

# Procedural report (project phase III)

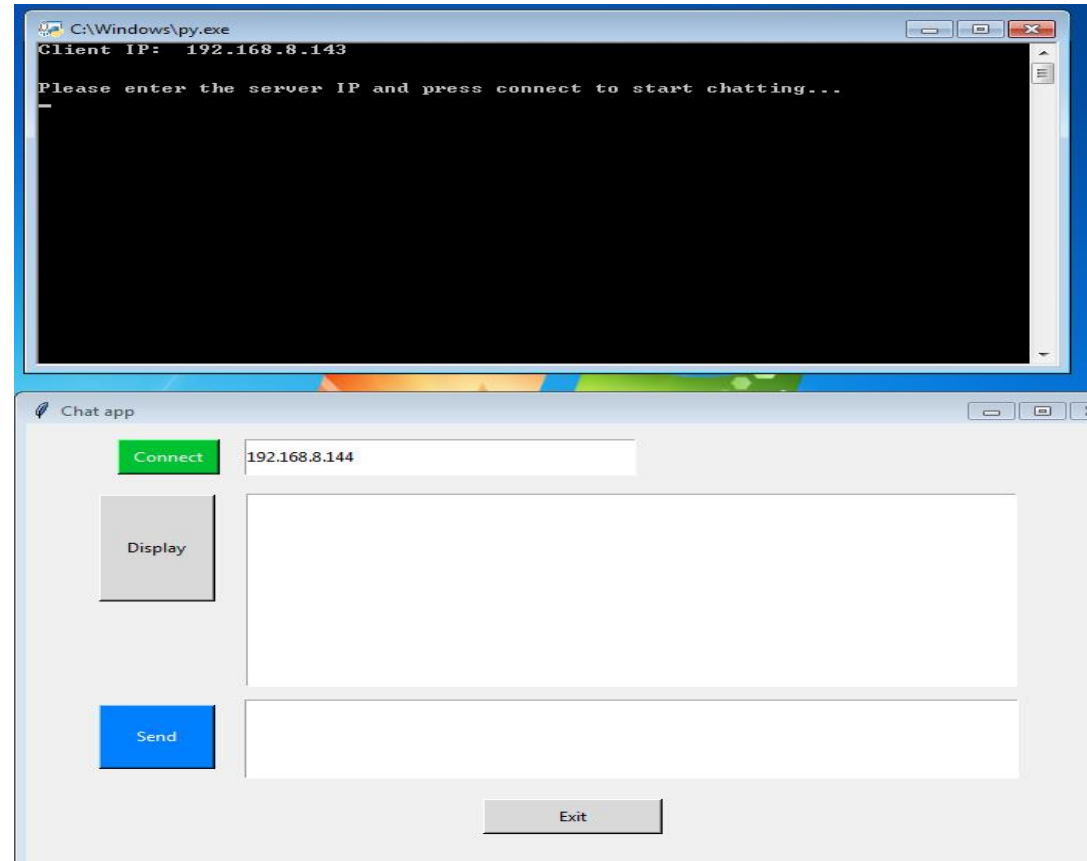
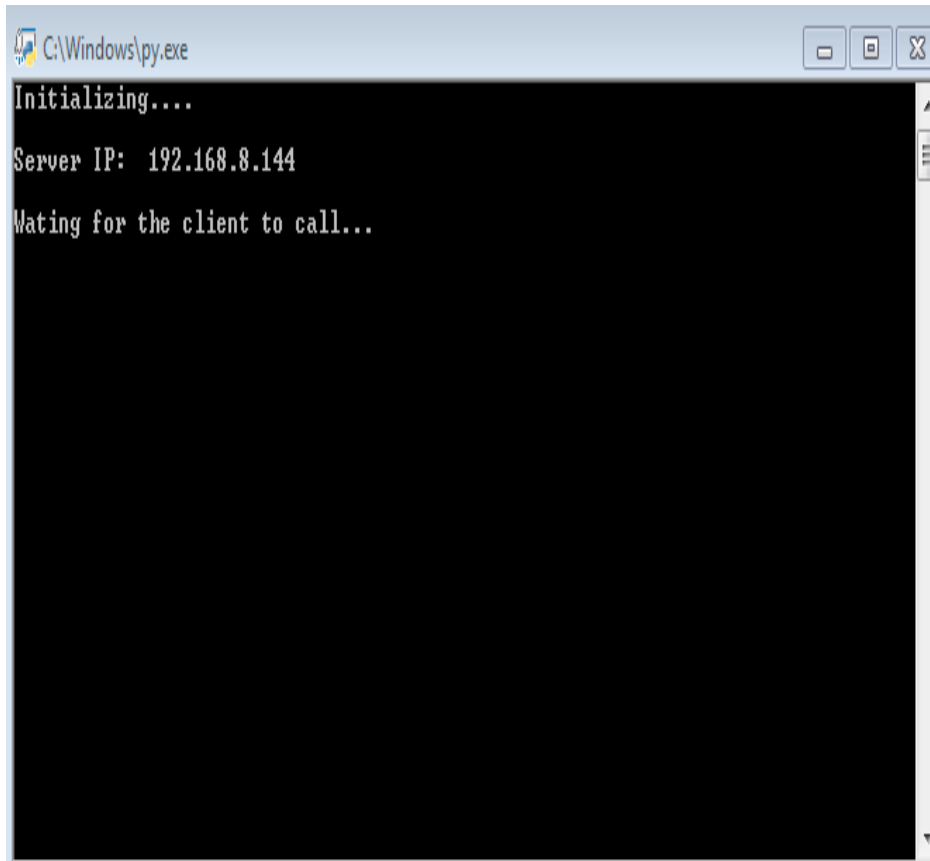
Name: Abdulwahab Hassan Alzahrani  
ID: 201337310

