基于口令的身份验证协议

> 沙之洲 2020012408

0 代码说明

首先启动 server

```
python server.py
```

server 会在本机的 2333 端口等待 client 的连接

接下来，在另一个窗口中启动 client

```
python client.py
```

即可复现实验结果

1 实现原理及细节

双方共享 password 为 `123456789101112131415`

首先由 client 依据 RSA 产生一对 public key 和 private key 。将自己的身份标识 A 和用 password 加密后的公钥发给 server，这里选择的加密方法是 DES

第二步，server 收到之后，用 password 解密得到 client 的 public key。接下来，随机生成会话秘钥 K_s ，先用 public key 加密之后，再用 DES 和 password 加密发回给 client

第三步，client 解密得到 K_s ，并且产生随机数 N_A 用会话秘钥加密发送给 server

第四步，server 解密得到 N_A 再产生一个 N_B ，将二者拼接之后用 K_s 加密，发回给 client

第五步，client 将 N_B 回复给 server。双方身份认证成功，可以开始通信

2 实验结果

client的输出如下

```
(x) PS D:\2023Spring\cyberSecurity\exp\authentication> python .\client.py
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAsky2+wvtBirPSg1ZLk/pDLx1h8V5gz9SjJ+NZRhN2h5+a8C5
TRJbhpjy69NN3hWUkbR8z2x4duF5kiFm06aJF0QqDnQ1X6a0nRU8SxxED6BTrR12
Qkg33Al9fs1LqgF+yEggWTOTH4bye+wz/HY0EWPGZ7TWy3Sqh7vJ5A/hFqiJyvP4
qf6fQQzqoGBQi3PuCedlS+gIXKJzmhPD9A3qbBTvHzg+7Jryew5oXBb/0WMc4/37
4H3ud36PlvmMqEbDSKQwtJQ+QR2ZXsTpBKRG3ccShUkvDZfze79Lgc9bpTXZ34Im
1DVuXSWMzfNXRsMhlGuTAKSAjOnBBGchMZRACQIDAQABAoIBACkOHhIXcGf7ooiA
I1lVICoFGSD+uRieE5F6ybGOE5sWa3C/S0uyXu3SuRjRKnxpRrD4OMcASIrDJ12d
IFK65ZU8Zly2qHWSasNC2QPIiel5NttFTe48N9SMQN/aQMJwHrPaW8x+YjGfvqUH
Qf8vbpTUfyJxEwZ9Iikn9fh0KZWwLRPBOSpfBEKX+vvlAhvc0wMXdT486JTl2+wQ
oN4Saf8cuhdOYX48fSMQ4XFSU0tEsl1JQh2lrkDvqk9IL2iYCOXJs97NxZT50pl2
wH3SFKGJ5GeVqBEOHEqh8frCpaUyUPjqjpPAJ16wU8u9R14rA0ByVUEIuI6JpzZj
e9WI7nMCgYEAvWgy3eHatsaW3hvlNlrjQfJUEc98xHf9IgaWCops0i8MXhvCnMgW
GMxtoADu83mjB3kIJl8tfhwLesuFUxTBEM36vLKg0sxN2o8/jGOrjjwhbS2ZZ/Xo
6EY6eKGmU2u6pNF6BZOOMozwT9PYzrUCcjeDREKUWS64uaArFTO+nhcCgYEA8PzJ
```

```
Aucl36406cBSl2n7Y21Hm9O2/Q2u90bAjmvwrFHJF01u0S7GMMaoX8AspMHPtsqJ
AEhCGOVNjU9k4KCrqdjp+WgKKZAMoQZgqQjrT86Rc2iQqZ81a7TZVoppeQGGb0w/
dYjXSqA2at9vOdsXaG+RFzQZ6krBXZHOTQhMBt8CgYEAh0Xh/mIN6LgQi/TOUUu8
Px8pN8cuXssreJ+njUOr0LlVZekBpyOn1HI8YSgJgM6AxxeD4JPdU9IHyN2ODPYn
pS7XQul4vtS3Tb89LbEJl34OiYElrQAOJcXygLFCrxWjqY8KTO1Dg4rxHrI4h/jz
FEvdbmT2unMJ71kbK/tWymUCgYAcpgCDftUqzTvvGfT3mRrQjBo6NSYI2UqWjOux
QrW+1o4wXf0xkvzuqX80utTT1VKLKXK1/OEWspPQm8KjTZZ6v5W5F5w1qrFFp0tw
bOYEe8sgzCp+b7XbEwnPVu8I+pxvuMHGiDkH3xn5BIzldN1IhhLajlASYUaxh/bd
g4H+QwKBgQCIt2yVAcyHewWgBAFZjh+Ir91eGFgiDEw/5fmC5VIB81vgRlKOVJBT
EQvfzUOw5c32NQ+5E42vKA7LZZHykFTwfmRwK4CUmNR/Mm9A1cwNE7UE1Vqe6R8F
2SvkUTVQoUA/k6Pc/79ep2OwYnvjSPOalqb8AvDeQPkVCNuSJdaUXQ==
-----END RSA PRIVATE KEY-----
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsky2+wvtBirPSg1ZLk/p
DLx1h8V5gz9SjJ+NZRhN2h5+a8C5TRJbhpjy69NN3hWUkbR8z2x4duF5kiFm06aJ
FOQqDnQ1X6a0nRU8SxxED6BTrR12Qkg33Al9fs1LqgF+yEggWTOTH4bye+wz/HY0
EWPGZ7TWy3Sqh7vJ5A/hFqiJyvP4qf6fQQzqoGBQi3PuCedlS+gIXKJzmhPD9A3q
bBTvHzg+7Jryew5oXBb/0WMc4/374H3ud36PlvmMqEbDSKQwtJQ+QR2ZXsTpBKRG
3ccShUkvDZfze79Lgc9bpTXZ34Im1DVuXSWMzfNXRsMhlGuTAKSAjOnBBGchMZRA
CQIDAQAB
-----END PUBLIC KEY-----
connect to server
Ks is b'8rAgIfGsLD6pjViz'
NA is b'73QT9nlIZiytarEj'
pass test, session key is b'8rAgIfGsLD6pjViz'
NB is b'VjNg5pnRLAef0kdr'
input msg send to server: 666
data revieved from server: 666
```

