# Diffie-Hellman 密钥交换机制验证

选择的素数 (p): 139

选择的原根 (g): 2

A 的私钥 (a): 39

B 的私钥 (b): 66

A 计算公钥 (A = g^a mod p):

A = 2^39 mod 139 = 105

B 计算公钥 (B = g^b mod p):

B = 2^66 mod 139 = 52

A 计算共享秘密密钥 (s\_A = B^a mod p):

s\_A = 52^39 mod 139 = 80

B 计算共享秘密密钥 (s\_B = A^b mod p):

s\_B = 105^66 mod 139 = 80

验证成功：A 和 B 得到了相同的共享秘密密钥。