

Lowwe's fix (1995)









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

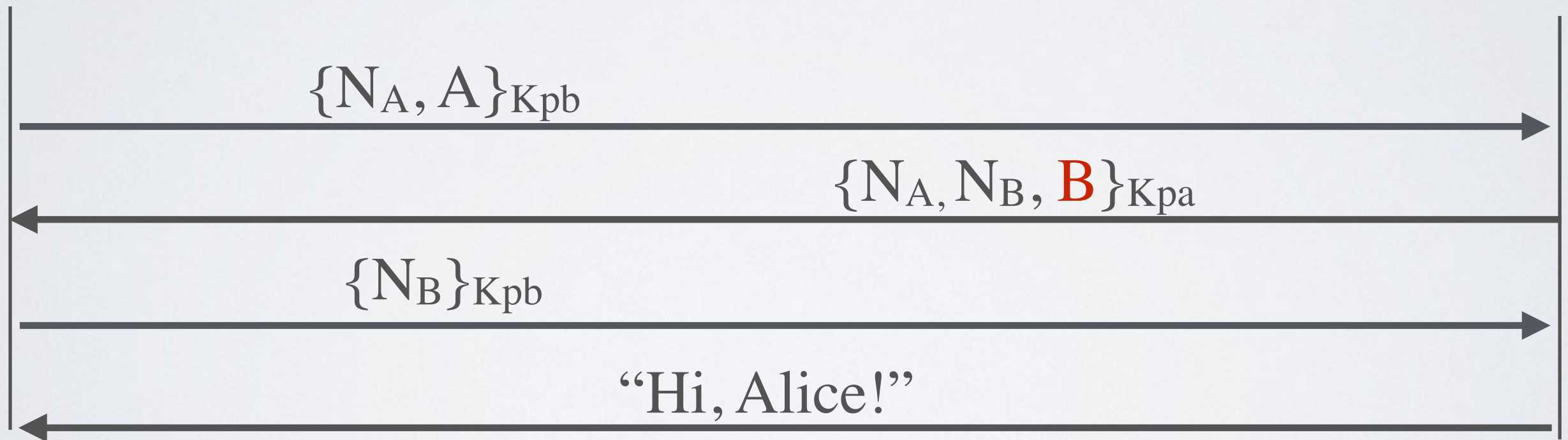



$$\{N_B\}_{K_{pb}}$$


“Hi, Alice!”



Lowe's fix (1995)



Not a perfect protocol yet

- ✓ Does authenticate Alice and bob
- ✓ Does prevent replay attacks
- ✓ Does ensure the authenticity of the public keys
- ⦿ But the Public Key Server is a single point of failure