

**Initiator**

generate random  $x$   
 $X = 'g'^x$

$X$

**Responder**

generate random  $y$   
 $Y = 'g'^y$

$Y$

shared key  
 $KI = KDF(<Y^x, I, R>)$

shared key  
 $KR = KDF(<X^y, I, R>)$

