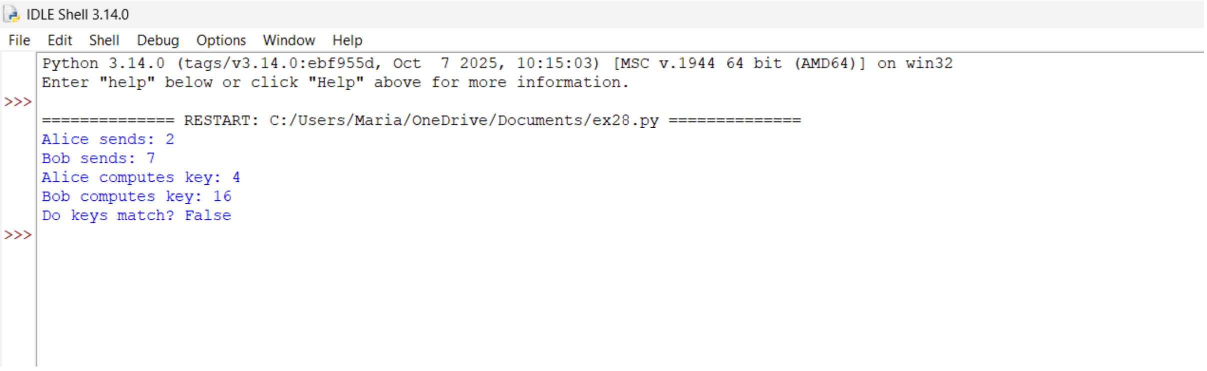
28. Write a python program for Diffie-Hellman protocol, each participant selects a secret number x and sends the other participant ax mod q for some public number a. What would happen if the participants sent each other xa for some public number a instead? Give at least one method Alice and Bob could use to agree on a key. Can Eve break your system without finding the secret numbers? Can Eve find the secret numbers?

Code:

```
def wrong_dh(a, q, x, y):
    # Alice sends x^a mod q
    A = pow(x, a, q)
    # Bob sends y^a mod q
    B = pow(y, a, q)
 # Alice computes supposed key
    KA = pow(B, x, q)
    # Bob computes supposed key
    KB = pow(A, y, q)
return A, B, KA, KB
a = 5
q = 23
x = 6  # Alice's secret
y = 15 # Bob's secret
A, B, KA, KB = wrong_dh(a, q, x, y)
print("Alice sends:", A)
print("Bob sends:", B)
print("Alice computes key:", KA)
print("Bob computes key:", KB)
print("Do keys match?", KA == KB)
```



```
Python 3.14.0 (tags/v3.14.0:ebf955d, Oct  7 2025, 10:15:03) [MSC v.1944 64 bit (AMD64)] on win32
Enter "help" below or click "Help" above for more information.
>>>
============== RESTART: C:/Users/Maria/OneDrive/Documents/ex28.py ==============
Alice sends: 2
Bob sends: 7
Alice computes key: 4
Bob computes key: 16
Do keys match? False
>>>
```