小组成员：

喻瑞20214180

王昌杰20214065

共享素数P=109， 以及其原根整数α=6，使用离散对数作为单向函数，计算过程如下所示：

A：生成私钥，计算公钥，A收到B的公钥 ，计算得到最终的共享密钥

B：生成私钥，计算公钥，B收到A的公钥，计算得到最终的共享密钥

计算过程中使用快速模幂算法实现如下：

def fast\_power(base, exponent, modulus):

result = 1

base = base % modulus # 取模以防止溢出

while exponent > 0:

# 如果指数是奇数，则乘以当前的base

if exponent % 2 == 1:

result = (result \* base) % modulus

# 将指数减半，base变为base的平方

exponent = exponent // 2

base = (base \* base) % modulus

return result

# 计算 6^10 mod 109

result = fast\_power(6, 10, 109)

print(result)