

Alice

Bob

a, g, p

$$A = g^a \bmod p$$

$$K = B^a \bmod p$$

choose
challenge C_2

share secret $w = h(\text{pwd})$

"Alice", $w(A)$

$w(B, C_1)$

$K(C_1, C_2)$

$K(C_2)$

b

$$B = g^b \bmod p$$

choose
challenge C_1

$$K = A^b \bmod p$$

$$K = A^b \bmod p = (g^a \bmod p)^b \bmod p = g^{ab} \bmod p = (g^b \bmod p)^a \bmod p = B^a \bmod p$$