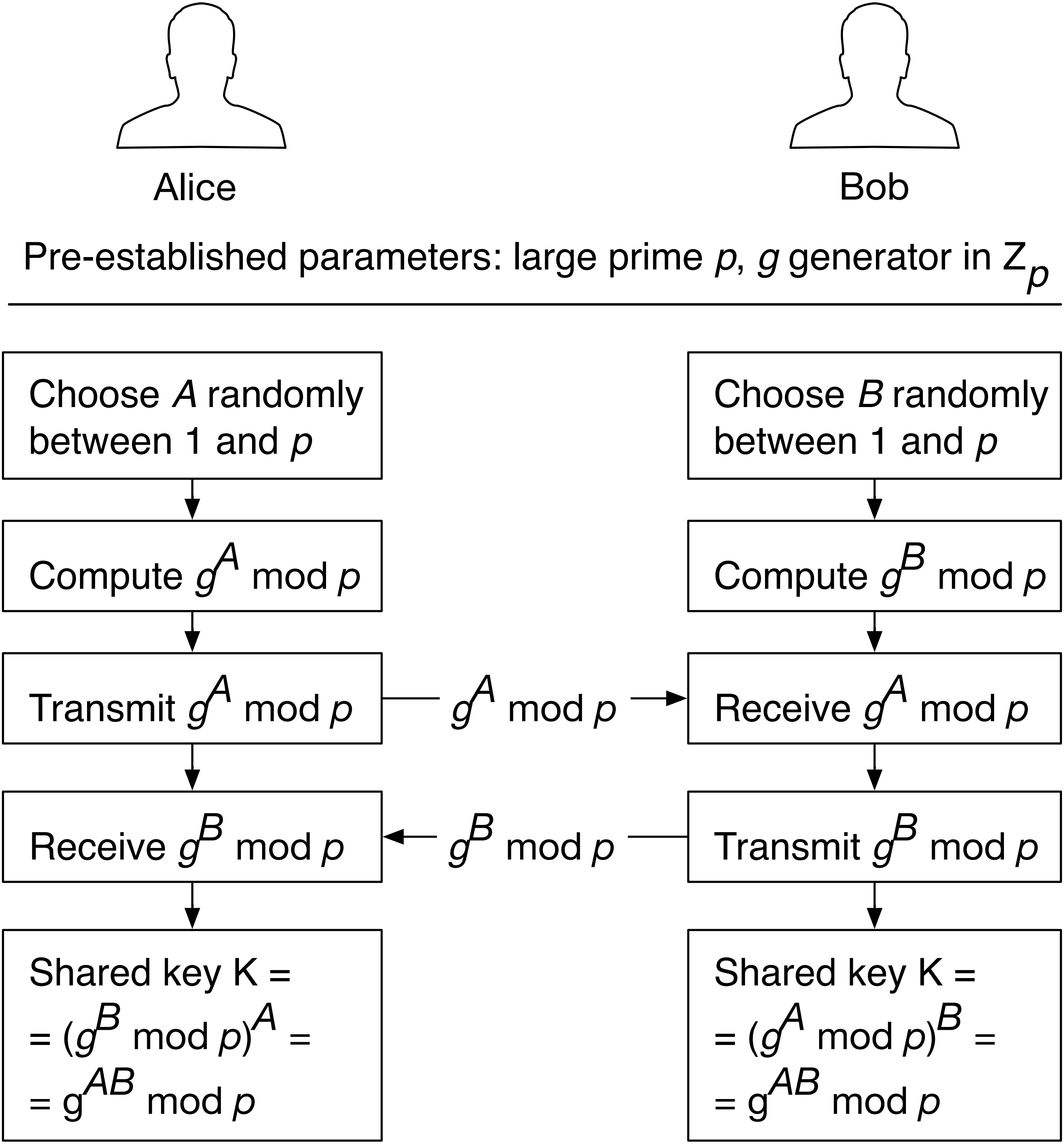

Alice

Bob

Pre-established parameters: large prime p, g generator in Z_p

Choose A randomly between 1 and p

Compute $g^A \bmod p$

Transmit $g^A \bmod p$

$g^A \bmod p$

Receive $g^B \bmod p$

$g^B \bmod p$

Shared key K = $= (g^B \bmod p)^A =$ $= g^{AB} \bmod p$

Choose B randomly between 1 and p

Compute $g^B \bmod p$

Receive $g^A \bmod p$

Transmit $g^B \bmod p$

Shared key K = $= (g^A \bmod p)^B =$ $= g^{AB} \bmod p$