

```
In [1]: import random
import math
```

```
In [2]: def generate(n,g):
print("Diffie-Hellman Key Exchange\n")

print("Modulus chosen:",n)
print("Base chosen:",g)

#Choose random numbers
a=random.randint(2,1000)
b=random.randint(2,1000)

print("Number chosen by A:",a)
print("Number chosen by B:",b)

print("\nCalculating shared keys for both A and B\n")
A=pow(g,a)%n
B=pow(g,b)%n

print("A's calculated value:",A)
print("B's calculated value:",B)

#Exchange calculated values
print("\nExchanging calculated values\n")
k1=pow(B,a)%n
k2=pow(A,b)%n

print("A's secret key:",k1)
print("B's secret key:",k2)
```

```
In [7]: generate(95,23)
```

Diffie-Hellman Key Exchange

Modulus chosen: 95

Base chosen: 23

Number chosen by A: 521

Number chosen by B: 697

Calculating shared keys for both A and B

A's calculated value: 43

B's calculated value: 28

Exchanging calculated values

A's secret key: 93

B's secret key: 93

```
In [ ]:
```