Diffie-Hellman 密钥交换计算过程

1. 公共参数选择

①素数 p=101 g=2

②验证原根代码

```
p = 101
g = 2
sequence = [pow(g, i, p) for i in range(1, p)]
assert len(set(sequence)) == p - 1, "g 不是原根"
print("g 是原根")
```

③结果

2. 私钥与公钥计算

①成员 A 的私钥 a = 19，公钥 A = g^a mod p = 98

②成员 B 的私钥 b = 45，公钥 B = b^a mod p = 41

3. 共享密钥计算

①A 的共享密钥 Ka = B^a mod p = 69

②B 的共享密钥 Kb = A^b mod p = 69

验证 Ka = Kb ，共享密钥一致

4. 结果

使用 D-H 密钥交换生成的共享密钥为 69

附录 1　D-H 验证

```
import random


# 公共参数
p = 211  # 素数
g = 2    # 原根


# A 选择私钥和公钥
a = random.randint(1, p - 1)
A = pow(g, a, p)


# B 选择私钥和公钥
b = random.randint(1, p - 1)
B = pow(g, b, p)


# 计算共享密钥
K_A = pow(B, a, p)  # A 的共享密钥
K_B = pow(A, b, p)  # B 的共享密钥


# 打印结果
print(f"p = {p}, g = {g}")
print(f"A 的私钥: {a}, 公钥: {A}")
print(f"B 的私钥: {b}, 公钥: {B}")
print(f"A 计算的共享密钥: {K_A}")
print(f"B 计算的共享密钥: {K_B}")
assert K_A == K_B, "共享密钥不一致！"
```

附录 2　题目所给的 p，g 验证

```
p = 101, g = 2
A的私钥: 19, 公钥: 98
B的私钥: 45, 公钥: 41
A计算的共享密钥: 69
B计算的共享密钥: 69

p = 103, g = 5
A的私钥: 55, 公钥: 96
B的私钥: 62, 公钥: 55
A计算的共享密钥: 2
B计算的共享密钥: 2

p = 107, g = 2
A的私钥: 63, 公钥: 46
B的私钥: 10, 公钥: 61
A计算的共享密钥: 102
B计算的共享密钥: 102

p = 109, g = 6
A的私钥: 91, 公钥: 58
B的私钥: 31, 公钥: 40
A计算的共享密钥: 96
B计算的共享密钥: 96

p = 113, g = 3
A的私钥: 15, 公钥: 54
B的私钥: 99, 公钥: 19
A计算的共享密钥: 68
B计算的共享密钥: 68

p = 127, g = 3
A的私钥: 115, 公钥: 7
B的私钥: 66, 公钥: 100
A计算的共享密钥: 38
B计算的共享密钥: 38

p = 131, g = 2
A的私钥: 59, 公钥: 88
B的私钥: 10, 公钥: 107
A计算的共享密钥: 99
B计算的共享密钥: 99

p = 137, g = 3
A的私钥: 29, 公钥: 94
B的私钥: 88, 公钥: 133
A计算的共享密钥: 59
B计算的共享密钥: 59

p = 139, g = 2
A的私钥: 51, 公钥: 14
B的私钥: 52, 公钥: 28
A计算的共享密钥: 45
B计算的共享密钥: 45

p = 149, g = 2
A的私钥: 81, 公钥: 21
B的私钥: 125, 公钥: 34
A计算的共享密钥: 50
B计算的共享密钥: 50

p = 151, g = 6
A的私钥: 110, 公钥: 105
B的私钥: 33, 公钥: 60
A计算的共享密钥: 59
B计算的共享密钥: 59

p = 157, g = 5
A的私钥: 6, 公钥: 82
B的私钥: 82, 公钥: 3
A计算的共享密钥: 101
B计算的共享密钥: 101

p = 163, g = 2
A的私钥: 115, 公钥: 89
B的私钥: 67, 公钥: 130
A计算的共享密钥: 117
B计算的共享密钥: 117

p = 167, g = 5
A的私钥: 32, 公钥: 28
B的私钥: 88, 公钥: 48
A计算的共享密钥: 16
B计算的共享密钥: 16

p = 173, g = 2
A的私钥: 163, 公钥: 74
B的私钥: 148, 公钥: 118
A计算的共享密钥: 160
B计算的共享密钥: 160

p = 173, g = 2
A的私钥: 163, 公钥: 74
B的私钥: 148, 公钥: 118
A计算的共享密钥: 160
B计算的共享密钥: 160

p = 179, g = 2
A的私钥: 74, 公钥: 65
B的私钥: 129, 公钥: 143
A计算的共享密钥: 48
B计算的共享密钥: 48

p = 181, g = 2
A的私钥: 91, 公钥: 179
B的私钥: 57, 公钥: 6
A计算的共享密钥: 175
B计算的共享密钥: 175

p = 191, g = 19
A的私钥: 12, 公钥: 54
B的私钥: 107, 公钥: 137
A计算的共享密钥: 50
B计算的共享密钥: 50

p = 193, g = 5
A的私钥: 139, 公钥: 70
B的私钥: 39, 公钥: 74
A计算的共享密钥: 180
B计算的共享密钥: 180

p = 197, g = 2
A的私钥: 57, 公钥: 159
B的私钥: 157, 公钥: 152
A计算的共享密钥: 153
B计算的共享密钥: 153

p = 199, g = 3
A的私钥: 38, 公钥: 131
B的私钥: 44, 公钥: 178
A计算的共享密钥: 43
B计算的共享密钥: 43

p = 211, g = 2
A的私钥: 11, 公钥: 149
B的私钥: 207, 公钥: 132
A计算的共享密钥: 60
B计算的共享密钥: 60

p = 223, g = 3
A的私钥: 158, 公钥: 213
B的私钥: 149, 公钥: 117
A计算的共享密钥: 177
B计算的共享密钥: 177

p = 227, g = 2
A的私钥: 160, 公钥: 221
B的私钥: 92, 公钥: 9
A计算的共享密钥: 44
B计算的共享密钥: 44

p = 229, g = 6
A的私钥: 168, 公钥: 27
B的私钥: 203, 公钥: 160
A计算的共享密钥: 53
B计算的共享密钥: 53

p = 233, g = 3
A的私钥: 202, 公钥: 110
B的私钥: 206, 公钥: 56
A计算的共享密钥: 169
B计算的共享密钥: 169

p = 239, g = 7
A的私钥: 195, 公钥: 92
B的私钥: 127, 公钥: 118
A计算的共享密钥: 235
B计算的共享密钥: 235

p = 241, g = 7
A的私钥: 129, 公钥: 156
B的私钥: 206, 公钥: 108
A计算的共享密钥: 125
B计算的共享密钥: 125

p = 251, g = 6
A的私钥: 85, 公钥: 40
B的私钥: 198, 公钥: 39
A计算的共享密钥: 243
B计算的共享密钥: 243
```