## Abstract

This report shows the procedural process of the modified SSH protocol along with AES\_256\_CBC cryptosystem.

Left pictures are for Bob(server) and right pictures are for Alice(Client)

Test case 1\_Session 1:



- Before clicking connect (same case for all remaining sessions)

```
C:\Windows\py.exe
Initializing....
Server IP: 192.168.8.144
Waiting for the client to call...

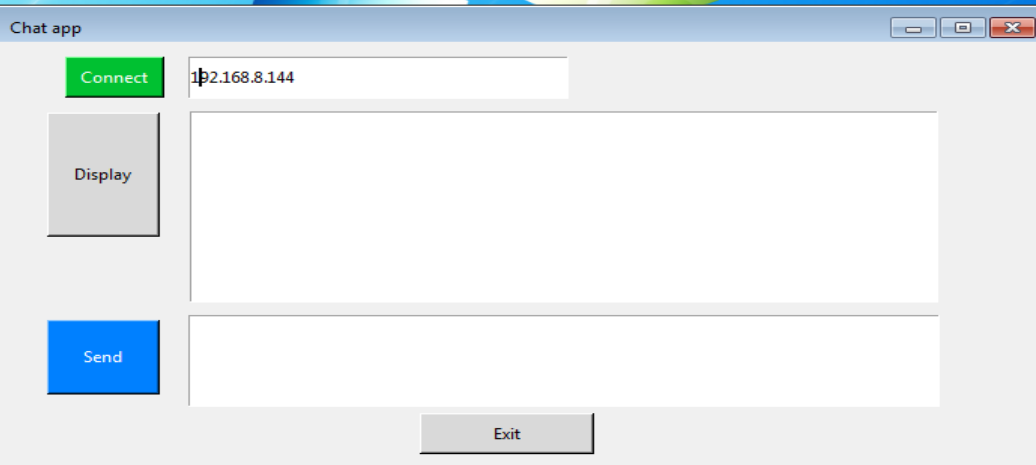
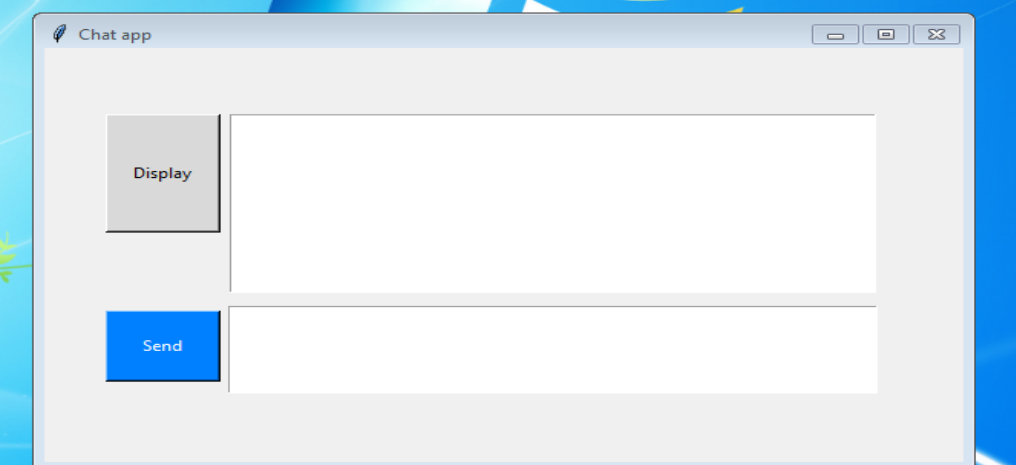
b: 2552904140391849401172299218891454080288993274508530908890141300225147919260
59004630966480083654220773825151081991549337929601934828694136326765156949006340
55090689893654886492332853563194055160473929093993945830937622383336620432033480
09585276365880092472069041223953664361878206918562110478098606509330207004563032
92588840524937624775290206358288413821378416680489018218344874816372932238683149
0746758860857590917819440241228888575390026869407282601513344206057671968337179
92251145211838154982968587781379297002163837138528774515335191905674101895690140
0506807509993082434764908121906975162749868891397977685124944

RA: 940959082672396416707941976660584327867036266889664641153621521756951612517
38
RB: 688903360635561404428133738075847098298620183605136665181256522423518234599
53
k: 011fc7d287b068422f2a0a3903a748f1a3d51a4d12156d259651092a3343fbe4
IV: 669217b491a4d1cf30b51b4f0f87e2a1
Alice was authenticated
-
```

