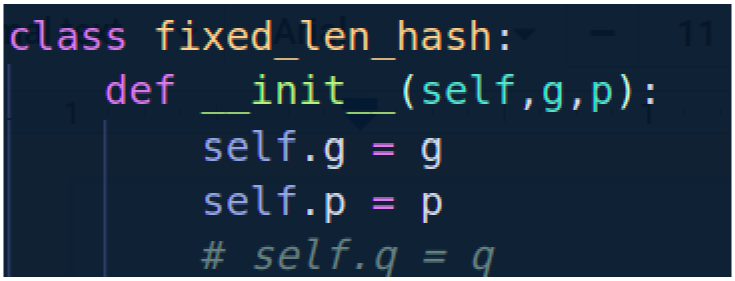
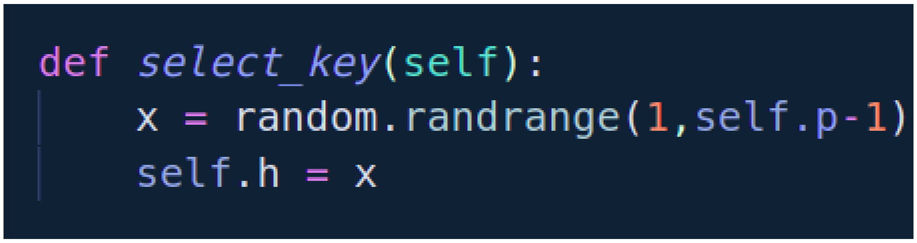
FIXED LENGTH HASH FUNCTION CODE DOCUMENTATION

A Class named **fixed_len_hash** is created incorporating all required variables and functions.



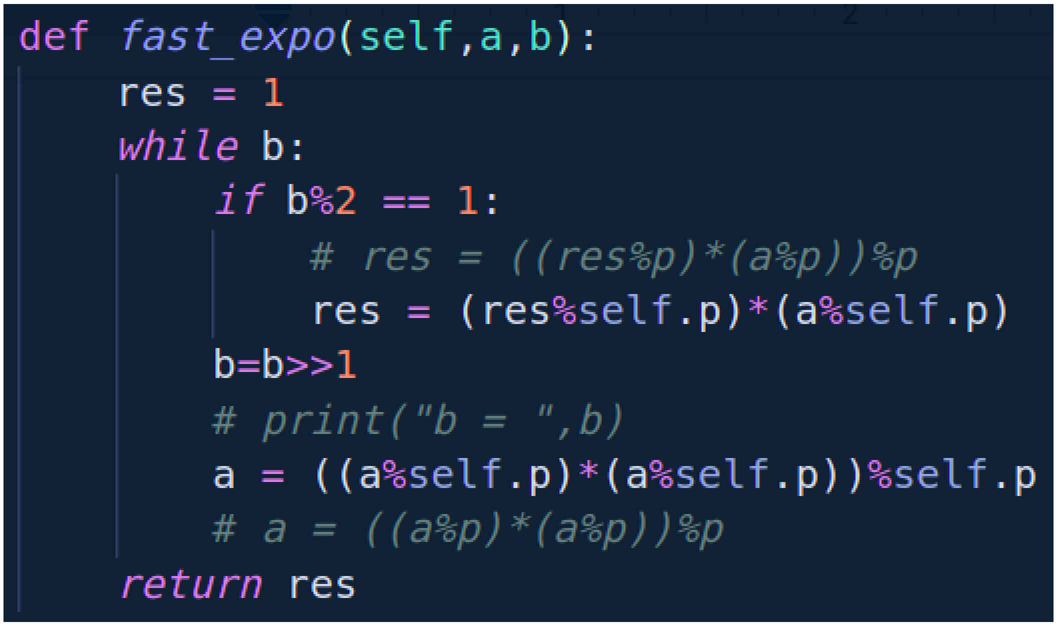
```
class fixed_len_hash:
    def __init__(self,g,p):
        self.g = g
        self.p = p
        # self.g = g
```

The value of group generator **g** and the value of prime number **p** is initialized here



