NSSII Assignment 2

Manavjeet Singh, 2018295

Part 1, IRC client

Dependencies

The application is dependent on following python modules

- socket
- pickle
- cryptography
- threading
- os
- time
- random
- base64

Running

- Use “make server” to run the server
- Use “make c0” to run the client 0
- Use “make c1” to run the client 1
- Use “make c2” to run the client 2
- Use “make c3” to run the client 3

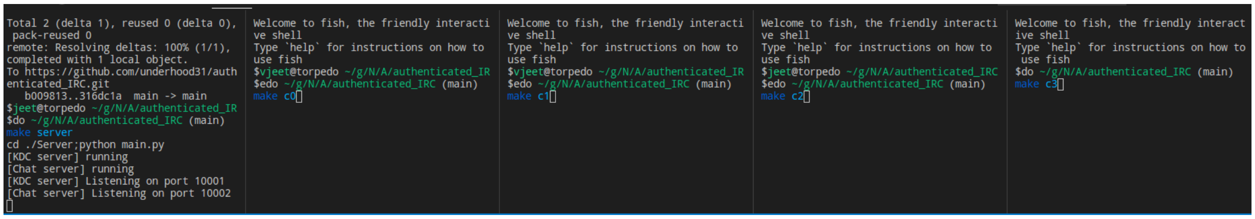
Configure

The server and clients are preconfigured.
But if you want to configure again, run “python configure.py” and enter the relevant details and follow the following steps:

- Move “all_client_listening.info” and “ all_client_secrets.info” files generated in root folder to the Server folder.
- Move the respective client config info files to the client folders.

Test Run

Run the programs as instructed in Running section and do the following:



```
Total 2 (delta 1), reused 0 (delta 0),
 pack-reused 0
remote: Resolving deltas: 100% (1/1),
completed with 1 local object.
To https://github.com/underhood31/auth
enticated_IRC.git
   b009813..316dc1a  main -> main
$jeet@torpedo ~/g/N/A/authenticated_IR
$do ~/g/N/A/authenticated_IRC (main)
make server
cd ./Server;python main.py
[KDC server] running
[Chat server] running
[KDC server] Listening on port 10001
[Chat server] Listening on port 10002
```

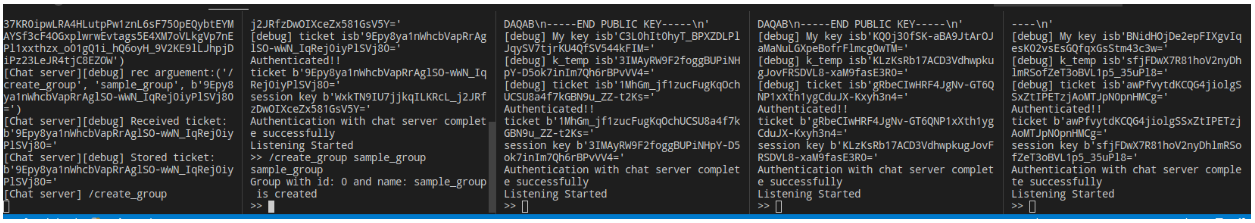
```
Welcome to fish, the friendly interacti
ve shell
Type `help` for instructions on how to
use fish
$vjeet@torpedo ~/g/N/A/authenticated_IR
$edo ~/g/N/A/authenticated_IRC (main)
make c0
```

```
Welcome to fish, the friendly interacti
ve shell
Type `help` for instructions on how to
use fish
$vjeet@torpedo ~/g/N/A/authenticated_IR
$edo ~/g/N/A/authenticated_IRC (main)
make c1
```

```
Welcome to fish, the friendly interacti
ve shell
Type `help` for instructions on how to
use fish
$jeet@torpedo ~/g/N/A/authenticated_IRC
$edo ~/g/N/A/authenticated_IRC (main)
make c2
```

```
Welcome to fish, the friendly interact
ive shell
Type `help` for instructions on how to
 use fish
$do ~/g/N/A/authenticated_IRC (main)
make c3
```

- Run “/create_group sample_group” on client0. A group id will be returned. Following steps are assuming that the group id is 0.



```
37KR0ipwLRA4HLutpPw1znL6sF750pEQybtEYM
AYSf3cF4OGxplwrwEvtags5E4XM7oVLkgVp7nE
Pl1xxthzx_o01gQ1i_hQ6oyH_9V2KE9lLJhpjD
iPz23LeJR4tjC8EZOW')
[Chat server][debug] rec arguement:('/
create_group', 'sample_group', b'9Epy8
ya1nWhcbVapRrAglSO-wWN_IqRej0iyPlSVj80
=')
[Chat server][debug] Received ticket:
b'9Epy8ya1nWhcbVapRrAglSO-wWN_IqRej0iy
PlSVj80='
[Chat server][debug] Stored ticket:
b'9Epy8ya1nWhcbVapRrAglSO-wWN_IqRej0iy
PlSVj80='
[Chat server] /create_group
```

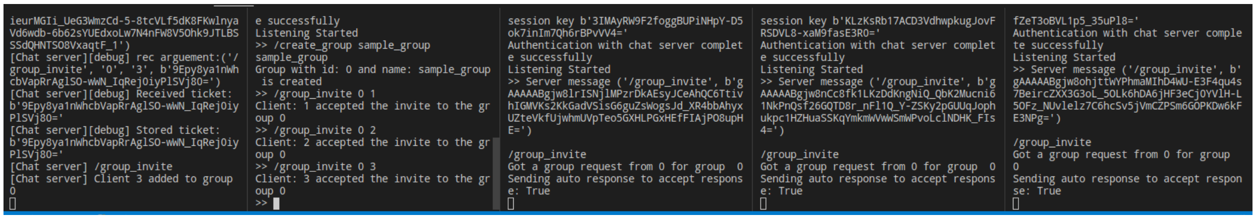
```
j2JRfzDwOIXceZx581GsV5Y='
[debug] ticket isb'9Epy8ya1nWhcbVapRrAg
lSO-wWN_IqRej0iyPlSVj80='
Authenticated!!
ticket b'9Epy8ya1nWhcbVapRrAglSO-wWN_Iq
Rej0iyPlSVj80='
session key b'WxkTN9IU7jjkqILKRcL_j2JRf
zDwOIXceZx581GsV5Y='
Authentication with chat server complet
e successfully
Listening Started
>> /create_group sample_group
sample_group
Group with id: 0 and name: sample_group
 is created
>>
```

```
DAQAB\n-----END PUBLIC KEY-----\n'
[debug] My key isb'C3L0hIt0hyT_BPXZDLPl
JqySV7tjrKU4QfSV544kFIM='
[debug] k_temp isb'3IMAyRW9F2foggBUPiNH
pY-D5ok7inIm7Qh6rBPvVV4='
[debug] ticket isb'1MhGm_jf1zucFugKqOch
UCSU8a4f7kGBN9u_ZZ-t2Ks='
Authenticated!!
ticket b'1MhGm_jf1zucFugKqOchUCSU8a4f7k
GBN9u_ZZ-t2Ks='
session key b'3IMAyRW9F2foggBUPiNHpY-D5
ok7inIm7Qh6rBPvVV4='
Authentication with chat server complet
e successfully
Listening Started
>>
```

```
DAQAB\n-----END PUBLIC KEY-----\n'
[debug] My key isb'KQ0j30fSK-aBA9JtArOJ
aMaNuLGXpeBofrFlmcg0wTM='
[debug] k_temp isb'KLzKsRb17ACD3Vdhwpku
gJovFRSDVL8-xaM9fasE3R0='
[debug] ticket isb'gRbeCIwHRF4JgNv-GT6Q
NP1xXth1ygCduJX-Kxyh3n4='
Authenticated!!
ticket b'gRbeCIwHRF4JgNv-GT6QNP1xXth1yg
CduJX-Kxyh3n4='
session key b'KLzKsRb17ACD3VdhwpkugJovF
RSDVL8-xaM9fasE3R0='
Authentication with chat server complet
e successfully
Listening Started
>>
```

```
----\n'
[debug] My key isb'BNidHOjDe2epFIXgvIq
esKO2vsEsGQfqxGsStm43c3w='
[debug] k_temp isb'sfjFDwX7R81hoV2nyDh
lmRSofZeT3oBVL1p5_35uPl8='
[debug] ticket isb'awPfvytdKCQG4jiolgS
SxZtIPETzjAoMTJpN0pnHMCg='
Authenticated!!
ticket b'awPfvytdKCQG4jiolgSSxZtIPETzj
AoMTJpN0pnHMCg='
session key b'sfjFDwX7R81hoV2nyDhlmRSo
fZeT3oBVL1p5_35uPl8='
Authentication with chat server comple
te successfully
Listening Started
>>
```