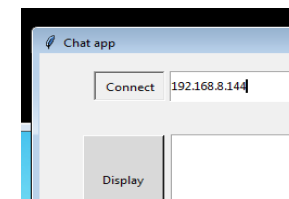
```
C:\Windows\py.exe
Client IP: 192.168.8.143
Please enter the server IP and press connect to start chatting...

a: 2827522060067017761968865238527324247048979867592152153034064046174979982922
47061287431664785178520503512359600063022198041814424508895118213155767157599885
92480920970617097898622139568997424735965838664134972808535522936026828244502932
71747534327411282242035238482427443029425243376289198679249618411183483734118084
98870276396300304511611572234209574725237387317060866076936093748302588569007613
257805049126337521220256676445004740885097608836689552495724941972229461045967287
71904943274520182878159155474616953691597587216160281016058086925318120988398106
0675130767308586147884673886132167712145391969063882042924572

RA: 940959082672396416707941976660584327867036266889664641153621521756951612517
38
RB: 688903360635561404428133738075847098298620183605136665181256522423518234599
53
k: 011fc7d287b068422f2a0a3903a748f1a3d51a4d12156d259651092a3343fbe4
IV: 669217b491a4d1cf30b51b4f0f87e2a1
Bob was authenticated
```



- After clicking connect, it will take few seconds (6 s) as delay for buffers to be loaded correctly.
- Alice prints the following (a, RA, RB, K, IV and if Bob was authenticated or not)
- Bob prints the following (b, RA, RB, K, IV and if Alice was authenticated or not)



```
C:\Windows\py.exe
Initializing....
Server IP: 192.168.8.144
Waiting for the client to call...

b: 2552904140391849401172999218891454080288993274508530908890141300225147919260
59004630966480083654220773825151081991549337929601934828694136326765156949006340
55090689893654886492332853563194055160473929093993945830937622383336620432033480
09585276365880092472069041223953664361878206918562110478098606509330207004563032
92588840524937624775290206358288413821378416680489018218344874816372932238683149
07467588608575909178194402412728888575390026869407282601513344206057671968337179
99251145211838154982968587781379297002163837138528774515335191905674101895690140
0506807509993082434764908121906975162749868891397977685124944

RA: 940959082672396416707941976660584327867036266889664641153621521756951612517
38
RB: 688903360635561404428133738075847098298620183605136665181256522423518234599
53
k: 011fc7d287b068422f2a0a3903a748f1a3d51a4d12156d259651092a3343fbe4
IV: 669217b491a4d1cf30b51b4f0f87e2a1

Alice was authenticated
```

