Alice

1. *Elegir* $a = k_{pr,A} \in 2, \ldots, p-2\}$
2. *Calcular* $A = k_{pub,A} \equiv \alpha^a \mod p$

Bob

1. *Elegir* $b = k_{pr,B} \in 2, \ldots, p-2\}$
2. *Calcular* $B = k_{pub,B} \equiv \alpha^b \mod p$

$$\xleftarrow{\quad k_{pub,A} = A \quad}$$

$$\xrightarrow{\quad k_{pub,B} = B \quad}$$

$$k_{AB} = k_{k_{pub,B}}^{k_{pr,A}} = B^a \mod p$$

$$k_{AB} = k_{k_{pub,A}}^{k_{pr,B}} = A^b \mod p$$