- Enter “/group_invite 0 1” to invite client 1 to group 0. Similarly for client2, and client3



```
ieurMGIi_UeG3WmzCd-5-8tcVLf5dK8FKwlnya
Vd6wdb-6b62sYUEdxoLw7N4nFW8V5Ohk9JTLBS
SSdQHNTSO8VxaqtF_1')
[Chat server][debug] rec arguement:('/
group_invite', '0', '3', b'9Epy8ya1nWh
cbVapRrAglSO-wWN_IqRej0iyPlSVj80=')
[Chat server][debug] Received ticket:
b'9Epy8ya1nWhcbVapRrAglSO-wWN_IqRej0iy
PlSVj80='
[Chat server][debug] Stored ticket:
b'9Epy8ya1nWhcbVapRrAglSO-wWN_IqRej0iy
PlSVj80='
[Chat server] /group_invite
[Chat server] Client 3 added to group
0
```

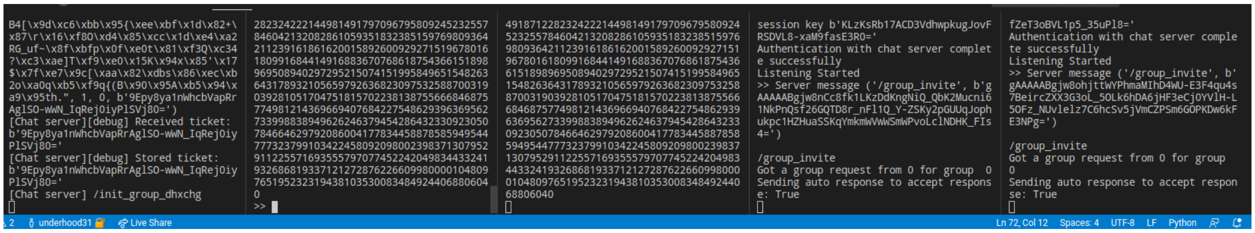
```
e successfully
Listening Started
>> /create_group sample_group
sample_group
Group with id: 0 and name: sample_group
 is created
>> /group_invite 0 1
Client: 1 accepted the invite to the gr
oup 0
>> /group_invite 0 2
Client: 2 accepted the invite to the gr
oup 0
>> /group_invite 0 3
Client: 3 accepted the invite to the gr
oup 0
>>
```

```
session key b'3IMAyRW9F2foggBUPiNHpY-D5
ok7inIm7Qh6rBPvVV4='
Authentication with chat server complet
e successfully
Listening Started
>> Server message ('/group_invite', b'g
AAAAABgjw8lrISNjlMPzrDkAEsyJCeAhQC6Ttiv
hIGMVKs2KkGadVSisG6guZsWogsJd_XR4bbAhyx
UZteVkfUjwhmUVpTeo5GXHLPGxHEfFIAjPO8upH
E=')

/group_invite
Got a group request from 0 for group  0
Sending auto response to accept respons
e: True
```

```
session key b'KLzKsRb17ACD3VdhwpkugJovF
RSDVL8-xaM9fasE3R0='
Authentication with chat server complet
e successfully
Listening Started
>> Server message ('/group_invite', b'g
AAAAABgjw8nCc8fk1LKzDdKngNiQ_QbK2Mucni6
1NkPnQsf26GQTD8r_nFl1Q_Y-ZSKy2pGUUqJoph
ukpc1HZHuaSSKqYmkmWVwWSmWPvoLclNDHK_FIs
4=')

/group_invite
Got a group request from 0 for group  0
Sending auto response to accept respons
e: True
```

```
fZeT3oBVL1p5_35uPl8='
Authentication with chat server comple
te successfully
Listening Started
>> Server message ('/group_invite', b'
gAAAAABgjw8ohjttWYPhmaMIhD4WU-E3F4qu4s
7BeircZXX3G3oL_5OLk6hDA6jHF3eCj0YVlH-L
5OFz_NUvlelz7C6hcSv5jVmCZPSm6GOPKDw6kF
E3NPg=')

/group_invite
Got a group request from 0 for group
0
Sending auto response to accept respon
se: True
```

- Run “/init_group_dhxchg 0 1” to do a DH key exchange with client3 for group0. Repeat this for client2 and client3 to update the group key for their DH keys.



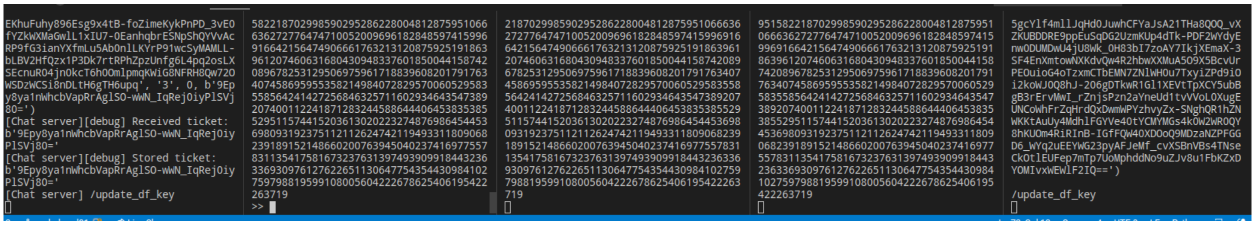
```
B4[\x9d\xc6\xbb\x95{\xee\xbf\x1d\x82+\
x87\r\x16\xf8O\xd4\x85\xcc\x1d\xe4\xa2
RG_uf~\x8f\xbfp\x0f\xe0t\x81\xf3Q\xc34
?\xc3\xae]T\xf9\xe0\x15K\x94x\x85'\x17
$\x7f\xe7\x9c[\xaa\x82\xdbs\x86\xec\xb
2o\xa0q\xb5\xf9q{(B\x90\x95A\xb5\x94\x
a9\x95th.", 1, 0, b'9Epy8ya1nWhcbVapRr
AglSO-wWN_IqRej0iyPlSVj80=')
[Chat server][debug] Received ticket:
b'9Epy8ya1nWhcbVapRrAglSO-wWN_IqRej0iy
PlSVj80='
[Chat server][debug] Stored ticket:
b'9Epy8ya1nWhcbVapRrAglSO-wWN_IqRej0iy
PlSVj80='
[Chat server] /init_group_dhxchg
```

```
282324222144981491797096795809245232557
846042132082861059351832385159769809364
211239161861620015892600929271519678016
180991684414916883670768618754366151898
969508940297295215074151995849651548263
643178932105659792636823097532588700319
039281051704751815702238138755666846875
774981214369669407684227548629396369562
733998838949626246379454286432330923050
784664629792086004177834458878585949544
777323799103422458092098002398371307952
911225571693555797077452242049834433241
932686819337121272876226609980000104809
765195232319438103530083484924406880604
0
>>
```

```
491871228232422214498149179709679580924
523255784604213208286105935183238515976
980936421123916186162001589260092927151
967801618099168441491688367076861875436
615189896950894029729521507415199584965
154826364317893210565979263682309753258
870031903928105170475181570223813875566
684687577498121436966940768422754862939
636956273399883894962624637945428643233
092305078466462979208600417783445887858
594954477732379910342245809209800239837
130795291122557169355579707745224204983
443324193268681933712127287622660998000
010480976519523231943810353008348492440
68806040
```

```
session key b'KLzKsRb17ACD3VdhwpkugJovF
RSDVL8-xaM9fasE3R0='
Authentication with chat server complet
e successfully
Listening Started
>> Server message ('/group_invite', b'g
AAAAABgjw8nCc8fk1LKzDdKngNiQ_QbK2Mucni6
1NkPnQsf26GQTD8r_nFl1Q_Y-ZSKy2pGUUqJoph
ukpc1HZHuaSSKqYmkmWVwWSmWPvoLclNDHK_FIs
4=')

/group_invite
Got a group request from 0 for group  0
Sending auto response to accept respons
e: True
```

```
fZeT3oBVL1p5_35uPl8='
Authentication with chat server comple
te successfully
Listening Started
>> Server message ('/group_invite', b'
gAAAAABgjw8ohjttWYPhmaMIhD4WU-E3F4qu4s
7BeircZXX3G3oL_5OLk6hDA6jHF3eCj0YVlH-L
5OFz_NUvlelz7C6hcSv5jVmCZPSm6GOPKDw6kF
E3NPg=')

/group_invite
Got a group request from 0 for group
0
Sending auto response to accept respon
se: True
```



