小组名： Impact
小组成员：陈财祥 20214851
张傲然 20214872

实验思路：首先我们需要找到 100-255 之间的素数。在这个范围内，有以下素数： 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179,181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251
我们选择其中一个素数作为模数 p，并找到它的原根。然后我们再选择一个私有的整数作为私钥 a，并计算出公钥 A。接着，对方也选择一个私有的整数作为私钥 b，并计算出公钥 B。最后，双方交换公钥并计算出共享密钥。
参数选择： p = 103（大素数） g = 5（原根）

密钥生成者 A 和 B 执行以下步骤：

a. A 选择私有密钥 a = 3，B 选择私有密钥 b = 6。

b. A 计算公开值 A = g^a mod p = 5^3 mod 103 = 125 mod 103 = 22。B 计算公开值 B = g^b mod p = 5^6 mod 103 = 15625 mod 103 = 97。

c. A 将 A = 22 发送给 B，B 将 B = 97 发送给 A。

密钥计算： A 计算 K = B^a mod p = 97^3 mod 103 = 912673 mod 103 = 88。 B 计算 K = A^b mod p = 22^6 mod 103 = 113379904 mod 103 = 88。

由于 A 和 B 计算所得的共享密钥 K 都是 88，可以证明 A 和 B 通过 D-H 协议计算得到了相同的共享密钥。这意味着 A 和 B 现在可以使用共享密钥 K 进行加密通信。