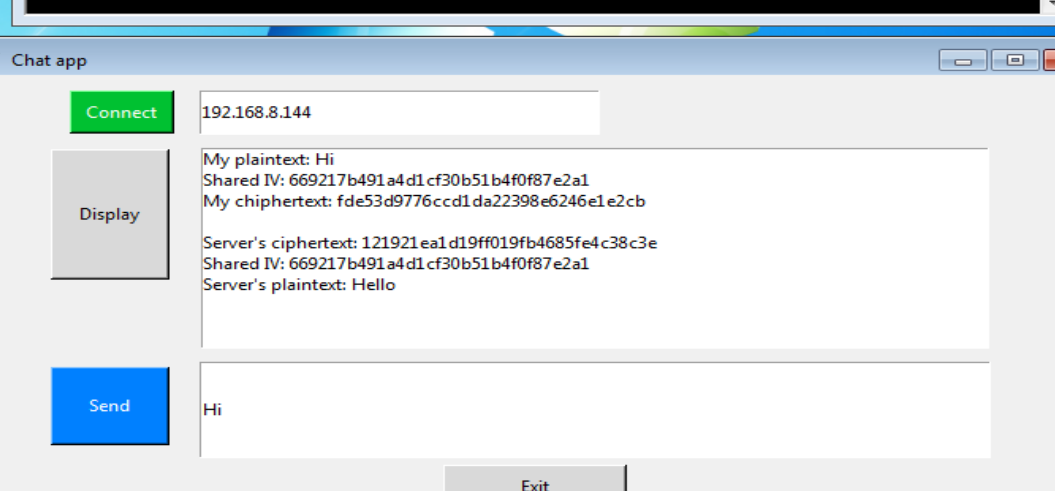
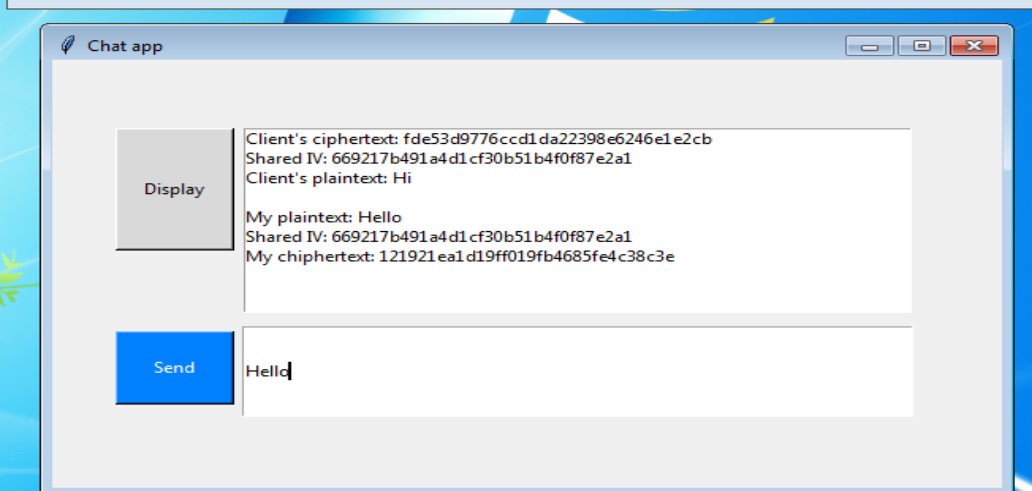
```
C:\Windows\py.exe
Client IP: 192.168.8.143

Please enter the server IP and press connect to start chatting...

a: 2827522060067017761968865238527324247048979867592152153034064046174979982922
47061287431664785178520503512359600063022198041814424500895118213155767157599885
92480920979617097898622139568997424735965838664134972808535522936026828244502932
71747534327411282242035238482427443029425243376289198679249618411183483734118084
98870276396300304511611572234209574725237387317060866076936093748302588569007613