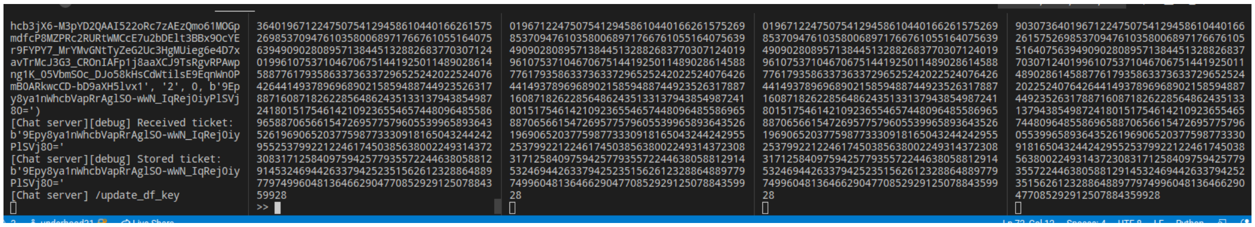
```
EKhuFuhy896Esg9x4tB-foZimeKykPnPD_3vE0
fYZkWXMaGwlL1xIU7-0EanhqbrESNpShQYVvAc
RP9fG3ianYXfmLu5Ab0nlLKYrP91wcSyMAMLL-
bLBV2HfQzx1P3Dk7rtRPhZpzUnfg6L4pq2osLX
SEcnuR04jn0kcT6h0OmlpmqKWiG8NFRH8Qw72O
WSDzWCSi8nDLtH6gTH6upq', '3', 0, b'9Ep
y8ya1nWhcbVapRrAglSO-wWN_IqRej0iyPlSVj
80=')
[Chat server][debug] Received ticket:
b'9Epy8ya1nWhcbVapRrAglSO-wWN_IqRej0iy
PlSVj80='
[Chat server][debug] Stored ticket:
b'9Epy8ya1nWhcbVapRrAglSO-wWN_IqRej0iy
PlSVj80='
[Chat server] /update_df_key
```

```
582218702998590295286228004812875951066
636272776474710052009696182848597415996
916642156474906661763213120875925191863
961207460631680430948337601850044158742
089678253129506975961718839608201791763
407458695955358214984072829570060529583
558564241427256846325711602934643547389
207400112241871283244588644406453835385
529511574415203613020223274876986454453
698093192375112112624742119493311809068
239189152148660200763945040237416977557
831135417581673237631397493909918443236
336930976127622651130647754354430984102
759798819599108005604222678625406195422
263719
>>
```

```
218702998590295286228004812875951066636
272776474710052009696182848597415996916
642156474906661763213120875925191863961
207460631680430948337601850044158742089
678253129506975961718839608201791763407
458695955358214984072829570060529583558
564241427256846325711602934643547389207
400112241871283244588644406453835385529
511574415203613020223274876986454453698
093192375112112624742119493311809068239
189152148660200763945040237416977557831
135417581673237631397493909918443236336
930976127622651130647754354430984102759
798819599108005604222678625406195422263
719
```

```
951582218702998590295286228004812875951
066636272776474710052009696182848597415
996916642156474906661763213120875925191
863961207460631680430948337601850044158
742089678253129506975961718839608201791
763407458695955358214984072829570060529
583558564241427256846325711602934643547
389207400112241871283244588644406453835
385529511574415203613020223274876986454
453698093192375112112624742119493311809
068239189152148660200763945040237416977
557831135417581673237631397493909918443
236336930976127622651130647754354430984
102759798819599108005604222678625406195
422263719
```

```
5gcYlf4mllJqHd0JuwhCFYaJsA21THa8QOQ_vX
ZKUBDDRE9ppEuSqDG2UzmKUp4dTk-PDF2WYdyE
nw0DUMDwU4jU8Wk_0H83bI7zoAY7IkjXEmaX-3
SF4EnXmtowNXKdvQw4R2hbwXXMuA5O9X5BcvUr
PEOuioG4oTzxmCTbEMN7ZNlWH0u7TxyiZPd9iO
i2koWJOQ8hJ-206gDTkwR1Gl1XEVtTpXCY5ubB
gB3rErvMwI_rZnjsPzn2aYneUd1tvVVoL0XugE
UNCoWhFrZqHrdQxDwmWPYzhvyZx-SNghQR1hZN
WKKtAuUy4MdhlFGYVe40tYCMYMGs4k0W2WROQY
8hKUOm4RiRInB-IGfFQW40XDOoQ9MDzaNZPFGG
D6_WYq2uEEYWG23pyAFJeMf_cvXSBnVBs4TNse
CkOtlEUFep7mTp7UoMphddNo9uZJv8u1FbKZxD
YOMIvxWEWlF2IQ==')

/update_df_key
```



```
hcb3jX6-M3pYD2QAAI522oRc7zAEzQmo61MOGp
mdfcP8MZPRc2RURtWMCcE7u2bDElt3BBx9OcYE
r9FYPY7_MrYMvGNtTyZeG2Uc3HgMUieg6e4D7x
avTrMcJ3G3_CROnIAFp1j8aaXCJ9TsRgvRPAwp
ng1K_05VbmSOc_DJo58kHsCdWtilsE9EqnWn0P
mBOARkwcCD-bD9aXH5lvx1', '2', 0, b'9Ep
y8ya1nWhcbVapRrAglSO-wWN_IqRej0iyPlSVj
80=')
[Chat server][debug] Received ticket:
b'9Epy8ya1nWhcbVapRrAglSO-wWN_IqRej0iy
PlSVj80='
[Chat server][debug] Stored ticket:
b'9Epy8ya1nWhcbVapRrAglSO-wWN_IqRej0iy
PlSVj80='
[Chat server] /update_df_key
```

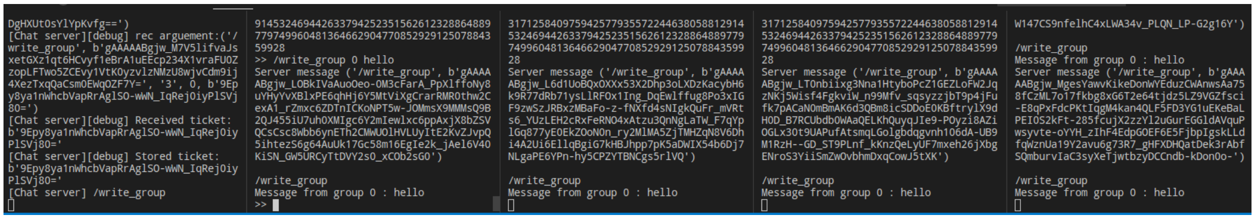
```
364019671224750754129458610440166261575
269853709476103580068971766761055164075
639490902808957138445132882683770307124
019961075371046706751441925011489028614
588776179358633736337296525242022524076
426441493789696890215859488744923526317
887160871826228564862435133137943854987
241801517546142109236554657448096485586
965887065661547269577579605539965893643
526196906520377598773330918165043244242
955253799221224617450385638002249314372
308317125840975942577935572244638058812
914532469442633794252351562612328864889
779749960481364662904770852929125078843
59928
>>
```

```
019671224750754129458610440166261575269
853709476103580068971766761055164075639
490902808957138445132882683770307124019
961075371046706751441925011489028614588
776179358633736337296525242022524076426
441493789696890215859488744923526317887
160871826228564862435133137943854987241
801517546142109236554657448096485586965
887065661547269577579605539965893643526
196906520377598773330918165043244242955
253799221224617450385638002249314372308
317125840975942577935572244638058812914
532469442633794252351562612328864889779
749960481364662904770852929125078843599
28
```

```
019671224750754129458610440166261575269
853709476103580068971766761055164075639
490902808957138445132882683770307124019
961075371046706751441925011489028614588
776179358633736337296525242022524076426
441493789696890215859488744923526317887
160871826228564862435133137943854987241
801517546142109236554657448096485586965
887065661547269577579605539965893643526
196906520377598773330918165043244242955
253799221224617450385638002249314372308
317125840975942577935572244638058812914
532469442633794252351562612328864889779
749960481364662904770852929125078843599
28
```

```
90307364019671224750754129458610440166
26157526985370947610358006897176676105
51640756394909028089571384451328826837
70307124019961075371046706751441925011
48902861458877617935863373633729652524
20225240764264414937896968902158594887
44923526317887160871826228564862435133
13794385498724180151754614210923655465
74480964855869658870656615472695775796
05539965893643526196906520377598773330
91816504324424295525379922122461745038
56380022493143723083171258409759425779
35572244638058812914532469442633794252
35156261232886488977974996048136466290
477085292912507884359928
```

