DIFFIE - HELLMAN Key Exchange

```
print("Both Parties Agree To A Single Prime No.")
prime = int(input(" Enter A Prime No To Be Considered : "))
print("Both Must Agree With A Single Primitive Root To Use")
root = int(input(" Enter The Primitive Root : "))
```

```
Both Parties Agree To A Single Prime No.
 Enter A Prime No To Be Considered : 31
Both Must Agree With A Single Primitive Root To Use
 Enter The Primitive Root : 11
```

```
alicesecret = int(input("Enter A Secret No From User 1 : "))
bobsecret = int(input("Enter A Secret no From User 2 : "))
print('\n')
```

```
Enter A Secret No From User 1 : 98
Enter A Secret no From User 2 : 60
```

```
print("Party1's Public Key -> A = root^alicesecre*mod(prime))")
alicepublic = (root**alicesecret)%prime
print("Party1's Public Key Is : ", alicepublic, "\n")

print("Party2's Public Key -> A = root^bobsecre*mod(prime))")
bobpublic = (root**bobsecret)%prime
print("Party2's Public Key Is : ", bobpublic, "\n")
```

```
Party1's Public Key -> A = root^alicesecre*mod(prime))
Party1's Public Key Is :  19

Party2's Public Key -> A = root^bobsecre*mod(prime))
Party2's Public Key Is :  1
```