25780504912633752122025667644500474088589760883668955249572494197229461045967287
71904943274520182878159155474616953691597587216160281016058086925318120988398106
0675130767308586147884673886132167712145391969063882042924572

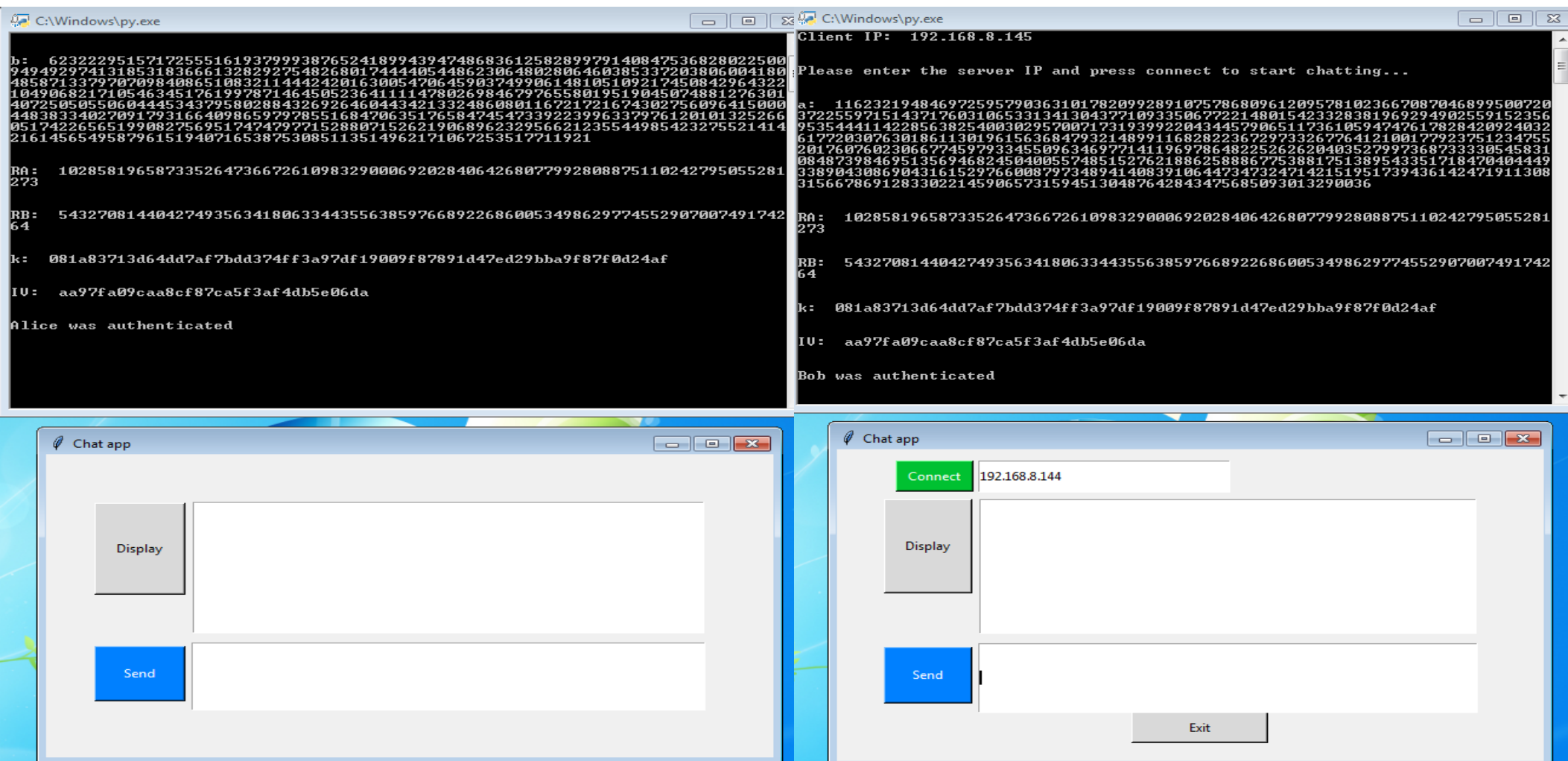
RA: 940959082672396416707941976660584327867036266889664641153621521756951612517
38
RB: 688903360635561404428133738075847098298620183605136665181256522423518234599
53
k: 011fc7d287b068422f2a0a3903a748f1a3d51a4d12156d259651092a3343fbe4
IV: 669217b491a4d1cf30b51b4f0f87e2a1

Bob was authenticated
```



