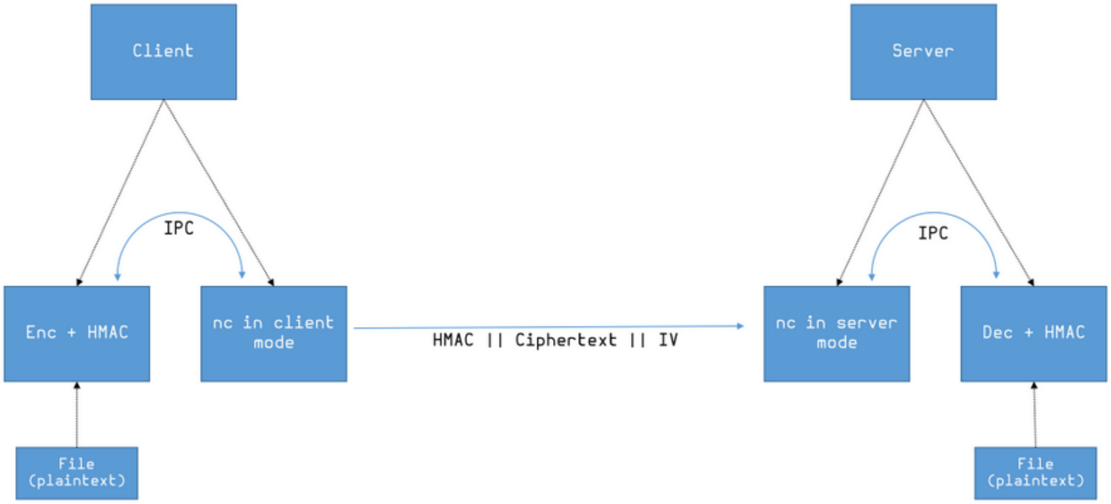
CSE 554 Networks and Systems Security II
Assignment 3

Name: Harsh Kumar **Roll No:** 2019043

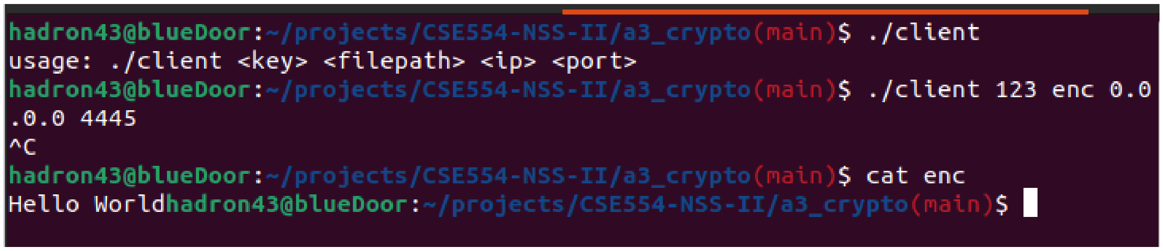


Assumptions:

- The file size is smaller than the buffer size (around 900 bytes)
- Key is preshared and static.

Client-Side

The client-side is implemented in *client.cpp* file. For all cryptographic functions, I've implemented a C++ wrapper over standard EVP functions from *libcrypto* library. The client-side forks, and creates processes. One of the processes reads from a plain text file, encrypts it, and sends it to the other processes via a pipe. The other process just repaces the *STDIN* file descriptor with the read end of the pipe. It gets the message from the peer process and transmits it to the server.

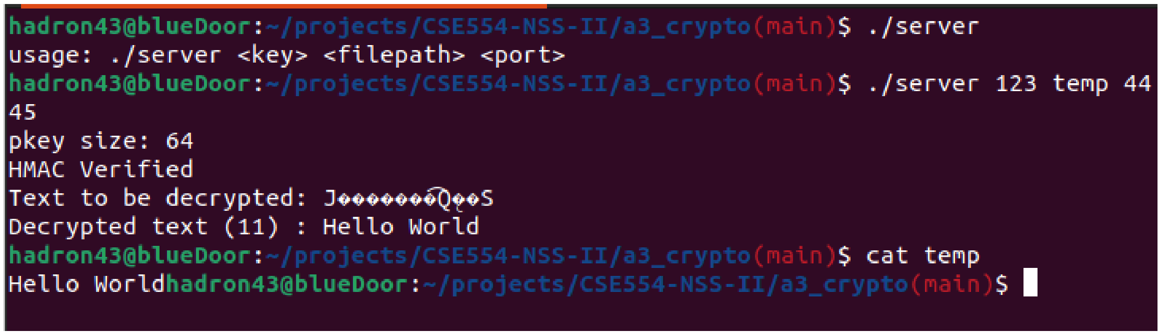


```
hadron43@blueDoor:~/projects/CSE554-NSS-II/a3_crypto(main)$ ./client
usage: ./client <key> <filepath> <ip> <port>
hadron43@blueDoor:~/projects/CSE554-NSS-II/a3_crypto(main)$ ./client 123 enc 0.0
.0.0 4445
^C
hadron43@blueDoor:~/projects/CSE554-NSS-II/a3_crypto(main)$ cat enc
Hello Worldhadron43@blueDoor:~/projects/CSE554-NSS-II/a3_crypto(main)$ 
```

We send a file enc to the server listening on port 4445, after encryption and HMAC calculation.

Server Side

The server-side is implemented in *server.cpp* file. The server side forks, and creates two processes. One of the processes starts listening to incoming connections through netcat. When it received a message, it passes it to the other peer process with the help of a pipe. The IV, HMAC, and payload are extracted from the incoming message. HMAC is verified. If verification is successful, packet is decrypted and stored in a file.



```
hadron43@blueDoor:~/projects/CSE554-NSS-II/a3_crypto(main)$ ./server
usage: ./server <key> <filepath> <port>
hadron43@blueDoor:~/projects/CSE554-NSS-II/a3_crypto(main)$ ./server 123 temp 44
45
pkey size: 64
HMAC Verified
Text to be decrypted: J�������Q��S
Decrypted text (11) : Hello World
hadron43@blueDoor:~/projects/CSE554-NSS-II/a3_crypto(main)$ cat temp
Hello Worldhadron43@blueDoor:~/projects/CSE554-NSS-II/a3_crypto(main)$ █
```

We receive a file from client and store it in temp file. HMAC is successfully verified, then only the message is decrypted.