Welcome to Cryptography Interactive Learning System!

I want to learn: [Diffie Hellman]

Why Diffie Hellman?

(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)

In the following, we call the sender Alice, and the receiver Bob

p : a large prime integer here

g : an integer g of prime order in F_p^*

Click Check to see if your number work

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

Alice randomly picks a secret integer a

a : input a secret integer a

Bob randomly picks a secret integer a

b : input a secret integer b

Alice computes:

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

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

Bob computes:

B : $B = g^b \pmod p$ 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 B)

GREAT JOB! You have finished encryption!

Now Alice and Bob can exchange their encrypted messages!

Alice ------ A ------> Bob

Bob ------- B -----> Alice

Now, let's do decryption!

Alice computes:

B^a : $B^a \pmod p$ Check if it's correct

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

Bob computes:

A^b : $A^b \pmod p$ Check if it's correct

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

You will find out that Alice and Bob share the secret value $B^a = (g^b)^a = g^{ab} = (g^a)^b = A^b \pmod p$!