

IKE_D-H

0. 概述

本仓库为信息安全导论课程作业：验证D-H密钥交换机制。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，通过socket套接字在主机间交换公钥，实现密钥交换。

1. 验证素数及原根

1. **原根定理**：如果 (n) 是素数，那么存在一个模 (n) 的原根。
2. **找到原根的方法**：
 - 计算 $(n-1)$ 的所有素因子。
 - 对于每个素因子 (p) ，找到模 (n) 的一个原根 (g) ，使得 $(g^{(n-1)/p} \not\equiv 1 \pmod{n})$ 。

如：测试素数6的原根251（部分截图）：

```
6^241 mod 251 = 191
6^242 mod 251 = 142
6^243 mod 251 = 99
6^244 mod 251 = 92
6^245 mod 251 = 50
6^246 mod 251 = 49
6^247 mod 251 = 43
6^248 mod 251 = 7
6^249 mod 251 = 42
6^250 mod 251 = 1
Primitive Root Group
```

2. 按照D-H协议机制流程进行计算

代码详见：[服务端](#) [客户端](#)

2.1 选择素数及原根

选用素数 $p = 2$ 及其原根 $g = 101$

2.2 构建单向函数f

```
1 def f(g, x, p):
2     return pow(g, x) % p
```

2.3 选择私密整数并计算公开的数

```
1 privateKey = input("输入你的私钥：")
2 privateKey = int(privateKey)
3 publicKey = f(g, privateKey, p)
```

2.4 相互交换公开的数

服务端：

```
1 # 启动服务端
2 server_socket = socket(AF_INET, SOCK_STREAM)
3 host = gethostbyname(gethostname())
4 print(host)
5 server_socket.bind((host, 12345))
6 server_socket.listen(1)
7 print('等待连接...')
8 conn, addr = server_socket.accept()
9 print('连接来自: ', addr)
10
11 # 发送公钥给客户端
12 print(f"发送公钥: {publicKey}")
13 conn.send(str(publicKey).encode())
14
15 # 接收客户端消息并打印
16 counter_publicKey = conn.recv(1024)
17 print(f"对方公钥: {int(counter_publicKey.decode())}")
```

客户端：

```
1 privateKey = input("输入你的私钥: ")
2 privateKey = int(privateKey) # 连接到服务端
3 host = 'localhost'
4 conn = socket(AF_INET, SOCK_STREAM)
5 conn.connect((host, 12345))
6 print('连接到: ', host)
7
8 # 发送公钥给服务端
9 print(f"发送公钥: {publicKey}")
10 conn.send(str(publicKey).encode())
11
12 # 接收服务端消息并打印
13 counter_publicKey = conn.recv(1024)
14 print(f"对方公钥: {counter_publicKey.decode()}")
```

2.5 各自计算会话密钥

```
1 ks = f(int(counter_publicKey), privateKey, p)
2 print(f"会话密钥: {ks}")
```

3. 测试结果

服务端：

```
Input your private key:11
10.234.112.64
等待连接...
连接来自: ('10.234.107.185', 63824)
发送公钥: 28
对方公钥: 8
会话密钥: 35
(venv) PS D:\JetBrains\PycharmProjects\IKE_D-H>
```

客户端：

```
(base) PS D:\Code\IKE_D-H> & 'C:\Users\Max\AppData\Local\Programs\Python\Python310\python.exe' 'c:\Users\Max\.vscode\extensions\ms-python.python-2023.14.0\pythonFiles\lib\python\debugpy\adapter\..\..\debugpy\launcher' '54584' '--' 'D:\Code\IKE_D-H\D-H_client.py'
Input your private key:3
连接到: 10.234.112.64
发送公钥: 8
对方公钥: 28
会话密钥: 35
```

由图可见，通过迪菲-赫尔曼密钥交换机制，通信双方可以在不直接传递密钥的情况下协商一个共享的密钥。