作业三： 验证D-H密钥交换机制

教学班： 992987-003

任课教师： 陈欣

小组代号： JOJO

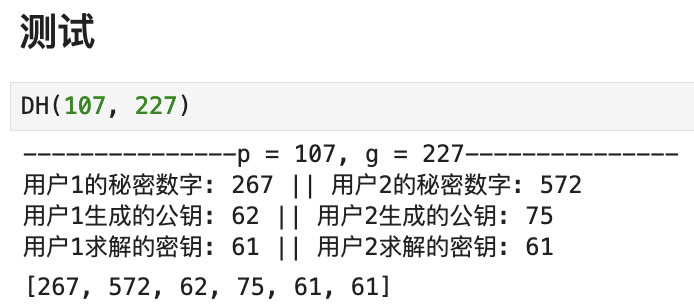
小组成员： 姬舜赢，李建康

实验过程：











全部结果：

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | p | g | 用户1的秘密数字 | 用户2的秘密数字 | 用户1生成的公钥 | 用户2生成的公钥 | 用户1求解的密钥 | 用户2求解的密钥 |
| 0 | 101 | 2 | 303 | 2005 | 8 | 32 | 44 | 44 |
| 1 | 103 | 5 | 1965 | 1798 | 94 | 36 | 93 | 93 |
| 2 | 107 | 2 | 267 | 572 | 103 | 57 | 39 | 39 |
| 3 | 109 | 6 | 1913 | 1694 | 30 | 94 | 20 | 20 |
| 4 | 113 | 3 | 493 | 1834 | 55 | 69 | 44 | 44 |
| 5 | 127 | 3 | 1925 | 1200 | 90 | 100 | 107 | 107 |
| 6 | 131 | 2 | 844 | 1011 | 65 | 93 | 100 | 100 |
| 7 | 137 | 3 | 396 | 3 | 99 | 27 | 65 | 65 |
| 8 | 139 | 2 | 1580 | 1059 | 38 | 84 | 34 | 34 |
| 9 | 149 | 2 | 1687 | 1447 | 87 | 108 | 34 | 34 |
| 10 | 151 | 2 | 2002 | 1004 | 128 | 76 | 105 | 105 |
| 11 | 157 | 2 | 1401 | 807 | 59 | 155 | 98 | 98 |
| 12 | 163 | 6 | 195 | 34 | 38 | 65 | 85 | 85 |
| 13 | 167 | 5 | 1526 | 523 | 28 | 123 | 150 | 150 |
| 14 | 173 | 2 | 1646 | 909 | 56 | 103 | 78 | 78 |
| 15 | 179 | 2 | 295 | 1189 | 104 | 53 | 115 | 115 |
| 16 | 181 | 2 | 925 | 221 | 109 | 78 | 61 | 61 |
| 17 | 191 | 19 | 764 | 1150 | 59 | 52 | 136 | 136 |
| 18 | 193 | 5 | 1668 | 1219 | 143 | 78 | 64 | 64 |
| 19 | 197 | 2 | 108 | 705 | 158 | 126 | 40 | 40 |
| 20 | 199 | 3 | 93 | 137 | 101 | 68 | 76 | 76 |
| 21 | 211 | 2 | 811 | 311 | 116 | 145 | 149 | 149 |
| 22 | 223 | 3 | 130 | 1433 | 38 | 160 | 143 | 143 |
| 23 | 227 | 2 | 1883 | 1082 | 66 | 19 | 160 | 160 |
| 24 | 229 | 6 | 1443 | 1750 | 175 | 178 | 168 | 168 |
| 25 | 233 | 3 | 700 | 710 | 81 | 178 | 16 | 16 |
| 26 | 239 | 7 | 1769 | 1409 | 212 | 191 | 237 | 237 |
| 27 | 241 | 7 | 686 | 2002 | 108 | 12 | 151 | 151 |
| 28 | 251 | 6 | 1591 | 1102 | 55 | 218 | 9 | 9 |