使用100-255之间的素数(和原根)构建单向函数 按照D-H协议机制流程进行计算

素数 q= 101
本原根 g= 2
A获取的私钥 Xa= 22
B获取的私钥 Xb= 87
A计算得到的公钥 Ya为： 77
B计算得到的公钥 Yb为： 46
------X_A与B交换公钥------
A计算得到的key为： 22
B计算得到的key为： 22

素数 q= 103
本原根 g= 5
A获取的私钥 Xa= 93
B获取的私钥 Xb= 88
A计算得到的公钥 Ya为： 37
B计算得到的公钥 Yb为： 4
------X_A与B交换公钥------
A计算得到的key为： 23
B计算得到的key为： 23

素数 q= 107
本原根 g= 2
A获取的私钥 Xa= 85
B获取的私钥 Xb= 84
A计算得到的公钥 Ya为： 78
B计算得到的公钥 Yb为： 39
------X_A与B交换公钥------
A计算得到的key为： 37
B计算得到的key为： 37

素数 q= 109
本原根 g= 6
A获取的私钥 Xa= 73
B获取的私钥 Xb= 106
A计算得到的公钥 Ya为： 52
B计算得到的公钥 Yb为： 106
------X_A与B交换公钥------
A计算得到的key为： 83
B计算得到的key为： 83

素数 q= 113
本原根 g= 3
A获取的私钥 Xa= 14
B获取的私钥 Xb= 65

A计算得到的公钥 Ya为： 18
B计算得到的公钥 Yb为： 92
------X_A与B交换公钥------
A计算得到的key为： 18
B计算得到的key为： 18

素数 q= 127
本原根 g= 3
A获取的私钥 Xa= 112
B获取的私钥 Xb= 100
A计算得到的公钥 Ya为： 52
B计算得到的公钥 Yb为： 79
------X_A与B交换公钥------
A计算得到的key为： 52
B计算得到的key为： 52

素数 q= 131
本原根 g= 2
A获取的私钥 Xa= 10
B获取的私钥 Xb= 79
A计算得到的公钥 Ya为： 107
B计算得到的公钥 Yb为： 122
------X_A与B交换公钥------
A计算得到的key为： 107
B计算得到的key为： 107

素数 q= 137
本原根 g= 3
A获取的私钥 Xa= 60
B获取的私钥 Xb= 4
A计算得到的公钥 Ya为： 64
B计算得到的公钥 Yb为： 81
------X_A与B交换公钥------
A计算得到的key为： 59
B计算得到的key为： 59

素数 q= 139
本原根 g= 2
A获取的私钥 Xa= 34
B获取的私钥 Xb= 128
A计算得到的公钥 Ya为： 25
B计算得到的公钥 Yb为： 30
------X_A与B交换公钥------
A计算得到的key为： 107
B计算得到的key为： 107

素数 q= 149
本原根 g= 2
A获取的私钥 Xa= 106
B获取的私钥 Xb= 106
A计算得到的公钥 Ya为： 20
B计算得到的公钥 Yb为： 20
------X_A与B交换公钥------
A计算得到的key为： 49
B计算得到的key为： 49

素数 q= 151
本原根 g= 6
A获取的私钥 Xa= 125
B获取的私钥 Xb= 34
A计算得到的公钥 Ya为： 119
B计算得到的公钥 Yb为： 58
------X_A与B交换公钥------
A计算得到的key为： 32
B计算得到的key为： 32

素数 q= 157
本原根 g= 5
A获取的私钥 Xa= 37
B获取的私钥 Xb= 7
A计算得到的公钥 Ya为： 24
B计算得到的公钥 Yb为： 96
------X_A与B交换公钥------
A计算得到的key为： 123
B计算得到的key为： 123

素数 q= 163
本原根 g= 2
A获取的私钥 Xa= 60
B获取的私钥 Xb= 139
A计算得到的公钥 Ya为： 136
B计算得到的公钥 Yb为： 129
------X_A与B交换公钥------
A计算得到的key为： 61
B计算得到的key为： 61

素数 q= 167
本原根 g= 5
A获取的私钥 Xa= 94
B获取的私钥 Xb= 142
A计算得到的公钥 Ya为： 3
B计算得到的公钥 Yb为： 72
------X_A与B交换公钥------
A计算得到的key为： 22
B计算得到的key为： 22

