CN ASSIGNMENT 2

SOCKET PROGRAMMING

Topic: Encryption and Decryption

Team Details

Name: Naren Chandrashekhar **SRN: PES2UG20CS216**

Name: Navtej Reddy **SRN: PES2UG20CS218**

Name: Nitin Jayachandran **SRN: PES2UG20CS231**

Section: D

Abstract:

Our project is encryption/decryption using socket programming in Python. Socket programming is about the connection between client and server or many clients for data communication, networking and data transfer. The network formed between the nodes is known as sockets.

In our project, we have used Caeser Cipher to encrypt and decrypt our messages. We have a client and server in our project and the server shows which client is connected for encryption/decryption. The server also shows the messages sent and received from the client. We have set the key value of encryption as 5, which means if we want to encrypt the letter 'a' the output will be 'f'. The same way, a message can be decrypted, where 'f' gives the output 'a'.

Code:

Server.py:

client.py server.py

D: > PES > Semester_4 > Computer Networks > Project > Socket_Programming > server.py

```python
import socket

import math

def encypt_func(txt, s):
    result = ""

#caeser encryption
# transverse the plain txt
    for i in range(len(txt)):
        char = txt[i]
        # encypt_func uppercase characters in plain txt

        if (char.isupper()):
            result += chr((ord(char) + s - 64) % 26 + 65)
        # encypt_func lowercase characters in plain txt
        else:
            result += chr((ord(char) + s - 96) % 26 + 97)
    return result

#caeser decryption
def decypt_func(msg):
    key = 5
    LETTERS = "ABCDEFGHIJKLMNOPQRSTUVWXYZ"
    LETTERS = LETTERS.lower()
    message = str(msg)
    translated = ''
    for symbol in message:
        if symbol in LETTERS:
            num = LETTERS.find(symbol)
```

```python
            num = num - key
            if num < 0:
                num = num + len(LETTERS)
            translated = translated + LETTERS[num]
        else:
            translated = translated + symbol
    return translated

# take the server name and port name
host = 'localhost'
port = 5000

# create a socket at server side
# using TCP / IP protocol
s = socket.socket(socket.AF_INET,
                  socket.SOCK_STREAM)

# bind the socket with server
# and port number
s.bind(('', port))

# allow maximum 1 connection to
# the socket
s.listen(1)
c, addr = s.accept()

# display client address
print("CONNECTION FROM:", str(addr))
while True:
    # wait till a client accept
    # connection

    # send message to the client after
    # encoding into binary string
    c.send(b"enter e to encrypt and d to decrypt and f to disconnect")
    while True:
        msg1 = c.recv(1024)
        print(msg1)
        msg_str = msg1.decode()
        if(msg_str == "f"):
            print("disconnecting ",str(addr))
            c.send(b"ack")
            c.close()
            exit(0)

        if(msg_str == "e"):
            c.send(b"enter message to encrypt")

            msg2 = c.recv(1024)
            msg2_str = msg2.decode()
            print(msg2_str)
            print(encypt_func(msg2_str,4)) #s=4,shift =s+1 =5
            answer =encypt_func(msg2_str,4)
            c.send(answer.encode())
            break

        if(msg_str == "d"):
            c.send(b"enter message to decrypt")
            msg2 = c.recv(1024)
            msg2_str = msg2.decode()
```

```python
            print(msg2_str)
            print(decypt_func(msg2_str))
            answer = decypt_func(msg2_str)

            c.send(answer.encode())
            break

        #c.send(b"connection end")
        #c.close() #added this line and below
        #break
#        if int(msg) == 3+4:
#            c.send("Correct answer".encode())
#            c.close()
#            break

#        else:
#            c.send("Wrong answer try again.".encode())


# disconnect the server
c.close()
exit(0)

```

Client.py:

client.py server.py

D: > PES > Semester_4 > Computer Networks > Project > Socket_Programming > client.py

```python
import socket

# take the server name and port name

host = 'localhost'
port = 5000

# create a socket at client side
# using TCP / IP protocol
s = socket.socket(socket.AF_INET,
                  socket.SOCK_STREAM)

# connect it to server and port
# number on local computer.
s.connect(('127.0.0.1', port))

# receive message string from
# server, at a time 1024 B


msg = s.recv(1024)

# repeat as long as message
# string are not empty
while msg:
    if(msg.decode() == "ack"):
        print("disconnecting from client")
        exit(0)
    print('Server says :' + msg.decode())
    if(msg.decode() == "enter e to encrypt and d to decrypt and f to disconnect"):
```

```python
            ans = str(input("Your answer : "))
            s.send(ans.encode())
        if(msg.decode() == "enter message to encrypt"):
            ans = str(input("message to encrypt : "))
            s.send(ans.encode())
        if(msg.decode() == "enter message to decrypt"):
            ans = str(input("message to decrypt : "))
            s.send(ans.encode())
        msg = s.recv(1024)


# disconnect the client
s.close()
```

Output Screenshots:

Running Server file on terminal:

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19043.1586]
(c) Microsoft Corporation. All rights reserved.

D:\PES\Semester_4\Computer Networks\Project\Socket_Programming>python server.py
CONNECTION FROM: ('127.0.0.1', 59769)
b'e'
naren
sfwjs
b'e'
sfwjs
xkbox
b'd'
sfwjs
naren
b'f'
disconnecting  ('127.0.0.1', 59769)

D:\PES\Semester_4\Computer Networks\Project\Socket_Programming>
```

Running Client file on terminal:

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.19043.1586]
(c) Microsoft Corporation. All rights reserved.

D:\PES\Semester_4\Computer Networks\Project\Socket_Programming>python client.py
Server says :enter e to encrypt and d to decrypt and f to disconnect
Your answer : e
Server says :enter message to encrypt
message to encrypt : naren
Server says :sfwjs
Server says :enter e to encrypt and d to decrypt and f to disconnect
Your answer : e
Server says :enter message to encrypt
message to encrypt : sfwjs
Server says :xkbox
Server says :enter e to encrypt and d to decrypt and f to disconnect
Your answer : d
Server says :enter message to decrypt
message to decrypt : sfwjs
Server says :naren
Server says :enter e to encrypt and d to decrypt and f to disconnect
Your answer : f
disconnecting from client

D:\PES\Semester_4\Computer Networks\Project\Socket_Programming>
```

Wireshark Output: Following the TCP stream on port 5000