- Run “/write_group 0 hello” to write the message to the group0, encrypted by their DH key.



```
DgHXUt0sYlYpKvfg==')
[Chat server][debug] rec arguement:('/
write_group', b'gAAAAABgjw_M7V5lifvaJs
xetGXz1qt6HCvyf1eBrA1uEEcp234X1vraFU0Z
zopLFTwo5ZCEvy1VtK0yzvlzNMzU8wjvCdm9ij
4XezTxqQaCsm0EWqOZF7Y=', '3', 0, b'9Ep
y8ya1nWhcbVapRrAglSO-wWN_IqRej0iyPlSVj
80=')
[Chat server][debug] Received ticket:
b'9Epy8ya1nWhcbVapRrAglSO-wWN_IqRej0iy
PlSVj80='
[Chat server][debug] Stored ticket:
b'9Epy8ya1nWhcbVapRrAglSO-wWN_IqRej0iy
PlSVj80='
[Chat server] /write_group
```

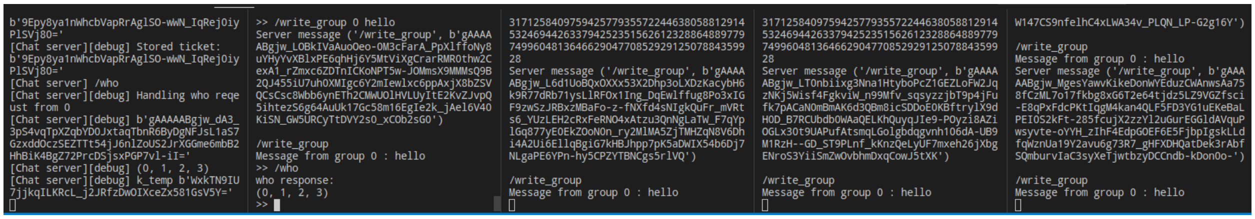
```
9145324694426337942523515626123288648889
7797499604813646629047708529291250788843
59928
>> /write_group 0 hello
Server message ('/write_group', b'gAAAA
ABgjw_LOBkIVaAuoOeo-0M3cFarA_PpXlffoNy8
uYHyYvXBlxPE6qhHj6Y5MtViXgCrarRMR0thw2C
exA1_rZmxc6ZDTnICKoNPT5w-JOMmsX9MMMsQ9B
2QJ455iU7uh0XMIgc6Y2mIewlxc6ppAxjX8bZSV
QCsCsc8Wbb6ynETh2CMWUOlHVLUyItE2KvZJvpQ
5ihtezS6g64AuUk17Gc58m16EgIe2k_jAel6V40
KiSN_GW5URCyTtDVY2s0_xCOb2sG0')

/write_group
Message from group 0 : hello
>>
```

```
3171258409759425779355722446380588129l4
5324694426337942523515626123288648889779
7499604813646629047708529291250788843599
28
Server message ('/write_group', b'gAAAA
ABgjw_L6d1UoBQxOXXx53X2Dhp3oLXDzKacybH6
k9R77dRb71ysLlRFOx1Ing_DqEwlffug8Po3xIG
F9zwSzJRBxzMBaFo-z-fNXfd4sNIgkQuFr_mVRt
s6_YUzLEH2cRxFeRNO4xAtzu3QnNgLaTW_F7qYp
lGq877yEOEkZOoN0n_ry2MlMA5ZjTMHZqN8V6Dh
i4A2Ui6EllqBgiG7kHBJhpp7pK5aDWIX54b6Dj7
NLgaPE6YPn-hy5CPZYTBNCgs5rlVQ')

/write_group
Message from group 0 : hello
```

```
3171258409759425779355722446380588129l4
5324694426337942523515626123288648889779
7499604813646629047708529291250788843599
28
Server message ('/write_group', b'gAAAA
ABgjw_LTOnbiixg3Nna1HtyboPcZ1GEZLoFW2Jq
zNKj5Wisf4FgkviW_n99Mfv_sqsyzzjbT9p4jFu
fk7pACaN0mBmAK6d3QBm8icSDDoE0KBftrylX9d
HOD_B7RCUbdb0WAaQELKhQuyqJIe9-POyzi8AZi
OGLx30t9UAPufAtsmqLGolgbdqgvnh106dA-UB9
M1RzH--GD_ST9PLnf_kKnzQeLyUF7mxeh26jXbg
ENroS3YiiSmZwOvbhmDxqCowJ5tXK')

/write_group
Message from group 0 : hello
```

```
W147CS9nfelhC4xLWA34v_PLQN_LP-G2g16Y')

/write_group
Message from group 0 : hello
Server message ('/write_group', b'gAAA
AABgjw_MgesYawvKikeDonWYEduzCWAnwsAa75
8fCzML7o17fkbg8xG6T2e64tjdz5LZ9VGZfsci
-E8qPxFdcPKtIqgM4kan4QLF5FD3YG1uEKeBaL
PEIOS2kFt-285fcujX2zzYl2uGurEGGldAVquP
wsyvte-oYYH_zIhF4EdpGOEF6E5FjbpIgskLLd
fqWznUa19Y2avu6g73R7_gHFXDHQatDek3rAbf
SQmburvIaC3syXeTjwtbzyDCCndb-kDon0o-')

/write_group
Message from group 0 : hello
```

- Run “/who” to see all those on the server



```
b'9Epy8ya1nWhcbVapRrAglSO-wWN_IqRej0iy
PlSVj80='
[Chat server][debug] Stored ticket:
b'9Epy8ya1nWhcbVapRrAglSO-wWN_IqRej0iy
PlSVj80='
[Chat server] /who
[Chat server][debug] Handling who reqe
ust from 0
[Chat server][debug] b'gAAAAABgjw_dA3_
3pS4vqTpXZqbYD0JxtaqTbnR6ByDgNFJsL1aS7
GzxddOczSEZTTt54jJ6nlZoUS2JrXGGme6mbB2
HhBiK4BgZ72PrcDSjsxPGP7vl-iI='
[Chat server][debug] (0, 1, 2, 3)
[Chat server][debug] k_temp b'WxkTN9IU
7jjkqILKRcL_j2JRfzDwOIXceZx581GsV5Y='
```

