

```
Diffie-Hellman Key Exchange.py
1 p = 1797693134862315907729305190789024733617976978942306572734300811577326758055009631327084773224075360211201138798713933576587897688
2 q = (p-1) / 2
3 g = 3
4 A = 112983575163002618947589666666735428181684517845144875096902910066434723952623016603393212501214127399908823223492478725971266042754892798177781267
5 B = 111772767805210239496365191691516881043394988196297062013853646674574743401042736447328886156429629192691601526398366088012736749454626686281467579
6
7 maxn = 10000
8 multiple = 1
9 Alice_a = 0
10 for a in range(1, maxn+1):
11     multiple = multiple * g % p
12     if (multiple % p) == A:
13         Alice_a = a
14         break
15
16 multiple = 1
17 Bob_b = 0
18 for b in range(1, maxn+1):
19     multiple = multiple * g % p
20     if multiple == B:
21         Bob_b = b
22         break
23
24 output_Alice = B ** Alice_a % p
25 output_Bob = A ** Bob_b % p
26
27 print(output_Bob)
28 print(output_Alice)
29
```

p =
179769313486231590772930519078902473361797697894230657273430081157732675805500963
132708477322407536021120113879871393357658789768814416622492847430639474124377767
893424865485276302219601246094119453082952085005768838150682342462881473913110540
827237163350510684586298239947245938479716304835356329624227998859

q = (p-1) / 2

g = 3

A =
112983575163002618947589666666735428181684517845144875096902910066434723952623016
603393212501214127399908823223492478725971266042754892798177781267512821607470545
283059472689034731313027619864228688466438258327552045437590203790635506728603774
799021127049872571983254506993921153718739796769296097404717448108

B =
111772767805210239496365191691516881043394988196297062013853646674574743401042736
447328886156429629192691601526398366088012736749454626686281467579205675084461989
494513294624066074137247913037330040487275346913253345733429767781900977102687185
378411660147190296412313303321533586102552123457499563789255321369

maxn = 10000

multiple = 1

Alice_a = 0

for a in range(1, maxn+1):

 multiple = multiple * g % p

 if (multiple % p) == A:

 Alice_a = a

 break

multiple = 1

Bob_b = 0

```
for b in range(1, maxn+1):  
    multiple = multiple * g % p  
    if multiple == B:  
        Bob_b = b  
        break
```

```
output_Alice = B ** a % p  
output_Bob = A ** b % p
```

```
print(output_Bob)  
print(output_Alice)
```

```
# k = output_Alice = output_Bob =  
108281127834534623810417078020561498665963920722439039409874596727792606753195226  
630990803887709039825462505249924203502002076243274206123001706208026653029057500  
457776843481258274843650075907186383731879368899673093247226552949922258154109141  
05072210725045953105019352457540772995508978315699107247398350128
```