

The vulnerable version (1978)









A, B



$$\{K_{pb}, B\}_{Kss}$$







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




$$\{N_A, N_B\} K_{pa}$$

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


B, A

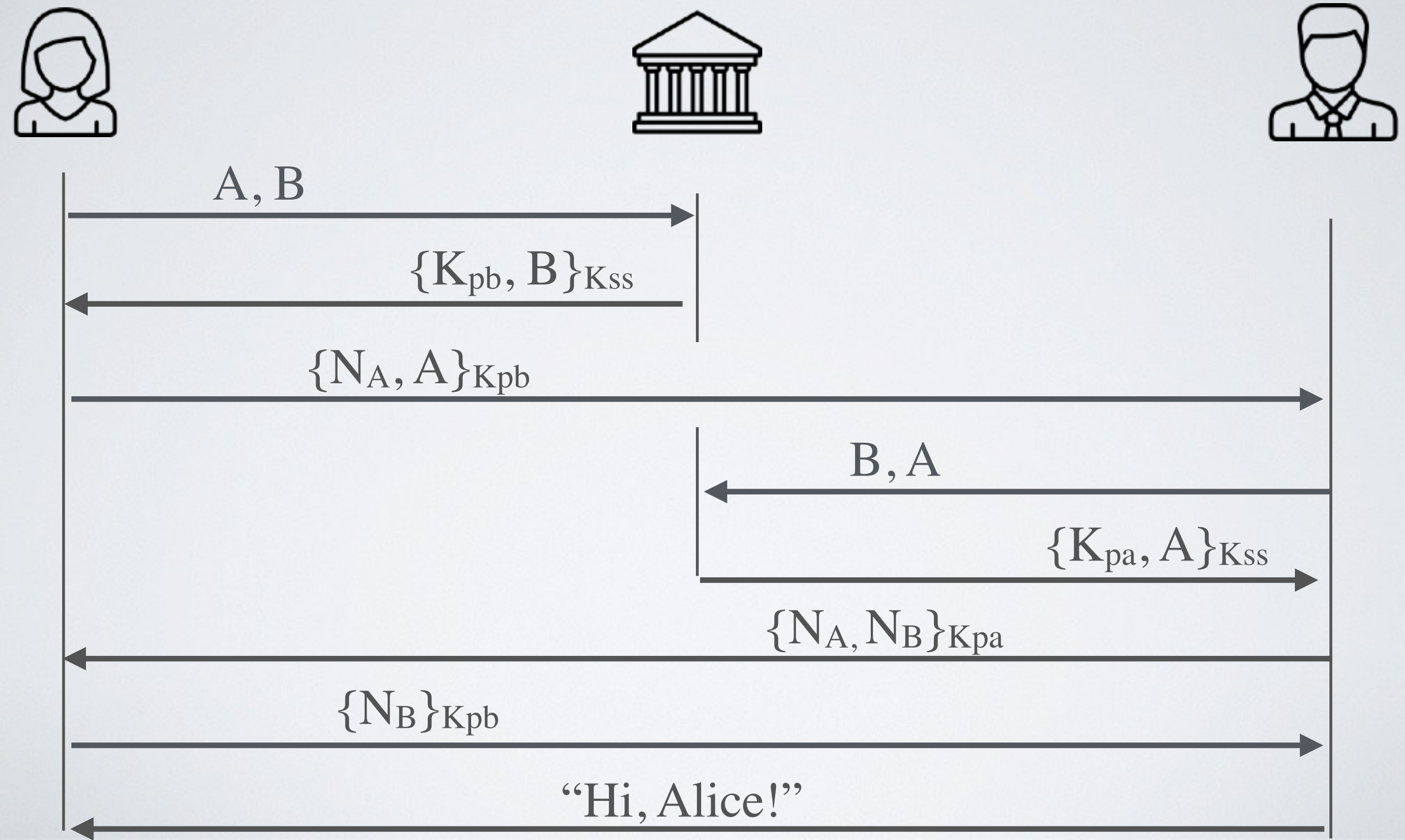


$$\{K_{pa}, A\} K_{ss}$$


“Hi, Alice!”



The vulnerable version (1978)



Simplified (but still vulnerable) version (1978)

