

Alice  
picks  $x$

Bob  
picks  $y$



1

$n, g, g^x \bmod n$



2

$g^y \bmod n$



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

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