

Nome: Felipe Panizio  
RA: 1997165

Primeiro passo:

Foi instalado a biblioteca CRYPTOGRAPHY e a importação da mesma

Figura 1

```
import socket
import sys
import time
import threading
import select
import traceback
from cryptography.fernet import Fernet
```

Segundo passo:

Foi gerada a chave de criptografia em um arquivo chamado KEY.  
Este arquivo serve somente para leitura dela.

Figura 2

```
file = open('key', 'rb')
key = file.read()
file.close()
f = Fernet(key)
```

Terceiro passo:

Após a realização do encode da mensagem é realizada a criptografia e enviada para o servidor.

Figura 3

```
data = msg.encode()
data = f.encrypt(data)
self.client(host, port, data)
```

Quarto passo:

O servidor recebe a mensagem e envia para todos os usuários conectados no servidor.  
Ao receber a mensagem ela é descriptografada e é realizado um decode na mesma.

Figura 4

```
chunk = s
chunk = f.decrypt(chunk)
print(chunk.decode() + '\n>>')
```

Problemas encontrados:

De vez em quando algumas mensagens enviadas pelo usuário 1 não são recebidas nos demais usuários.

Permite a entrada de múltiplos usuários na aplicação, não podendo assim ter um chat privado.

Após os usuários se desconectarem da aplicação ela entra em loop, tentando reconectar o usuário.