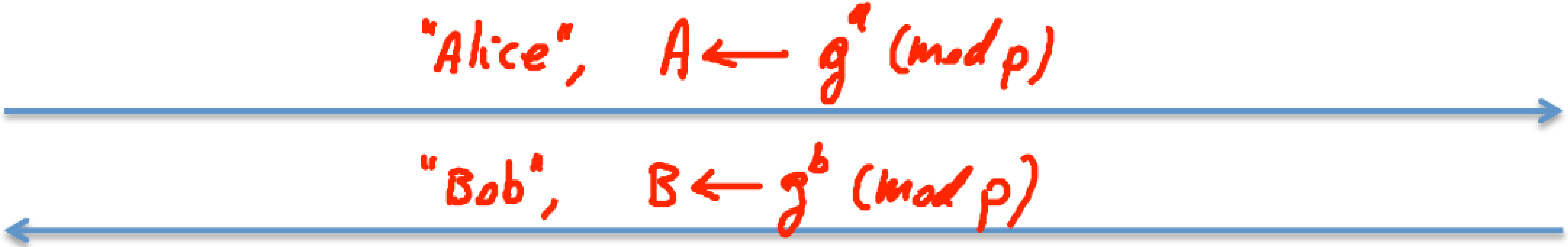
Alice **Bob**

choose random **a** in {1,…,p-1} choose random **b** in {1,…,p-1}



"Alice", $A \leftarrow g^a \pmod{p}$

"Bob", $B \leftarrow g^b \pmod{p}$

$$\mathbf{B^a} \pmod{p} = (g^b)^a = \mathbf{k_{AB} = g^{ab}} \pmod{p} = (g^a)^b = \mathbf{A^b} \pmod{p}$$