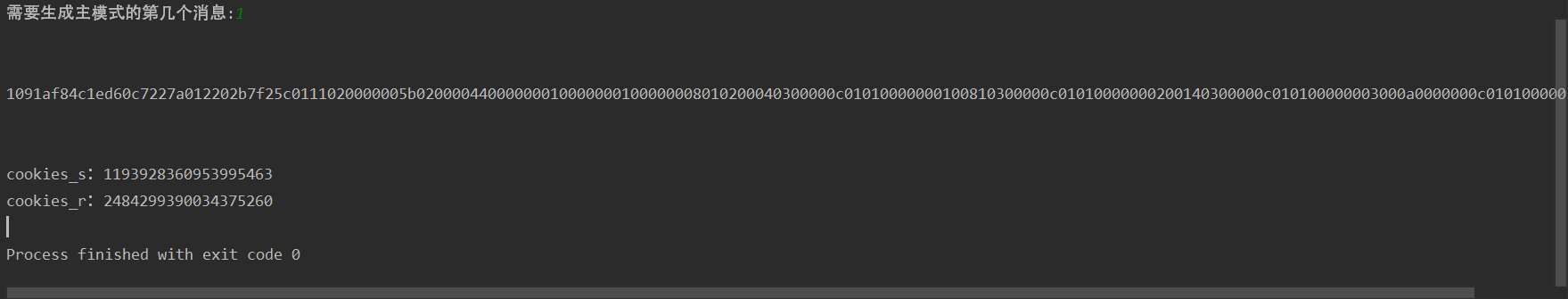
**测试文档**

1.生成主模式的消息一（发送方->响应方），同时得到发送方与响应方cookies



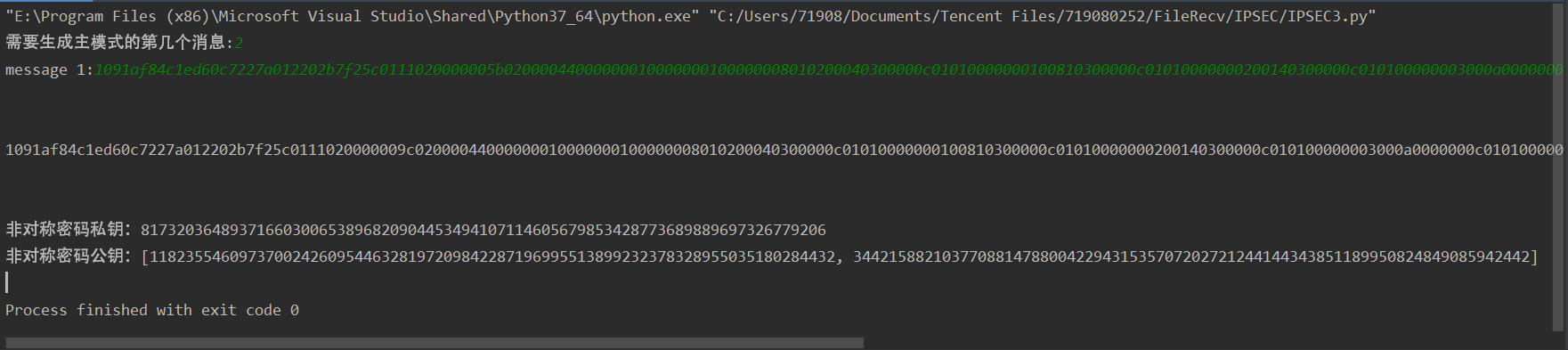
消息一：

1091af84c1ed60c7227a012202b7f25c0111020000005b02000044000000010000000100000008010200040300000c01010000000100810300000c01010000000200140300000c010100000003000a0000000c0101000000140002

发送方cookies cookies\_s: 1193928360953995463

响应方cookies cookies\_r: 2484299390034375260

2.输入消息一生成消息二（响应方->发送方），同时得到响应方的非对称密码私钥和非对称密码公钥



消息二：

1091af84c1ed60c7227a012202b7f25c0111020000009c02000044000000010000000100000008010200040300000c01010000000100810300000c01010000000200140300000c010100000003000a0000000c0101000000140002051a23e50ed072c1814db24175e3caa5244e020e7b8f431218d087110b88a73a10079c315eb4d407bf415fa6a1606cc0df650dc5dcf9503a37c0dbaec37715caaa

