In [1]:

```
import random
import math
```

In [2]:

```
def generate(p,g):
    print("Diffie-Hellman Key Exchange\n")

    #Choose random numbers
    a=random.randint(2,1000)
    b=random.randint(2,1000)
    print("Modulus chosen:",p)
    print("Base chosen:",g)
    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)%p
    B=pow(g,b)%p

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

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

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

In [3]:

```
generate(95,23)
```

```
Diffie-Hellman Key Exchange

Modulus chosen: 95
Base chosen: 23
Number chosen by A: 330
Number chosen by B: 905

Calculating shared keys for both A and B

A's calculated value: 49
B's calculated value: 93

Exchanging calculated values

A's secret key: 64
B's secret key: 64
```

In [ ]:

```

```