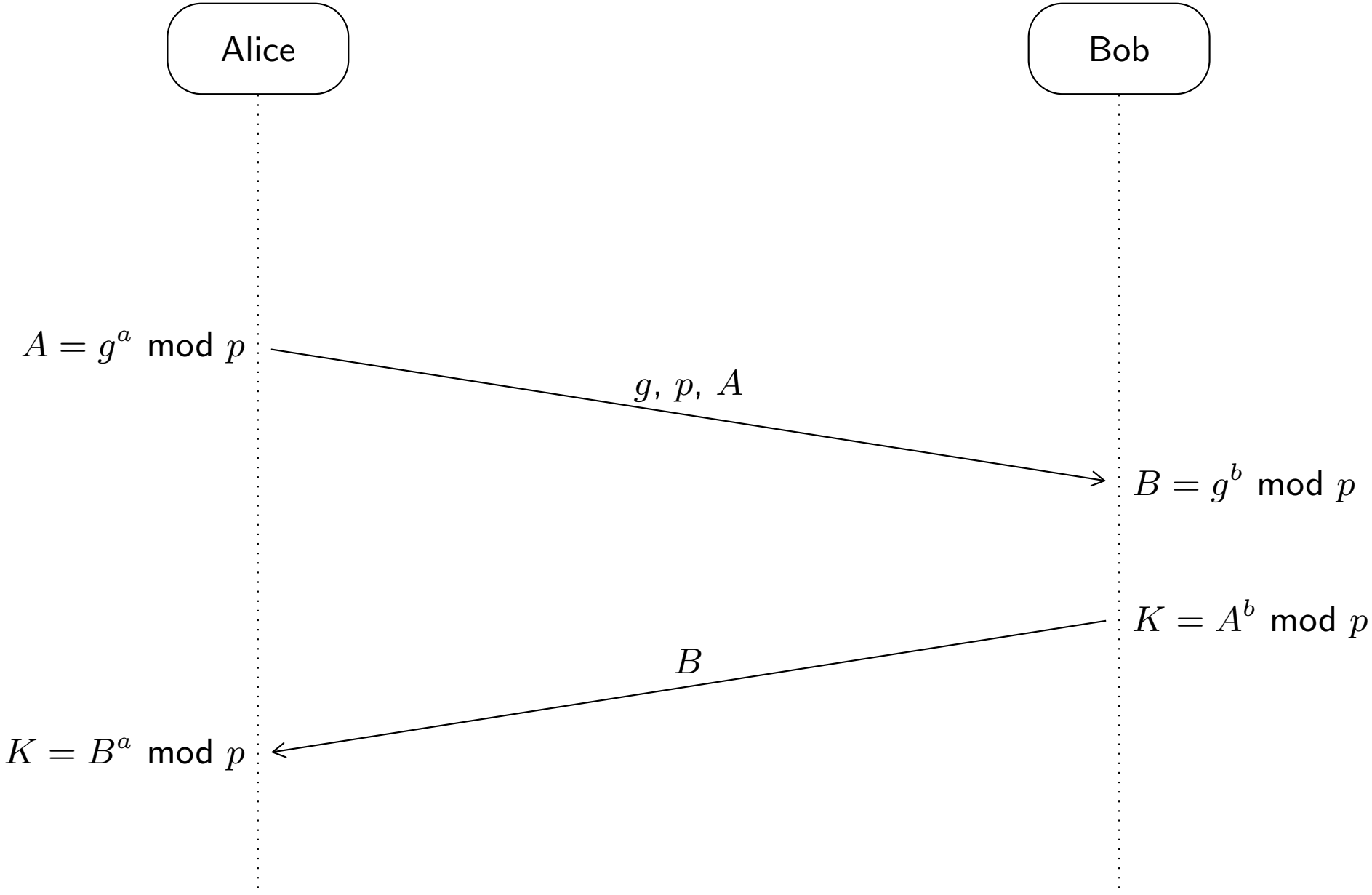
Alice
Bob
$A = g^a \bmod p$
$g,\ p,\ A$
$B = g^b \bmod p$
$K = A^b \bmod p$
B
$K = B^a \bmod p$