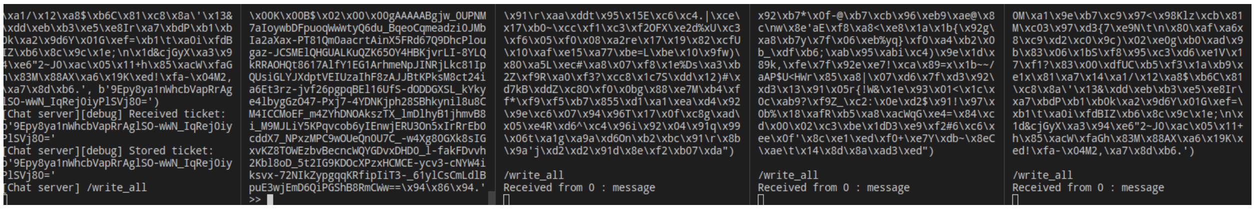
```
>> /write_group 0 hello
Server message ('/write_group', b'gAAAA
ABgjw_LOBkIVaAuoOeo-0M3cFarA_PpXlffoNy8
uYHyYvXBlxPE6qhHj6Y5MtViXgCrarRMR0thw2C
exA1_rZmxc6ZDTnICKoNPT5w-JOMmsX9MMMsQ9B
2QJ455iU7uh0XMIgc6Y2mIewlxc6ppAxjX8bZSV
QCsCsc8Wbb6ynETh2CMWUOlHVLUyItE2KvZJvpQ
5ihtezS6g64AuUk17Gc58m16EgIe2k_jAel6V40
KiSN_GW5URCyTtDVY2s0_xCOb2sG0')

/write_group
Message from group 0 : hello
>> /who
who response:
(0, 1, 2, 3)
>>
```

```
3171258409759425779355722446380588129l4
5324694426337942523515626123288648889779
7499604813646629047708529291250788843599
28
Server message ('/write_group', b'gAAAA
ABgjw_L6d1UoBQxOXXx53X2Dhp3oLXDzKacybH6
k9R77dRb71ysLlRFOx1Ing_DqEwlffug8Po3xIG
F9zwSzJRBxzMBaFo-z-fNXfd4sNIgkQuFr_mVRt
s6_YUzLEH2cRxFeRNO4xAtzu3QnNgLaTW_F7qYp
lGq877yEOEkZOoN0n_ry2MlMA5ZjTMHZqN8V6Dh
i4A2Ui6EllqBgiG7kHBJhpp7pK5aDWIX54b6Dj7
NLgaPE6YPn-hy5CPZYTBNCgs5rlVQ')

/write_group
Message from group 0 : hello
```

```
3171258409759425779355722446380588129l4
5324694426337942523515626123288648889779
7499604813646629047708529291250788843599
28
Server message ('/write_group', b'gAAAA
ABgjw_LTOnbiixg3Nna1HtyboPcZ1GEZLoFW2Jq
zNKj5Wisf4FgkviW_n99Mfv_sqsyzzjbT9p4jFu
fk7pACaN0mBmAK6d3QBm8icSDDoE0KBftrylX9d
HOD_B7RCUbdb0WAaQELKhQuyqJIe9-POyzi8AZi
OGLx30t9UAPufAtsmqLGolgbdqgvnh106dA-UB9
M1RzH--GD_ST9PLnf_kKnzQeLyUF7mxeh26jXbg
ENroS3YiiSmZwOvbhmDxqCowJ5tXK')

/write_group
Message from group 0 : hello
```

```
W147CS9nfelhC4xLWA34v_PLQN_LP-G2g16Y')

/write_group
Message from group 0 : hello
Server message ('/write_group', b'gAAA
AABgjw_MgesYawvKikeDonWYEduzCWAnwsAa75
8fCzML7o17fkbg8xG6T2e64tjdz5LZ9VGZfsci
-E8qPxFdcPKtIqgM4kan4QLF5FD3YG1uEKeBaL
PEIOS2kFt-285fcujX2zzYl2uGurEGGldAVquP
wsyvte-oYYH_zIhF4EdpGOEF6E5FjbpIgskLLd
fqWznUa19Y2avu6g73R7_gHFXDHQatDek3rAbf
SQmburvIaC3syXeTjwtbzyDCCndb-kDon0o-')

/write_group
Message from group 0 : hello
```

- Run “/write_all message” to broadcast message to all the clients



```
\xa1/\x12\xa8$\xb6C\x81\xc8\x8a\'\x13&
\xdd\xeb\xb3\xe5\xe8Ir\xa7\xbdP\xb1\xb
0k\xa2\x9d6Y\x01G\xef=\xb1\t\xa0i\xfdB
IZ\xb6\x8c\x9c\x1e;\n\x1d&cjGyX\xa3\x9
4\xe6"2~J0\xac\x05\x11+h\x85\xacW\xfaG
h\x83M\x88AX\xa6\x19K\xed!\xfa-\x04M2,
\xa7\x8d\xb6.', b'9Epy8ya1nWhcbVapRrAg
lSO-wWN_IqRej0iyPlSVj80=')
[Chat server][debug] Received ticket:
b'9Epy8ya1nWhcbVapRrAglSO-wWN_IqRej0iy
PlSVj80='
[Chat server][debug] Stored ticket:
b'9Epy8ya1nWhcbVapRrAglSO-wWN_IqRej0iy
PlSVj80='
[Chat server] /write_all
```

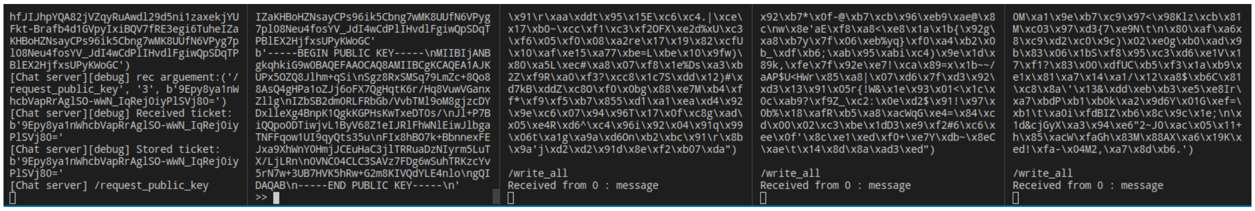
```
\x00K\x00B$\x02\x00\x00gAAAAABgjw_0UPNM
7aIoywbDFpuoqWwwtyQ6du_BqeoCqmeadzi0JMb
Ia2aXax-PT81Qm0aacrtAinX5FRd67Q9DhcPlou
gaz-JCSMElQHGUALKuQZK65OY4HBKjvrLI-8YLQ
kRRAOHQt8617AlfY1EG1ArhmeNpJINRjLkc81Ip
QUsiGLYJXdptVEIUzaIhF8zAJJBtKPksM8ct24i
a6Et3rz-jvf26pgpqBEl16UfS-dODDGXSL_kYky
e4lbygGzO47-Pxj7-4YDNKjph28SBhkynil8u8C
M4ICCMoEF_m4ZYhDNOAkszTX_lmDlhyB1jhmvB8
i_M9MJLiY5KPqvcob6yIEnwjERU3On5xIrRrEb0
cddX7_NPxzMPC9wOUeQn0U7C_-w4Xg80GXk8sIG
xvKZ8TOWEzbvBecncWQYGDvxDHD0_l-fakFDvvh
2Kbl8oD_5t2IG9KDOcXPzxHCMCE-ycv3-cNYW4i
ksvx-72NIkZypgqqKRfipIiT3-_61ylCsCmLdlB
puE3wjEmD6QiPGShB8RmCWw==\x94\x86\x94.'
>>
```

```
\x91\r\xaa\xddt\x95\x15E\xc6\xc4.|\xce\
x17\xb0~\xcc\xf1\xc3\xf2OFX\xe2d%xU\xc3
\xf6\x05\xf0\x08\xa2re\x17\x19\x82\xcfU
\x10\xaf\xe15\xa77\xbe=L\xbe\x10\x9fw)\
x80\xa5L\xec#\xa8\x07\xf8\x1e%Ds\xa3\xb
2Z\xf9R\xa0\xf3?\xcc8\x1c7S\xdd\x12)#\x
d7kB\xddZ\xc8O\xf0\x0bg\x88\xe7M\xb4\xf
f*\xf9\xf5\xb7\x855\xd1\xa1\xea\xd4\x92
\x9e\xc6\x07\x94\x96T\x17\x0f\xc8g\xad\
x05\xe4R\xd6^\xc4\x96i\x92\x04\x91q\x99
\x06t\xa1g\xa9a\xd6On\xb2\xbc\x91\r\x8b
\x9a'j\xd2\xd2\x91d\x8e\xf2\xb07\xda")

/write_all
Received from 0 : message
```

```
x92\xb7*\x0f-@\xb7\xcb\x96\xeb9\xae@\x8
c\nw\x8e'aE\xf8\xa8<\xe8\x1a\x1b{\x92g\
xa8\xb7y\x7f\x06\xeb%yq}\xf0\xa4\xb2\x0
b_\xdf\xb6;\xab\x95\xabi\xc4)\x9e\x1d\x
89k,\xfe\x7f\x92e\xe7!\xca\x89=x\x1b~~/
aAP$U<HWr\x85\xa8|\x07\xd6\x7f\xd3\x92\
xd3\x13\x91\x05r{!W&\x1e\x93\x01<\x1c\x
0c\xab9?\xf9Z_\xc2:\x0e\xd2$\x91!\x97\x
0b%\x18\xafR\xb5\xa8\xacWqG\xe4=\x84\xc
d\x00\x02\xc3\xbe\x1dD3\xe9\xf2#6\xc6\x
ee\x0f'\x8c\xe1\xed\xf0+\xe7Y\xdb~\x8eC
\xae\t\x14\x8d\x8a\xad3\xed")

/write_all
Received from 0 : message
```

```
0M\xa1\x9e\xb7\xc9\x97<\x98Klz\xcb\x81
M\xc03\x97\xd3{7\xe9N\t\n\x80\xaf\xa6x
8\xc9\xd2\xc0\x9c)\x02\xe0g\xb0\xad\x9
b\x83\x06\x1bS\xf8\x95\xc3\xd6\xe1V\x1
7\xf1?\x83\x00\xdfUC\xb5\xf3\x1a\xb9\x
e1x\x81\xa7\x14\xa1/\x12\xa8$\xb6C\x81
\xc8\x8a\'\x13&\xdd\xeb\xb3\xe5\xe8Ir\
xa7\xbdP\xb1\xb0k\xa2\x9d6Y\x01G\xef=\
xb1\t\xa0i\xfdBIZ\xb6\x8c\x9c\x1e;\n\x
1d&cjGyX\xa3\x94\xe6"2~J0\xac\x05\x11+
h\x85\xacW\xfaGh\x83M\x88AX\xa6\x19K\x
ed!\xfa-\x04M2,\xa7\x8d\xb6.')

/write_all
Received from 0 : message
```