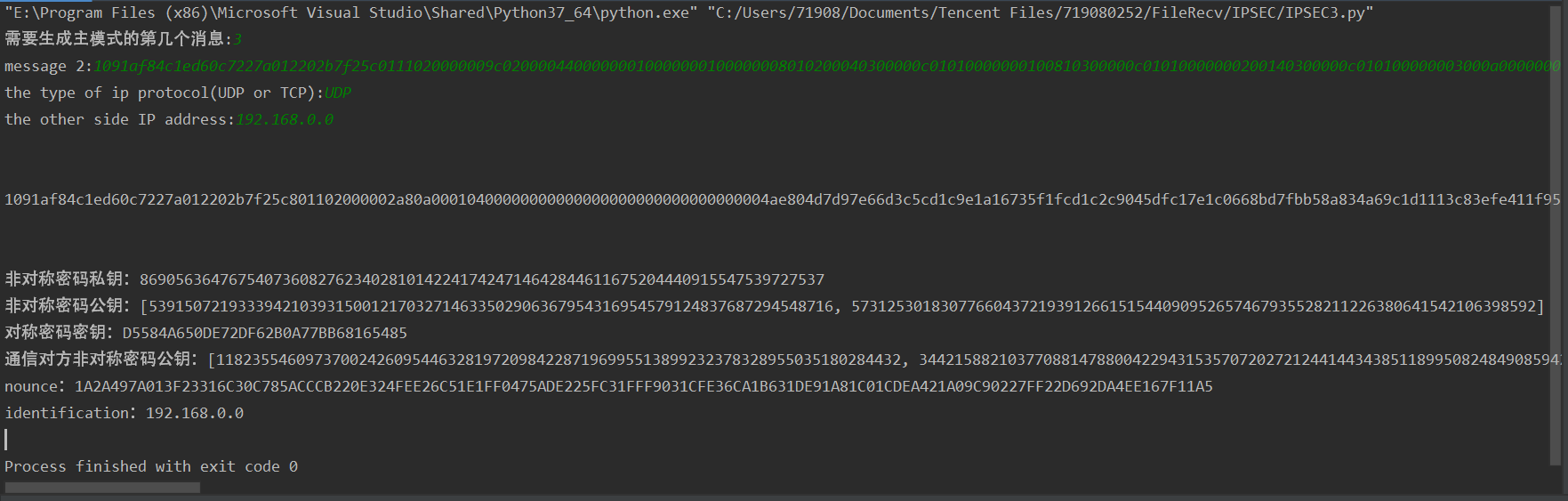
响应方的非对称密码私钥：

81732036489371660300653896820904453494107114605679853428773689889697326779206

响应方的非对称密码公钥：

[11823554609737002426095446328197209842287196995513899232378328955035180284432, 3442158821037708814788004229431535707202721244144343851189950824849085942442]

3.输入消息二，选择UDP协议，假设响应方IP地址为192.168.0.0，生成消息三（发送方->响应方），同时得到发送方的非对称密码私钥、非对称密码公钥，对称密码密钥，发送方还得到了通信对方，即响应方的非对称密码公钥，此外还生成了nonce



消息三：



发送方的非对称密码私钥：

86905636476754073608276234028101422417424714642844611675204440915547539727537

发送方的非对称密码公钥：

[53915072193339421039315001217032714633502906367954316954579124837687294548716, 57312530183077660437219391266151544090952657467935528211226380641542106398592]

对称密码密钥：D5584A650DE72DF62B0A77BB68165485

响应方的非对称密码公钥：

[11823554609737002426095446328197209842287196995513899232378328955035180284432, 3442158821037708814788004229431535707202721244144343851189950824849085942442]

nonce：

1A2A497A013F23316C30C785ACCCB220E324FEE26C51E1FF0475ADE225FC31FFF9031CFE36CA1B631DE91A81C01CDEA421A09C90227FF22D692DA4EE167F11A5

4.输入消息三和响应方的非对称密码私钥，选择UDP协议，假设发送方IP地址为192.168.3.0，再输入响应方的非对称密码公钥，生成消息四（响应方->发送方），同时得到响应方的非对称密码私钥、非对称密码公钥，对称密码密钥，响应方还得到了发生方的非对称密码公钥，生成了nonce



消息四：



响应方的非对称密码私钥：

81732036489371660300653896820904453494107114605679853428773689889697326779206

响应方的非对称密码公钥：

[11823554609737002426095446328197209842287196995513899232378328955035180284432, 3442158821037708814788004229431535707202721244144343851189950824849085942442]

