小组成员：蒋铭皓 20214554

郭景逸 20214148

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g。 A随机选择一个小于p的整数作为私钥，根据这个整数得出A的公钥。B随机选择一个小于p的整数作为私钥，根据这个整数得出B的公钥。最后，双方交换公钥并计算出共享密钥。计算过程可以由python代码得出

源代码：

import random

p\_all=[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]

g\_all=[2,5,2,6,3,3,2,3,2,2,6,5,2,5,2,2,2,19,5,2,3,2,3,2,6,3,7,7,6]

for i in range(len(p\_all)):

        p = p\_all[i]

        g = g\_all[i]

*# A和B随机选择私钥*

        private\_key\_A = random.randint(2, p - 1)

        private\_key\_B = random.randint(2, p - 1)

*# A计算公钥*

        public\_key\_A = pow(g, private\_key\_A, p)

*# B计算公钥*

        public\_key\_B = pow(g, private\_key\_B, p)

*# A和B交换公钥，计算共享密钥*

        shared\_key\_A = pow(public\_key\_B, private\_key\_A, p)

        shared\_key\_B = pow(public\_key\_A, private\_key\_B, p)

        print(f"素数p: {p}")

        print(f"原根g: {g}")

        print(f"A的私钥: {private\_key\_A}")

        print(f"A的公钥: {public\_key\_A}")

        print(f"B的私钥: {private\_key\_B}")

        print(f"B的公钥: {public\_key\_B}")

        print(f"A的共享密钥: {shared\_key\_A}")

        print(f"B的共享密钥: {shared\_key\_B}")

运行结果：

素数p: 101

原根g: 2

A的私钥: 4

A的公钥: 16

B的私钥: 65

B的公钥: 57

A的共享密钥: 87

B的共享密钥: 87

素数p: 103

原根g: 5

A的私钥: 28

A的公钥: 58

B的私钥: 51

B的公钥: 102

A的共享密钥: 1

B的共享密钥: 1

素数p: 107

原根g: 2

A的私钥: 12

A的公钥: 30

B的私钥: 91

B的公钥: 70

A的共享密钥: 29

B的共享密钥: 29

素数p: 109

原根g: 6

A的私钥: 91

A的公钥: 58

B的私钥: 46

B的公钥: 28

A的共享密钥: 20

B的共享密钥: 20

素数p: 113

原根g: 3

A的私钥: 61

A的公钥: 96

B的私钥: 48

B的公钥: 16

A的共享密钥: 49

B的共享密钥: 49

素数p: 127

原根g: 3

A的私钥: 114

A的公钥: 87

B的私钥: 108

B的公钥: 32

A的共享密钥: 8

B的共享密钥: 8

素数p: 131

原根g: 2

A的私钥: 42

A的公钥: 74

B的私钥: 100

B的公钥: 112

A的共享密钥: 84

B的共享密钥: 84

素数p: 137

原根g: 3

A的私钥: 66

A的公钥: 76

B的私钥: 17

B的公钥: 127

A的共享密钥: 100

B的共享密钥: 100

素数p: 139

原根g: 2

A的私钥: 18

A的公钥: 129

B的私钥: 12

B的公钥: 65

A的共享密钥: 44

B的共享密钥: 44

素数p: 149

原根g: 2

A的私钥: 16

A的公钥: 125

B的私钥: 111

B的公钥: 44

A的共享密钥: 1

B的共享密钥: 1

素数p: 151

原根g: 6

A的私钥: 115

A的公钥: 23

B的私钥: 34

B的公钥: 58

A的共享密钥: 38

B的共享密钥: 38

素数p: 157

原根g: 5

A的私钥: 89

A的公钥: 131

B的私钥: 147

B的公钥: 7

A的共享密钥: 23

B的共享密钥: 23

素数p: 163

原根g: 2

A的私钥: 111

A的公钥: 138

B的私钥: 155

B的公钥: 149

A的共享密钥: 37

B的共享密钥: 37

素数p: 167

原根g: 5

A的私钥: 16

A的公钥: 144

B的私钥: 133

B的公钥: 68

A的共享密钥: 150

B的共享密钥: 150

素数p: 173

原根g: 2

A的私钥: 40

A的公钥: 10

B的私钥: 4

B的公钥: 16

A的共享密钥: 139

B的共享密钥: 139

素数p: 179

原根g: 2

A的私钥: 38

A的公钥: 9

B的私钥: 158

B的公钥: 149

A的共享密钥: 107

B的共享密钥: 107

素数p: 181

原根g: 2

A的私钥: 47

A的公钥: 105

B的私钥: 13

B的公钥: 47

A的共享密钥: 21

B的共享密钥: 21

素数p: 191

原根g: 19

A的私钥: 105

A的公钥: 139

B的私钥: 124

B的公钥: 129

A的共享密钥: 25

B的共享密钥: 25

素数p: 193

原根g: 5

A的私钥: 114

A的公钥: 126

B的私钥: 37

B的公钥: 57

A的共享密钥: 24

B的共享密钥: 24

素数p: 197

原根g: 2

A的私钥: 165

A的公钥: 103

B的私钥: 29

B的公钥: 11

A的共享密钥: 147

B的共享密钥: 147

素数p: 199

原根g: 3

A的私钥: 18

A的公钥: 125

B的私钥: 193

B的公钥: 95

A的共享密钥: 18

B的共享密钥: 18

素数p: 211

原根g: 2

A的私钥: 112

A的公钥: 83

B的私钥: 121

B的公钥: 85

A的共享密钥: 83

B的共享密钥: 83

素数p: 223

原根g: 3

A的私钥: 44

A的公钥: 116

B的私钥: 35

B的公钥: 70

A的共享密钥: 199

B的共享密钥: 199

素数p: 227

原根g: 2

A的私钥: 80

A的公钥: 69

B的私钥: 107

B的公钥: 39

A的共享密钥: 62

B的共享密钥: 62

素数p: 229

原根g: 6

A的私钥: 140

A的公钥: 20

B的私钥: 139

B的公钥: 156

A的共享密钥: 82

B的共享密钥: 82

素数p: 233

原根g: 3

A的私钥: 79

A的公钥: 180

B的私钥: 96

B的公钥: 184

A的共享密钥: 117

B的共享密钥: 117

素数p: 239

原根g: 7

A的私钥: 57

A的公钥: 114

B的私钥: 122

B的公钥: 135

A的共享密钥: 17

B的共享密钥: 17

素数p: 241

原根g: 7

A的私钥: 83

A的公钥: 84

B的私钥: 190

B的公钥: 2

A的共享密钥: 120

B的共享密钥: 120

素数p: 251

原根g: 6

A的私钥: 225

A的公钥: 231

B的私钥: 182

B的公钥: 13

A的共享密钥: 149

B的共享密钥: 149

总结：

根据D-H协议机制流程对101-255之间的素数进行计算后，每个素数共享密钥各自相等，初步验证了D-H密钥交换机制。