素数 q= 173
本原根 g= 2
A获取的私钥 Xa= 169
B获取的私钥 Xb= 131
A计算得到的公钥 Ya为： 65
B计算得到的公钥 Yb为： 26
------X_A与B交换公钥------
A计算得到的key为： 42
B计算得到的key为： 42

素数 q= 179
本原根 g= 2
A获取的私钥 Xa= 145
B获取的私钥 Xb= 175
A计算得到的公钥 Ya为： 103
B计算得到的公钥 Yb为： 112
------X_A与B交换公钥------
A计算得到的key为： 50
B计算得到的key为： 50

素数 q= 181
本原根 g= 2
A获取的私钥 Xa= 64
B获取的私钥 Xb= 113
A计算得到的公钥 Ya为： 44
B计算得到的公钥 Yb为： 18
------X_A与B交换公钥------
A计算得到的key为： 15
B计算得到的key为： 15

素数 q= 191
本原根 g= 19
A获取的私钥 Xa= 20
B获取的私钥 Xb= 42
A计算得到的公钥 Ya为： 30
B计算得到的公钥 Yb为： 9
------X_A与B交换公钥------
A计算得到的key为： 160
B计算得到的key为： 160

素数 q= 193
本原根 g= 5
A获取的私钥 Xa= 120
B获取的私钥 Xb= 146
A计算得到的公钥 Ya为： 150
B计算得到的公钥 Yb为： 95
------X_A与B交换公钥------

A计算得到的key为： 112
B计算得到的key为： 112

素数 q= 197
本原根 g= 2
A获取的私钥 Xa= 131
B获取的私钥 Xb= 52
A计算得到的公钥 Ya为： 21
B计算得到的公钥 Yb为： 85
------X_A与B交换公钥------
A计算得到的key为： 28
B计算得到的key为： 28

素数 q= 199
本原根 g= 3
A获取的私钥 Xa= 82
B获取的私钥 Xb= 87
A计算得到的公钥 Ya为： 35
B计算得到的公钥 Yb为： 147
------X_A与B交换公钥------
A计算得到的key为： 132
B计算得到的key为： 132

素数 q= 211
本原根 g= 2
A获取的私钥 Xa= 81
B获取的私钥 Xb= 185
A计算得到的公钥 Ya为： 86
B计算得到的公钥 Yb为： 168
------X_A与B交换公钥------
A计算得到的key为： 153
B计算得到的key为： 153

素数 q= 223
本原根 g= 3
A获取的私钥 Xa= 184
B获取的私钥 Xb= 215
A计算得到的公钥 Ya为： 162
B计算得到的公钥 Yb为： 140
------X_A与B交换公钥------
A计算得到的key为： 116
B计算得到的key为： 116

素数 q= 227
本原根 g= 2
A获取的私钥 Xa= 147
B获取的私钥 Xb= 96
A计算得到的公钥 Ya为： 204

B计算得到的公钥 Yb为： 144
------X_A与B交换公钥------
A计算得到的key为： 34
B计算得到的key为： 34

素数 q= 229
本原根 g= 6
A获取的私钥 Xa= 166
B获取的私钥 Xb= 207
A计算得到的公钥 Ya为： 58
B计算得到的公钥 Yb为： 115
------X_A与B交换公钥------
A计算得到的key为： 11
B计算得到的key为： 11

素数 q= 233
本原根 g= 3
A获取的私钥 Xa= 71
B获取的私钥 Xb= 183
A计算得到的公钥 Ya为： 156
B计算得到的公钥 Yb为： 93
------X_A与B交换公钥------
A计算得到的key为： 3
B计算得到的key为： 3

素数 q= 239
本原根 g= 7
A获取的私钥 Xa= 219
B获取的私钥 Xb= 148
A计算得到的公钥 Ya为： 191
B计算得到的公钥 Yb为： 9
------X_A与B交换公钥------
A计算得到的key为： 91
B计算得到的key为： 91

素数 q= 241
本原根 g= 7
A获取的私钥 Xa= 8
B获取的私钥 Xb= 17
A计算得到的公钥 Ya为： 81
B计算得到的公钥 Yb为： 137
------X_A与B交换公钥------
A计算得到的key为： 187
B计算得到的key为： 187

素数 q= 251
本原根 g= 6
A获取的私钥 Xa= 189
B获取的私钥 Xb= 94
A计算得到的公钥 Ya为： 170
B计算得到的公钥 Yb为： 83
------X_A与B交换公钥------
A计算得到的key为： 3
B计算得到的key为： 3