对称密码密钥：D5584A650DE72DF62B0A77BB68165485

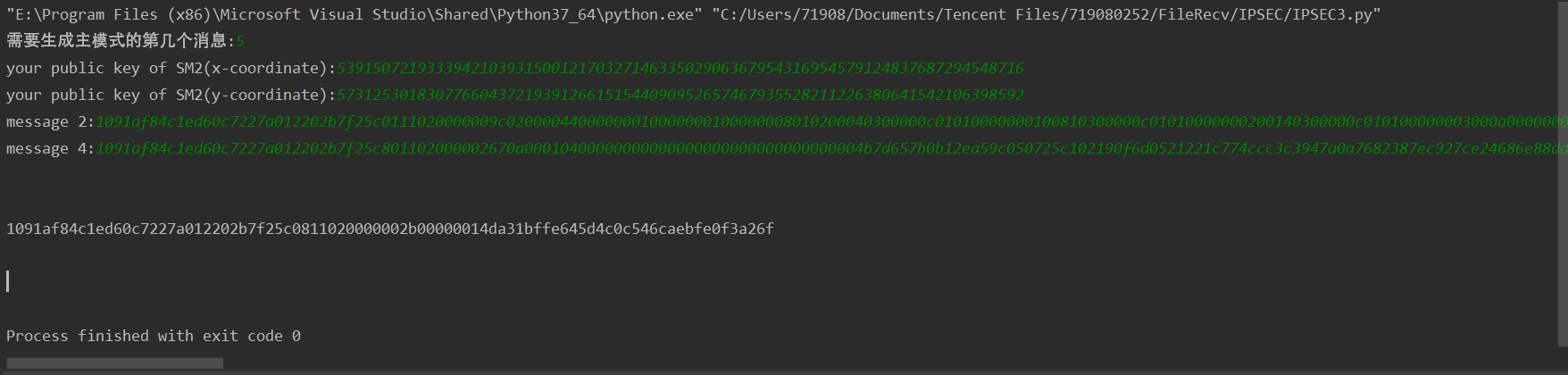
发送方的非对称密码公钥：

[53915072193339421039315001217032714633502906367954316954579124837687294548716, 57312530183077660437219391266151544090952657467935528211226380641542106398592]

nonce：

77483D689D91E98074A359D36125EF0D43A145E49645FA4528D8A45916D240A7B2B8D726DD7BB399858AB30B7FA2BB3CEDF23175D2FE73876E03B8D1664B97BD

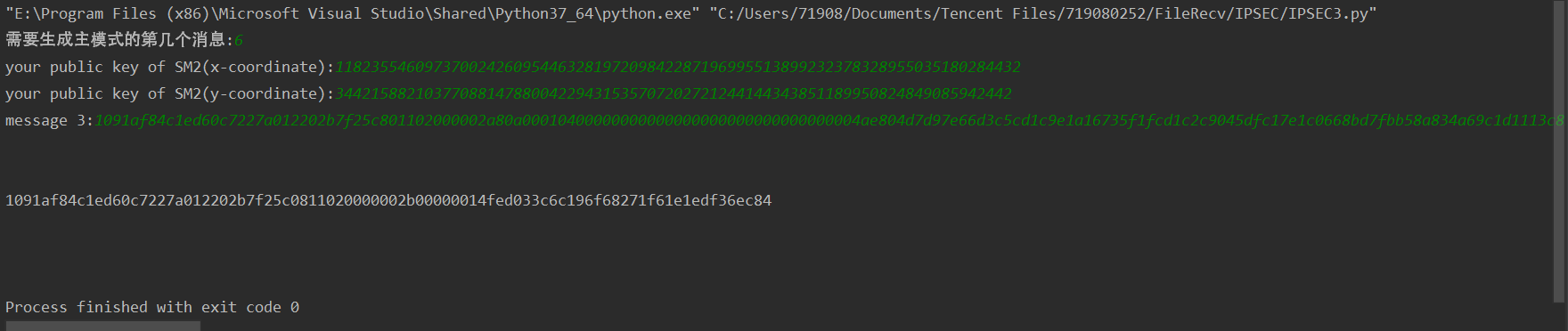
5.输入发送方的非对称密码公钥，再输入消息二和消息四，生成消息五（发送方->响应方）



消息五：

1091af84c1ed60c7227a012202b7f25c0811020000002b00000014da31bffe645d4c0c546caebfe0f3a26f

6.输入响应方的非对称密码公钥和消息三，生成消息六（响应方->发送方）



消息六：

1091af84c1ed60c7227a012202b7f25c0811020000002b00000014fed033c6c196f68271f61e1edf36ec84