For encryption purpose two parties Alice and Bob want to share some secrete key over a communication network using Diffie-Hellman Key Exchange algorithm. Prepare suitable environment for the same

CODE:

```
import random


p=int(input('Enter any prime number: '))
alpha=[]
l1=[]


def check(a, b):
    for i in range(1, b):
        if i in a:
            continue
        else:
            return False


for i in range(2, p):
    for j in range(1, p):
        val=(i**j)%p
        l1.append(val)
    alpha.append(l1)
    l1=[]


fin_alpha=[]
for i in range(len(alpha)):
    if check(alpha[i], p) != False:
```

```
            fin_alpha.append(alpha.index(alpha[i])+2)

    print('The available values for alpha will be: ', *fin_alpha)

    a=random.randint(1, p)
    b=random.randint(1, p)
    while a==b:
       b=random.randint(1, p)



    sel_alp=min(fin_alpha)

    public_A=(sel_alp**a)%p
    public_B=(sel_alp**b)%p
    c=a*b
    key_a=(sel_alp**c)%p
    key_b=(sel_alp**c)%p
    print(f'Selected value for alpha: {sel_alp}')
    print(f'Public_A: {public_A}')
    print(f'Public_B: {public_B}')
    print(f'Selected key: {key_a}')
```

OUTPUT:

Tejas Tripathi

```
In [3]: runfile('C:/Users/Admin/study material/sem5/
Practicals/Cryptography/Practical-9/
diffie_hellman.py', wdir='C:/Users/Admin/study
material/sem5/Practicals/Cryptography/Practical-9')

Enter any prime number: 101
The available values for alpha will be:  2 3 7 8 11
12 15 18 26 27 28 29 34 35 38 40 42 46 48 50 51 53 55
59 61 63 66 67 72 73 74 75 83 86 89 90 93 94 98 99
Selected value for alpha: 2
Public_A: 47
Public_B: 53
Selected key: 70

In [4]:
```