server 的输出如下

```
(x) PS D:\2023Spring\cyberSecurity\exp\authentication> python .\server.py
wait for client
client connected
client name A
client pub key b'-----BEGIN PUBLIC KEY-----
\nMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsky2+wvtBirPSg1ZLk/p\nDLx1h8V5gz9S
jJ+NZRhN2h5+a8C5TRJbhpjy69NN3hWUkbR8z2x4duF5kiFm06aJ\nFOQqDnQ1X6a0nRU8SxxED6BTrR
12Qkg33Al9fs1LqgF+yEggWTOTH4bye+wz/HY0\nEWPGZ7TWy3Sqh7vJ5A/hFqiJyvP4qf6fQQzqoGBQ
i3PuCedlS+gIXKJzmhPD9A3q\nbBTvHzg+7Jryew5oXBb/0WMc4/374H3ud36PlvmMqEbDSKQwtJQ+QR
2ZXsTpBKRG\n3ccShUkvDZfze79Lgc9bpTXZ34Im1DVuXSWMzfNXRsMhlGuTAKSAjOnBBGchMZRA\nCQ
IDAQAB\n-----END PUBLIC KEY-----'
Ks is b'8rAgIfGsLD6pjViz'
NA is b'73QT9nlIZiytarEj'
NB is b'VjNg5pnRLAef0kdr'
pass test, session key is b'8rAgIfGsLD6pjViz'
msg recieved from client 666
```

最后，server 和 client 通过互相发送 `666` 说明双方的会话被成功构建