- Run “/request_public_key 3” to get the public key of the client 3



```
hfJIJhpYQA82jVZqyRuAwdl29d5ni1zaxekjYU
Fkt-Brafb4d1GVpyIxiBQV7fRE3egi6TuheIZa
KHBoHZNsayCPs96ik5Cbng7wMK8UUfN6VPyg7p
l08Neu4fosYV_JdI4wCdPlIHvdlFgiwQpSDqTP
BlEX2HjfxsUPyKWoGC')
[Chat server][debug] rec arguement:('/
request_public_key', '3', b'9Epy8ya1nW
hcbVapRrAglSO-wWN_IqRej0iyPlSVj80=')
[Chat server][debug] Received ticket:
b'9Epy8ya1nWhcbVapRrAglSO-wWN_IqRej0iy
PlSVj80='
[Chat server][debug] Stored ticket:
b'9Epy8ya1nWhcbVapRrAglSO-wWN_IqRej0iy
PlSVj80='
[Chat server] /request_public_key
```

```
IZaKHBoHZNsayCPs96ik5Cbng7wMK8UUfN6VPyg
7pl08Neu4fosYV_JdI4wCdPlIHvdlFgiwQpSDqT
PBlEX2HjfxsUPyKWoGC'
b'-----BEGIN PUBLIC KEY-----\nMIIBIjANB
gkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1AJK
UPx5OZQ8Jlhm+qSi\nSgz8RxSMSq79LmZc+8Qo8
8AsQ4gHPa1oZJj6oFX7QgHqtK6r/Hq8VuwVGanx
Zllg\nIZbSB2dm0RLFRbGb/VvbTMl9oM8gjzcDY
DxlleXg4BnpK1QgkKGPHsKwTxeDT0s/\nJl+P7B
iQQpo0DTiwjvL1ByV68Z1eIJRlFhWNlEiwJlbga
TNFFqow1UI9qyQts35u\nFIx8hBO7k+BbnnexFE
Jxa9XhWnY0HmjJCEuHaC3jlTRRuaDzNIyrm5LuT
X/LjLRn\n0VNC04CLC3SAVz7FDg6wSuhTRKzcYv
5rN7w+3UB7HVK5hRw+G2m8KIVQdYLE4nlo\ngQI
DAQAB\n-----END PUBLIC KEY-----\n'
>>
```

```
\x91\r\xaa\xddt\x95\x15E\xc6\xc4.|\xce\
x17\xb0~\xcc\xf1\xc3\xf2OFX\xe2d%xU\xc3
\xf6\x05\xf0\x08\xa2re\x17\x19\x82\xcfU
\x10\xaf\xe15\xa77\xbe=L\xbe\x10\x9fw)\
x80\xa5L\xec#\xa8\x07\xf8\x1e%Ds\xa3\xb
2Z\xf9R\xa0\xf3?\xcc8\x1c7S\xdd\x12)#\x
d7kB\xddZ\xc8O\xf0\x0bg\x88\xe7M\xb4\xf
f*\xf9\xf5\xb7\x855\xd1\xa1\xea\xd4\x92
\x9e\xc6\x07\x94\x96T\x17\x0f\xc8g\xad\
x05\xe4R\xd6^\xc4\x96i\x92\x04\x91q\x99
\x06t\xa1g\xa9a\xd6On\xb2\xbc\x91\r\x8b
\x9a'j\xd2\xd2\x91d\x8e\xf2\xb07\xda")

/write_all
Received from 0 : message
```

```
x92\xb7*\x0f-@\xb7\xcb\x96\xeb9\xae@\x8
c\nw\x8e'aE\xf8\xa8<\xe8\x1a\x1b{\x92g\
xa8\xb7y\x7f\x06\xeb%yq}\xf0\xa4\xb2\x0
b_\xdf\xb6;\xab\x95\xabi\xc4)\x9e\x1d\x
89k,\xfe\x7f\x92e\xe7!\xca\x89=x\x1b~~/
aAP$U<HWr\x85\xa8|\x07\xd6\x7f\xd3\x92\
xd3\x13\x91\x05r{!W&\x1e\x93\x01<\x1c\x
0c\xab9?\xf9Z_\xc2:\x0e\xd2$\x91!\x97\x
0b%\x18\xafR\xb5\xa8\xacWqG\xe4=\x84\xc
d\x00\x02\xc3\xbe\x1dD3\xe9\xf2#6\xc6\x
ee\x0f'\x8c\xe1\xed\xf0+\xe7Y\xdb~\x8eC
\xae\t\x14\x8d\x8a\xad3\xed")

/write_all
Received from 0 : message
```

```
0M\xa1\x9e\xb7\xc9\x97<\x98Klz\xcb\x81
M\xc03\x97\xd3{7\xe9N\t\n\x80\xaf\xa6x
8\xc9\xd2\xc0\x9c)\x02\xe0g\xb0\xad\x9
b\x83\x06\x1bS\xf8\x95\xc3\xd6\xe1V\x1
7\xf1?\x83\x00\xdfUC\xb5\xf3\x1a\xb9\x
e1x\x81\xa7\x14\xa1/\x12\xa8$\xb6C\x81
\xc8\x8a\'\x13&\xdd\xeb\xb3\xe5\xe8Ir\
xa7\xbdP\xb1\xb0k\xa2\x9d6Y\x01G\xef=\
xb1\t\xa0i\xfdBIZ\xb6\x8c\x9c\x1e;\n\x
1d&cjGyX\xa3\x94\xe6"2~J0\xac\x05\x11+
h\x85\xacW\xfaGh\x83M\x88AX\xa6\x19K\x
ed!\xfa-\x04M2,\xa7\x8d\xb6.')

/write_all
Received from 0 : message
```

Commands and assumptions

- “/who”: Who all are logged in to the chat server, along with a user IDs.
- “/write_all”: Write message which gets broadcasted to all users.
- “/create_group <grp_name>”: Create a group to which users may be added. A group ID and name is returned.
- “/group_invite <grp_id> <client_to_id>”: Send an invite to individual users IDs.
- “/group_invite_accept”: Convert acceptance variable to true, all requests will be accepted
- “/group_invite_decline”: Convert acceptance variable to false, all requests will be denied
- “/request public key”: Send request for public key to a specific users.
- “/send_public_key”: Send back public key back as a response to the above request. This command works internally, the user cannot fill it.
- “/init_group_dhxchg”: This process initiates a DH exchange first with any two users and then adds more users to the set..

