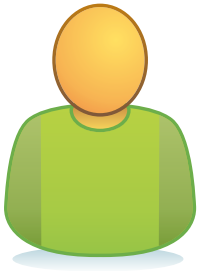

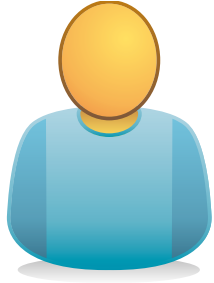

Secret: a

Public: p & g

Secret:b

send p & g

Secret: b

Public: p & g

g^b mod p = B

g^a mod p = A

send B

send A

B^a mod p = s

A^b mod p = s