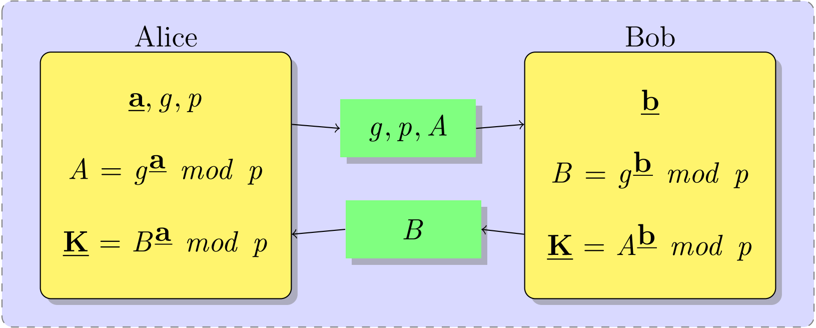

Alice
$\underline{\mathbf{a}}, g, p$
$A = g^{\underline{\mathbf{a}}}\ mod\ p$
$\underline{\mathbf{K}} = B^{\underline{\mathbf{a}}}\ mod\ p$
g, p, A
B
Bob
$\underline{\mathbf{b}}$
$B = g^{\underline{\mathbf{b}}}\ mod\ p$
$\underline{\mathbf{K}} = A^{\underline{\mathbf{b}}}\ mod\ p$