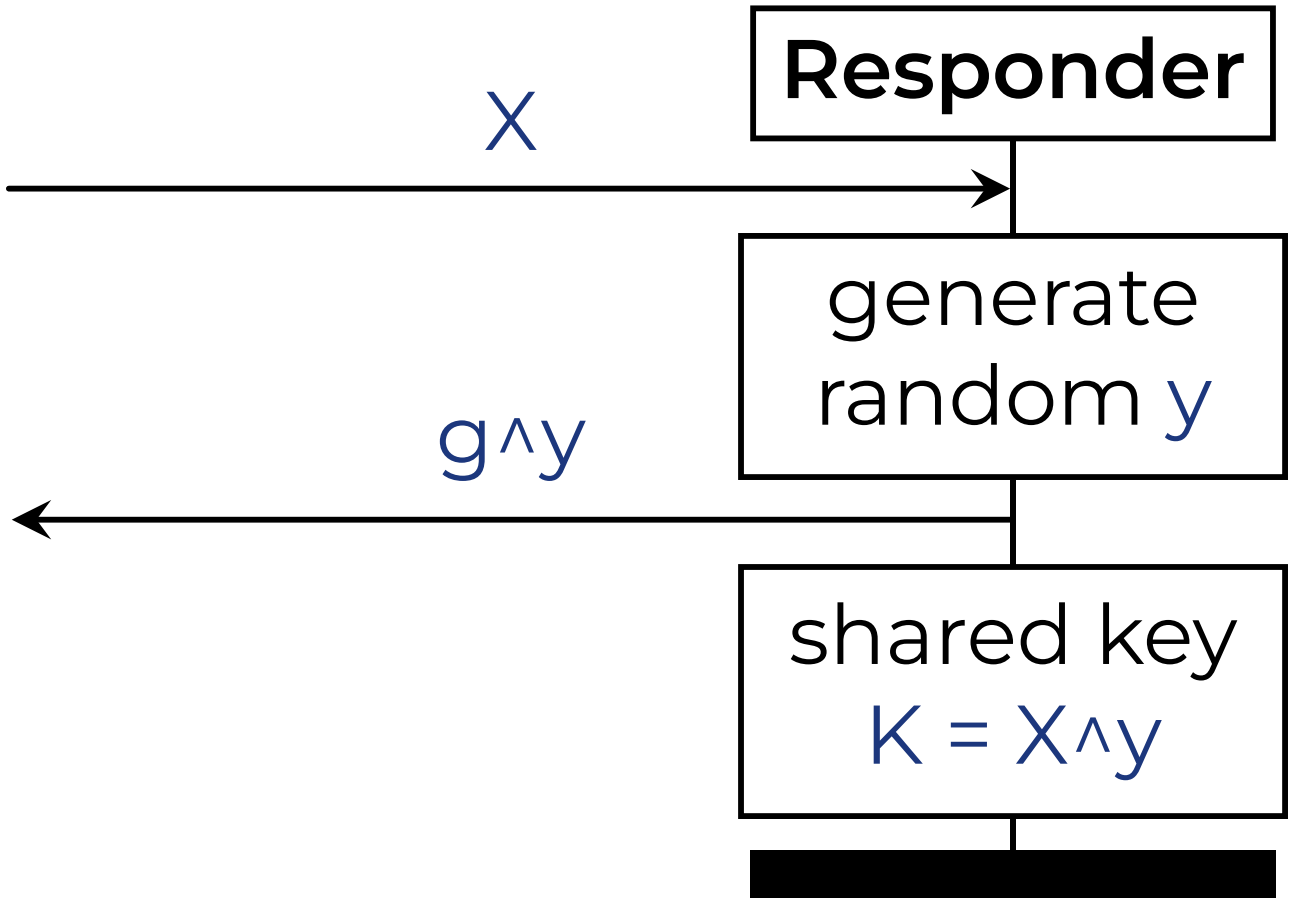
Responder
X
generate
random y
g^y
shared key
K = X^y