xuehai's input page:

(large) prime p: □

integer g having prime order in $\mathbb{F}_p^*$: □

secret int a (sender): □

Secret int b (reciever): □

Jonn's part:

* the sender computes $A \equiv g^a \pmod{p}$

A: □

correct

first compute g^a, then find the remainder of the division g^a/p.

* the reciever computes $B = g^b \pmod{p}$

B: □

correct

first compute g^b, then find the remainder of the division g^b/p.

* now, the individuals exchange A and B.

the shared secret value is:

$$B^a \equiv (g^b)^a \equiv g^{ab} = (g^a)^b \equiv A^b \pmod{p}$$

shared secret value: □

correct

a few options:

1) first calculat B^a, then find the remainder of the division B^a/p

2) first calculat A^b, then find the remainder of the division A^b/p

3) first calculat g^{ab}, then find the remainder of the division g^{ab}/p

* done! The individuals have sent a secret key over an insecure channel!