- “/write_group <grp_id> message”: Write messages to a group specifying its group ID.
- “/list_user_files <ip addr> <port>”: list the files in the client directory
- “/request_file <ip_addr> <port> <file_name>”: loads the file into local client directory

Documentation and Code

Some highlights of the documentation is given below:

Client to KDC server

KDC side:

```
"""
       Prereq: kdc and client will have a preshared key(K_c)

       KDC                                                         Client
                                       <-----------------
(ID_client, TS1)

       K_temp=gen_session_key()
       ticket=gen_ticket()

       E(K_c, (E(K_temp, Ticket), Nonce, TS2))    ------------------->
       """
```

Client Side:

```
"""
               Client                                               KDC

           (ID_client, TS1)         ---------------->

                                <-----------------    E(K_c, (E(K_temp,
Ticket), Nonce, TS2))
           K_temp=gen_session_key()
           ticket=decrypt(K_temp, Ticket)
       """
```

Session key is the function of K_c, TS and nonce.

Client to Chat server authentication

```
"""
       The client should have a valid ticket and session_key before
contacting
       the chat server.
       This can be done by calling the authenticate function of this class
```

```
Client                                          Chat Server
~~~~~~                                          ~~~~~~~~~~~~


(
ID,                                    --------->
E(k_temp,(request, pub_key,ticket))
)
#Here request would be /auth

                                <-------         Acknowledgement
                                                 "Authenticated"
                                                     or
                                                ot Authenticated"


"""
```

The chat server matches the ticket and authenticates the client.

There is a shared database data structure that keeps track of client session_keys, ports, ip addresses and tickets.

For detailed information on diffie hellman key exchange, read documentation of `dh_key_xchange_request` , `df_xchg_handler` and `start_listening` from client, server_chat and again client documentation from docs folder or the following links.

For detailed documentation and code open HTML files in the docs folder in the submissions or the following links. **(Ps, if some comment is not clear, click on the expand code button under to see the raw text that would be clear).**

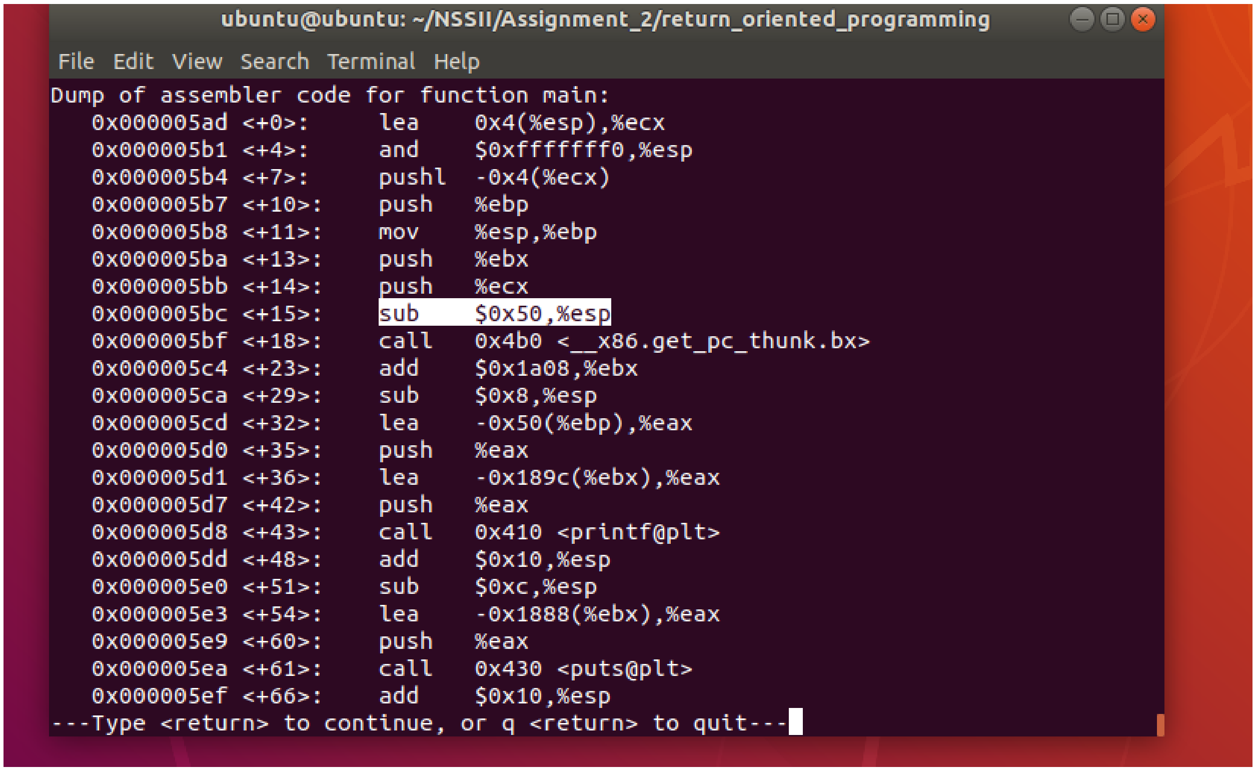
- client.py: https://underhood31.github.io/authenticated_IRC/client.html
- Server, main.py: https://underhood31.github.io/authenticated_IRC/server_main
- Server, kdc.py: https://underhood31.github.io/authenticated_IRC/server_kdc
- Server, chat.py: https://underhood31.github.io/authenticated_IRC/server_chat

Part 2, Return Oriented Programming

Steps:

- Disable virtual address space randomization using : `sudo bash -c 'echo 0 > /proc/sys/kernel/randomize_va_space'`

- Disable stack canaries(canaries prevent stack overflow by adding canaries at return point, if incorrect canaries are found program is terminated) using `-fno-stack-protector` when compiling.
- .From the screen shot below the structure of the stack would be as the following table:

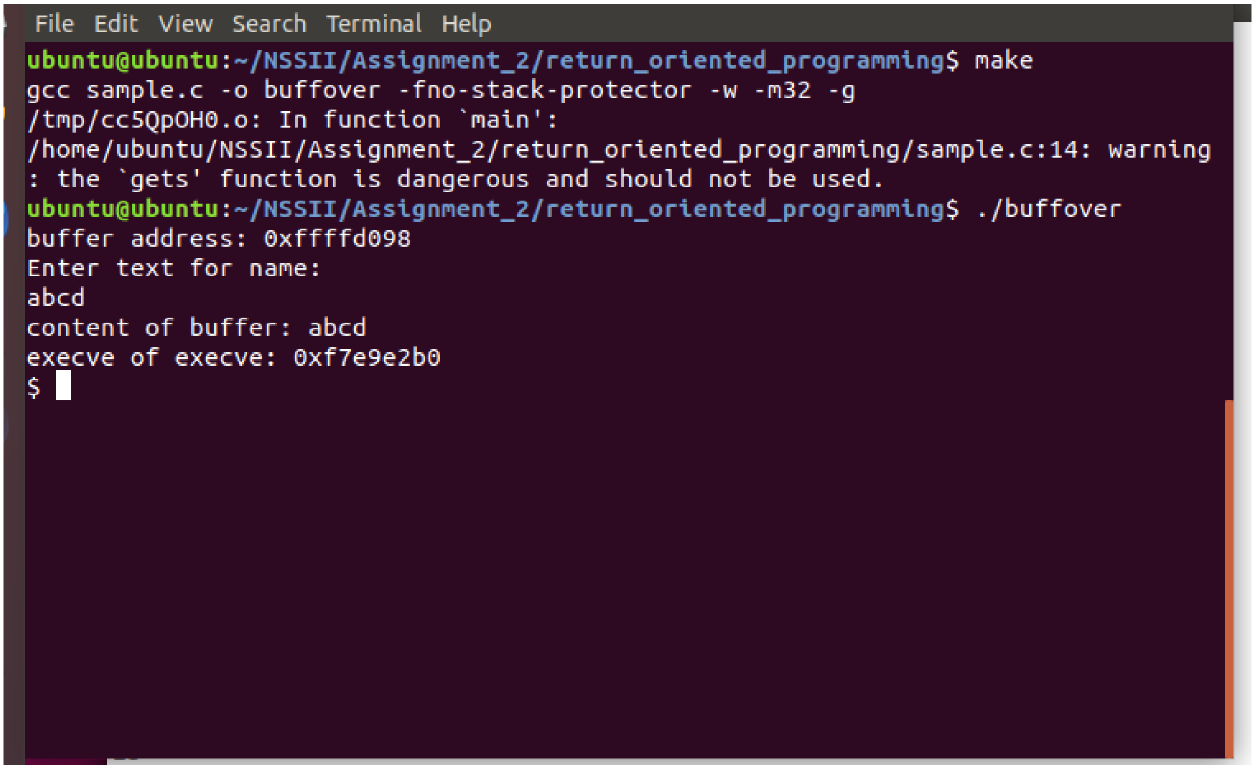

ubuntu@ubuntu: ~/NSSII/Assignment_2/return_oriented_programming
File Edit View Search Terminal Help

