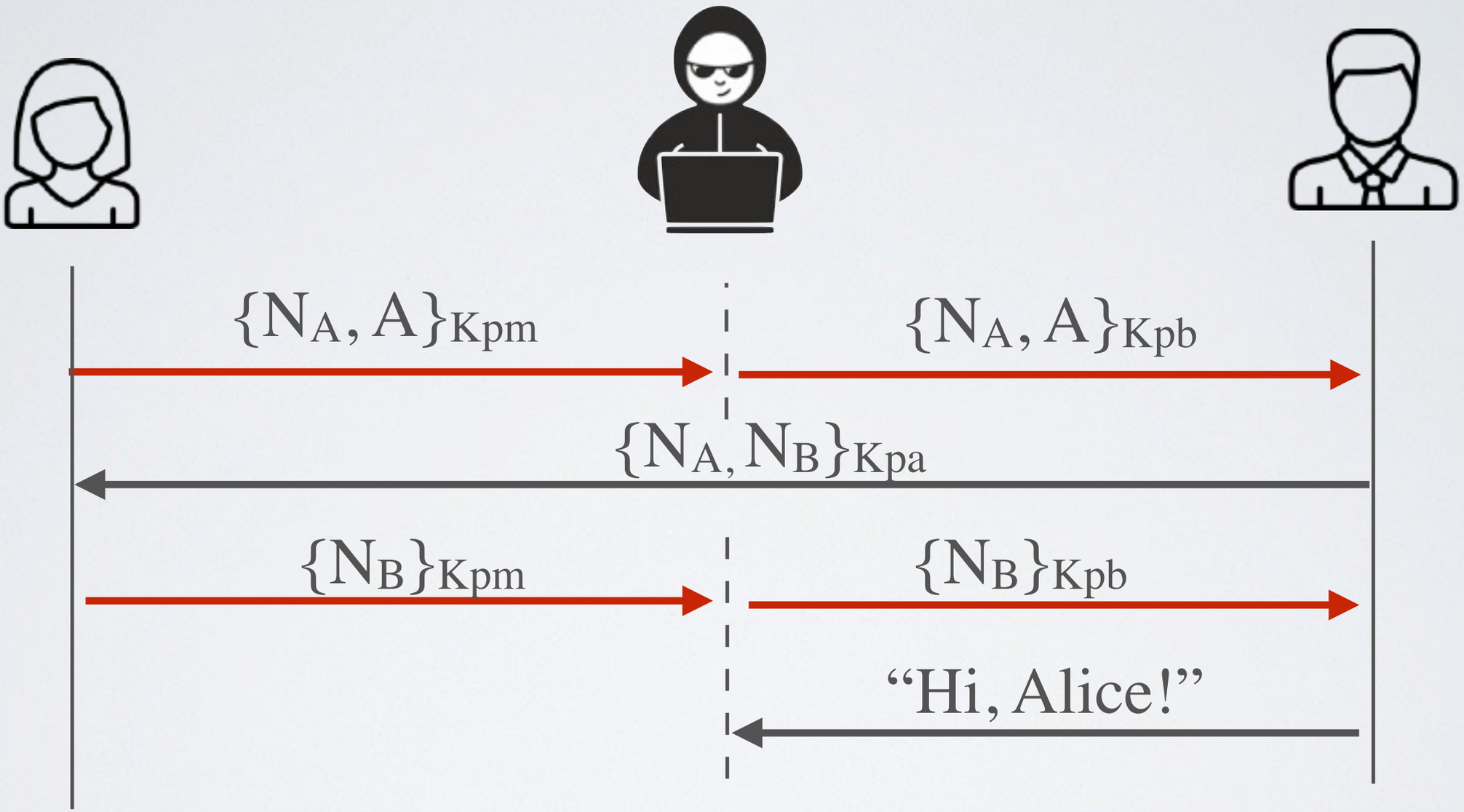
$\{N_A, N_B\}_{Kpa}$


{NA, A}Kpb


{N_B}Kpb


{N_B}_Kpm

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



Lowe's fix (1995)