

Alice

Bob

a, g, p

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

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

g, p, A

b

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

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

B

