آلیس   باب

$x \leftarrow \mathbb{Z}_q$

$h_A := g^x \quad \xrightarrow{\quad \mathbb{G}, q, g, h_A \quad} \quad y \leftarrow \mathbb{Z}_q$

$h_B := g^y$

$k_A := h_B^x \quad \xleftarrow{\quad h_B \quad} \quad k_B := h_A^y$