

Alice  
picks  $x$

Bob  
picks  $y$

Alice

Bob

1

$p, g, g^x \bmod p$



2

$g^y \bmod p$



Alice computes  
 $(g^y \bmod p)^x$   
 $= g^{xy} \bmod p$

Bob computes  
 $(g^x \bmod p)^y$   
 $= g^{xy} \bmod p$