p \_\_\_\_\_\_\_\_\_\_\_

α \_\_\_\_\_\_\_\_\_\_\_

**Alice**

Select a \_\_\_\_\_\_\_\_\_\_\_ (Private)

Compute A \_\_\_\_\_\_\_\_\_\_\_ A = αa mod p (Public)

Give A to Bob

**Bob**

Select b \_\_\_\_\_\_\_\_\_\_\_ (Private)

Compute B \_\_\_\_\_\_\_\_\_\_\_ B = αb mod p (Public)

Give B to Alice

**Alice computes key** = Ba mod p (she picked a, Bob gave her B ) \_\_\_\_\_\_\_\_\_\_\_

**Bob computes key** = Ab mod p (he picked b, Alice gave him A) \_\_\_\_\_\_\_\_\_\_\_