```
Dump of assembler code for function main:
   0x000005ad <+0>:     lea    0x4(%esp),%ecx
   0x000005b1 <+4>:     and    $0xfffffff0,%esp
   0x000005b4 <+7>:     pushl  -0x4(%ecx)
   0x000005b7 <+10>:    push   %ebp
   0x000005b8 <+11>:    mov    %esp,%ebp
   0x000005ba <+13>:    push   %ebx
   0x000005bb <+14>:    push   %ecx
   0x000005bc <+15>:    sub    $0x50,%esp
   0x000005bf <+18>:    call   0x4b0 <__x86.get_pc_thunk.bx>
   0x000005c4 <+23>:    add    $0x1a08,%ebx
   0x000005ca <+29>:    sub    $0x8,%esp
   0x000005cd <+32>:    lea    -0x50(%ebp),%eax
   0x000005d0 <+35>:    push   %eax
   0x000005d1 <+36>:    lea    -0x189c(%ebx),%eax
   0x000005d7 <+42>:    push   %eax
   0x000005d8 <+43>:    call   0x410 <printf@plt>
   0x000005dd <+48>:    add    $0x10,%esp
   0x000005e0 <+51>:    sub    $0xc,%esp
   0x000005e3 <+54>:    lea    -0x1888(%ebx),%eax
   0x000005e9 <+60>:    push   %eax
   0x000005ea <+61>:    call   0x430 <puts@plt>
   0x000005ef <+66>:    add    $0x10,%esp
---Type <return> to continue, or q <return> to quit---
```

4 Bytes //Return address
8 Bytes // from pushl instructions
4 Bytes // %ebp
4 Bytes // %ebx
4 Bytes // %ecx
80 Bytes // from sub $0x50, %esp instruction

- So in the code, name+80+8 gives the address of the saved ebp pointer value. Thus appropriate logic is applied in code.

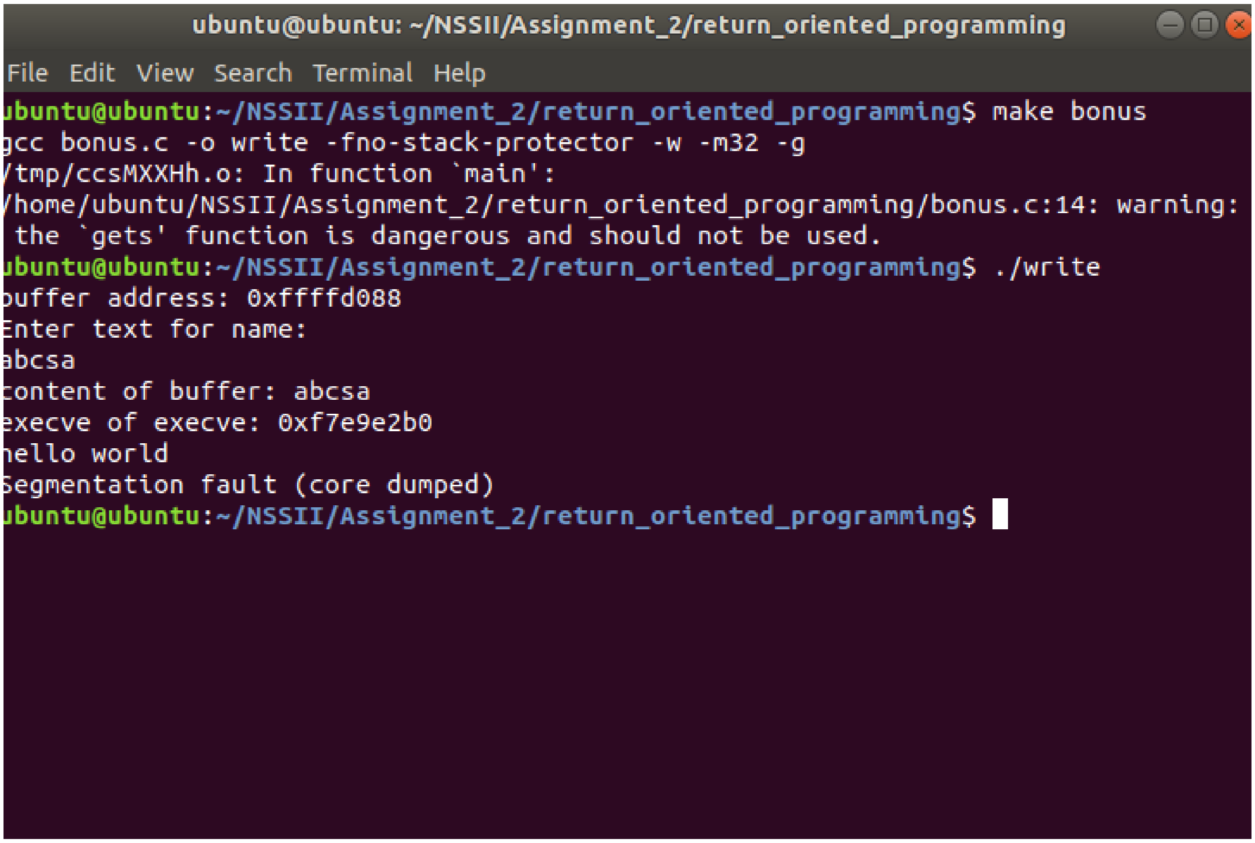
Now program is calling shell, use “make sample” and run “./buffover”



```
ubuntu@ubuntu:~/NSSII/Assignment_2/return_oriented_programming$ make
gcc sample.c -o buffover -fno-stack-protector -w -m32 -g
/tmp/cc5QpOH0.o: In function `main':
/home/ubuntu/NSSII/Assignment_2/return_oriented_programming/sample.c:14: warning
: the `gets' function is dangerous and should not be used.
ubuntu@ubuntu:~/NSSII/Assignment_2/return_oriented_programming$ ./buffover
buffer address: 0xffffd098
Enter text for name:
abcd
content of buffer: abcd
execve of execve: 0xf7e9e2b0
$ 
```

Bonus

Use “make bonus” to compile and run “./write”. This program was similar to the previous part the only difference is the size difference between pointer(4B), unsigned long/size_t(4B) and integers(2B)



ubuntu@ubuntu: ~/NSSII/Assignment_2/return_oriented_programming
File Edit View Search Terminal Help

```
ubuntu@ubuntu:~/NSSII/Assignment_2/return_oriented_programming$ make bonus
gcc bonus.c -o write -fno-stack-protector -w -m32 -g
/tmp/ccsMXXHh.o: In function `main':
/home/ubuntu/NSSII/Assignment_2/return_oriented_programming/bonus.c:14: warning:
 the `gets' function is dangerous and should not be used.
ubuntu@ubuntu:~/NSSII/Assignment_2/return_oriented_programming$ ./write
buffer address: 0xffffd088
Enter text for name:
abcsa
content of buffer: abcsa
execve of execve: 0xf7e9e2b0
hello world
Segmentation fault (core dumped)
ubuntu@ubuntu:~/NSSII/Assignment_2/return_oriented_programming$ 
```

References

https://www.sans.org/blog/stack-canaries-gingerly-sidestepping-the-cage/
https://stackoverflow.com/questions/2340259/how-to-turn-off-gcc-compiler-optimization-to-enable-buffer-overflow
http://www.learnlinux.org.za/courses/build/shell-scripting/ch01s04.html
https://nitratine.net/blog/post/asymmetric-encryption-and-decryption-in-python/#:~:text=Asymmetric%20encryption%20uses%20two%20keys,key%20can%20decrypt%20the%20message.
https://cryptography.io/en/latest/hazmat/primitives/asymmetric/rsa/
https://www.studytonight.com/python/python-threading-lock-object#:~:text=Lock%20Object%3A%20Python%20Multithreading&text=This%20lock%20helps%20us%20in,we%20initialize%20the%20Lock%20object
https://cryptography.io/en/latest/fernet/#using-passwords-with-fernet
https://devqa.io/encrypt-decrypt-data-python/
https://cryptography.io/en/latest/hazmat/primitives/cryptographic-hashes/