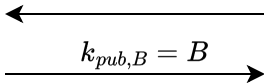


Alice

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

$$k_{pub,A} = A$$



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

Bob

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

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