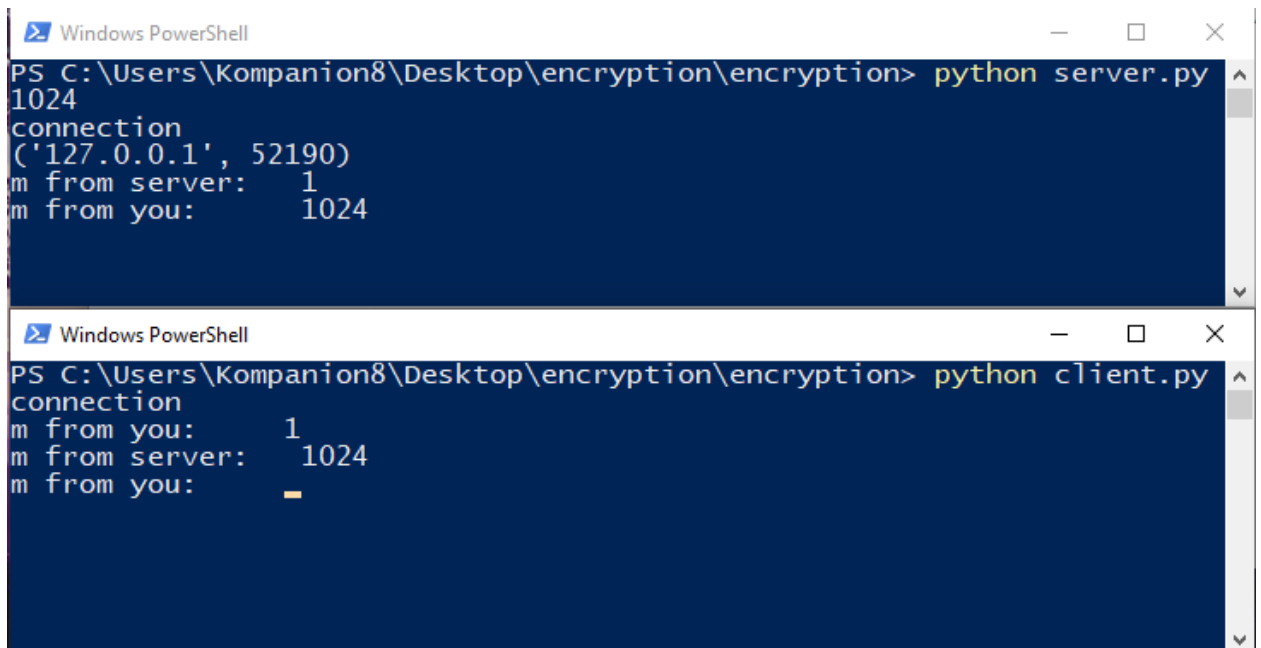


## Протокол шифрования Диффи Хеллмана

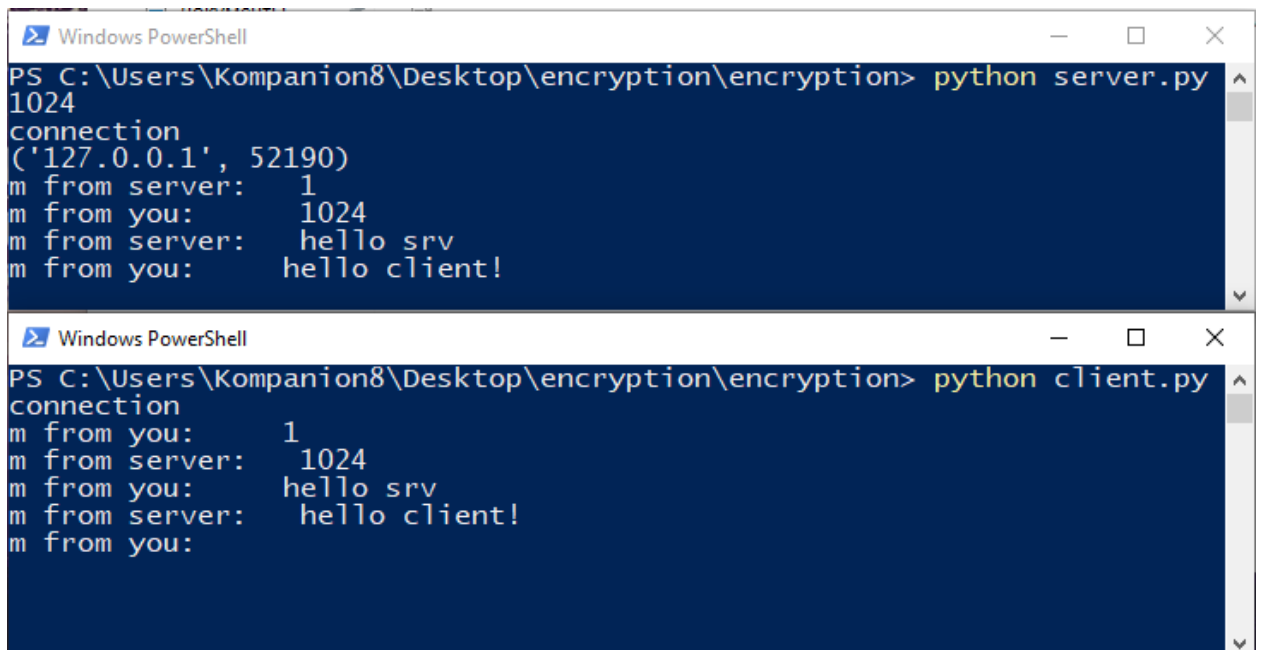
Пишем на сервер с клиента



```
Windows PowerShell
PS C:\Users\Kompanion8\Desktop\encryption\encryption> python server.py
1024
connection
('127.0.0.1', 52190)
m from server: 1
m from you: 1024

Windows PowerShell
PS C:\Users\Kompanion8\Desktop\encryption\encryption> python client.py
connection
m from you: 1
m from server: 1024
m from you: _
```

При первой отправке сообщения сервер ждёт клиента, после чего отправляет ему отладочное сообщение с цифрой 1024. После клиент и сервер поочередно отправляют друг другу сообщения.



```
Windows PowerShell
PS C:\Users\Kompanion8\Desktop\encryption\encryption> python server.py
1024
connection
('127.0.0.1', 52190)
m from server: 1
m from you: 1024
m from server: hello srv
m from you: hello client!

Windows PowerShell
PS C:\Users\Kompanion8\Desktop\encryption\encryption> python client.py
connection
m from you: 1
m from server: 1024
m from you: hello srv
m from server: hello client!
m from you:
```

При несоответствии ключа дешифровка сообщения будет некорректной у обеих сторон. Ключ не передаётся вместе с сообщением, так что стороннее приложение не сможет прочитать сообщение.