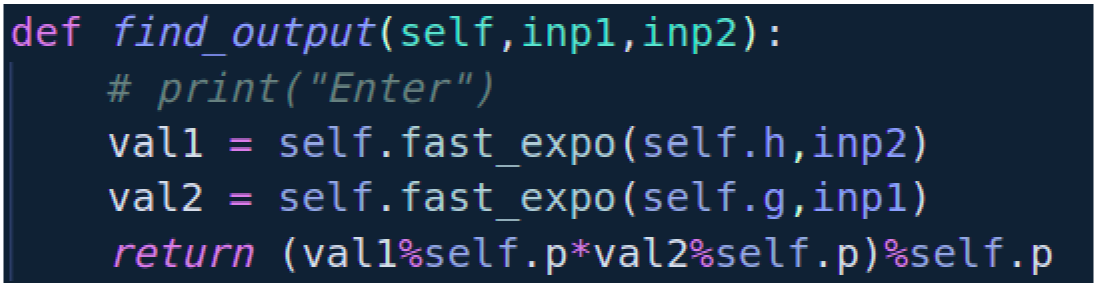
```
def select_key(self):
    x = random.randrange(1,self.p-1)
    self.h = x
```

This function selects a key, it basically selects an integer in the range of (1, p-1)



```
def fast_expo(self,a,b):
    res = 1
    while b:
        if b%2 == 1:
            # res = ((res%p)*(a%p))%p
            res = (res%self.p)*(a%self.p)
        b=b>>1
        # print("b = ",b)
        a = ((a%self.p)*(a%self.p))%self.p
        # a = ((a%p)*(a%p))%p
    return res
```

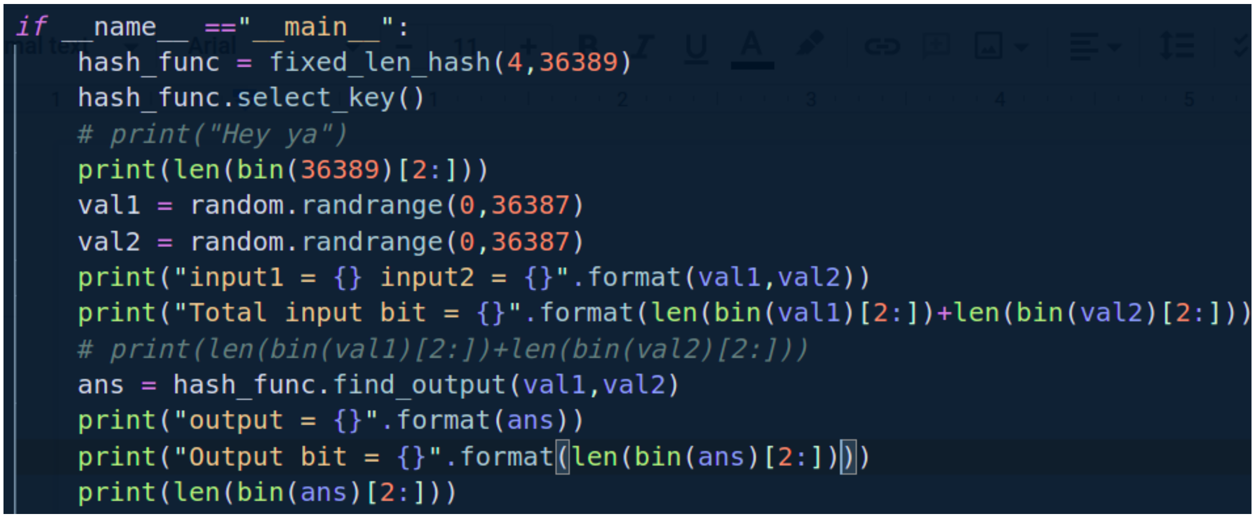
This function computes a^b in log(b) time.



```
def find_output(self,inp1,inp2):
    # print("Enter")
    val1 = self.fast_expo(self.h,inp2)
    val2 = self.fast_expo(self.g,inp1)
    return (val1%self.p*val2%self.p)%self.p
```

find_output function computes the hashed output for two inputs inp1 and inp2 using the properties of the hash function.

Inp1 and inp2 can be thought of as two n bit numbers that consists of total n bits and it is being mapped to a n bit value.



```
if __name__ =="__main__":
    hash_func = fixed_len_hash(4,36389)
    hash_func.select_key()
    # print("Hey ya")
    print(len(bin(36389)[2:]))
    val1 = random.randrange(0,36387)
    val2 = random.randrange(0,36387)
    print("input1 = {} input2 = {}".format(val1,val2))
    print("Total input bit = {}".format(len(bin(val1)[2:])+len(bin(val2)[2:]))
    # print(len(bin(val1)[2:])+len(bin(val2)[2:]))
    ans = hash_func.find_output(val1,val2)
    print("output = {}".format(ans))
    print("Output bit = {}".format(len(bin(ans)[2:])))
    print(len(bin(ans)[2:]))
```

This part is used to give all the inputs and to call all the outputs the input bit, output bits are being printed on the screen, this hash function is mapping a 2n bit input to n bit output.