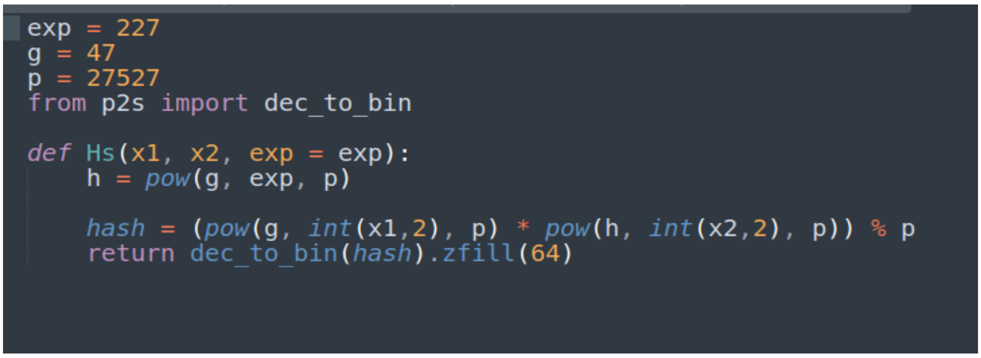
# POIS ASSIGNMENT 1

# TASK 6

# USE DLP TO BUILD A FIXED LENGTH COLLISION RESISTANT HASH FUNCTION

## CODE EXPLANATION



```
exp = 227
g = 47
p = 27527
from p2s import dec_to_bin

def Hs(x1, x2, exp = exp):
    h = pow(g, exp, p)

    hash = (pow(g, int(x1,2), p) * pow(h, int(x2,2), p)) % p
    return dec_to_bin(hash).zfill(64)
```

Hash value returned is :
hash = (g^x1 % p) * (((g^exp % p)^x2 % p)) %p

Where
exp = 227
g = 47
p = 27527