Xuehai's input:

(large) prime p: [ ]

element g of prime order: [ ]

private key (a): [ ]

message: [ ]

random key k: [ ]

Johns part:

* we must compute the public key $A = g^a \bmod p$ and publish it.

A: [ ]

correct!

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

* compute $C_1 = g^k \pmod p$

C_1: [ ]

correct!

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

* compute $C_2 = mA^k \pmod p$

C_2: [ ]

correct

first compute $m * A^k$,

then find the remainder of the divison $\frac{mA^k}{p}$

* That's it! the encrypted message (C_1, C_2).

Let's try decrypting the message:

compute: $(C_1^a)^{-1} * C_2 \pmod p$

decrypted message: [ ]

correct

first, calculate C_1^a.
the compute the division C_2 / C_1^a

* Done!