D-H密钥交换协议计算过程

# 1. 选择素数和原根

选择素数 p = 223, 原根 g = 5

# 2. 私钥选择

成员A选择私钥 a = 11

成员B选择私钥 b = 139

# 3. 公钥计算

成员A计算公钥 A = g^a mod p = 45

成员B计算公钥 B = g^b mod p = 176

# 4. 共享密钥计算

成员A计算共享密钥 K\_A = B^a mod p = 145

成员B计算共享密钥 K\_B = A^b mod p = 145

# 5. 结果验证

共享密钥一致: 145