Welcome to Cryptography Interactive Learning System!

I want to learn: [Elgamal]

Why Elgamal?

(Click it will show introduction and intention)

Let's start with **encryption**:

(Click encryption will show the following)

Method v

(hide steps before click on them, just like Chegg solutions)

Step 1 of 3 v
Step 2 of 3 v
Step 3 of 3 v

Example v

(Hide example before user click on example)

Step 1 of 3 v
Step 2 of 3 v
Step 3 of 3 v

Are you ready to try it yourself? Yes

(Hide the following until user click Yes)

Click here to see how to how to choose your numbers

(Click here: new tab to prime generator website)

or click on dice to generate a random prime number for you

You can use WolframAlpha to help with calculation!

(WolframAlpha with hyperlink)

p : input a large prime integer here 🎲

g : an element g of prime order 🎲

a : private key a, $1 \le a \le p-1$ 🎲

Click Check to see if your number work

(Check -> backend, 1. check if p, q is prime, 2. check if e works for inputted p and q
And show up the following)

m : Input the message you want to encrypt

A : hint: $A = g^a \pmod p$ Check if it's correct

Publish the public key A

(if it's correct -> show correct under the button, incorrect! Check your calculation again!)

c_1 : hint: $c_1 = g^k \pmod p$ Check if it's correct

(if it's correct -> show correct under the button, incorrect! Check your calculation again!)

c_2 : hint: $c_2 = mA^k \pmod p$ Check if it's correct

(if it's correct -> show correct under the button, incorrect! Check your calculation again!)

(show the following after click Check for c)

GREAT JOB! You have finished encryption!

Now you have your ciphertext!

(Display (c_1, c_2) here)

Now, let's do decryption!

m': $m' = c_1^a \pmod p$ Check if it's correct

(if it's correct -> show correct under the button, incorrect! Check your calculation again!)

You will find out m' is the same as your inputted message m!