- They can chat as in phase II but with the key k

## Test case 1\_Session 2:



- After clicking connect, as you can see the values have changed

```

C:\Windows\py.exe
b: 6232229515717255516193799938765241899439474868361258289979140847536828022500
94949297413185318366613282927548268017444405448623064802806460385337203806004180
48587133797070984086510832114442420163005470645903749906148105109217450842964322
10490682171054634517619978714645052364111147802698467976558019519045074881276301
4072505050604445343795802884326926460443421332486080116721721674302756096415000
44838334027091793166409865979785516847063517658474547339223996337976120101325266
05174226565199082756951747479771528807152621906896232956621235544985423275521414
216145654958796151940716538753085113514962171067253517711921

RA: 102858196587335264736672610983290006920284064268077992808875110242795055281
273

RB: 543270814404274935634180633443556385976689226860053498629774552907007491742
64

k: 081a83713d64dd7af7bdd374ff3a97df19009f87891d47ed29bba9f87f0d24af

IU: aa97fa09caa8cf87ca5f3af4db5e06da

Alice was authenticated

C:\Windows\py.exe
Client IP: 192.168.8.145

Please enter the server IP and press connect to start chatting...

a: 1162321948469725957903631017820992891075786809612095781023667087046899500720
37225597151437176031065331341304377109335067722148015423328381969294902559152356
95354441142285638254003029570071731939922043445790651173610594747617828420924032
61772030763018611301961563684793214899116828223672973326776412100177923751234755
2017607602306677459793345509634697714119697864822526262040352799736873330545831
08487398469513569468245040055748515276218862588867753881751389543351718470404449
33890430869043161529766008797348941408391064473473247142151951739436142471911308
3156678691283302214590657315945130487642843475685093013290036

RA: 102858196587335264736672610983290006920284064268077992808875110242795055281
273

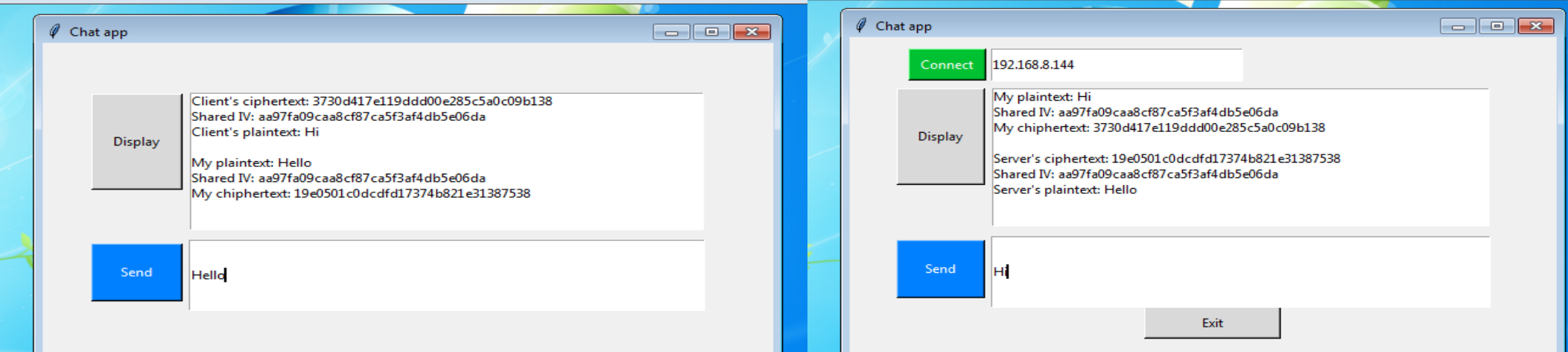
RB: 543270814404274935634180633443556385976689226860053498629774552907007491742
64

k: 081a83713d64dd7af7bdd374ff3a97df19009f87891d47ed29bba9f87f0d24af

IU: aa97fa09caa8cf87ca5f3af4db5e06da

Bob was authenticated

```



- They can chat as in phase II but with the key k

### Test case 1\_Session 3:

```
C:\Windows\py.exe
Initializing....
Server IP: 192.168.8.144
Waiting for the client to call...

b: 1772125174041072349095591244324112183144816788439698365250526948767913931706
1444665254847132836190615508583315261997345001213493170325304591930565522358844
32109100454012769514929188072415393683247827367534934261423827335048181102466168
59595309192709492530831366867664875151981463084839891571518344669131571062234280
63349577916370825198575506023562592476954455466468197469474820261224838990256726
92529712825911946611650444971311665517654532473354548735762775687709419490305105
41717233967382772312567363981926584542659215208615195754871082764361117403356851
4233598200202889534014150186425395617134786703838109985519226

RA: 589665523320632614562980350054125594490053565767429259929557266556251382071
6
RB: 544520198687852320574829265319351999860398017774930691739620424425874723311
32
k: c420267cee76cf37647a8657c05bfd584f52218f314030f22e171eadf0d46dd9
IU: 6cf2574f71d6ab7b4ba36c93f7af9bcb

Alice was authenticated
```

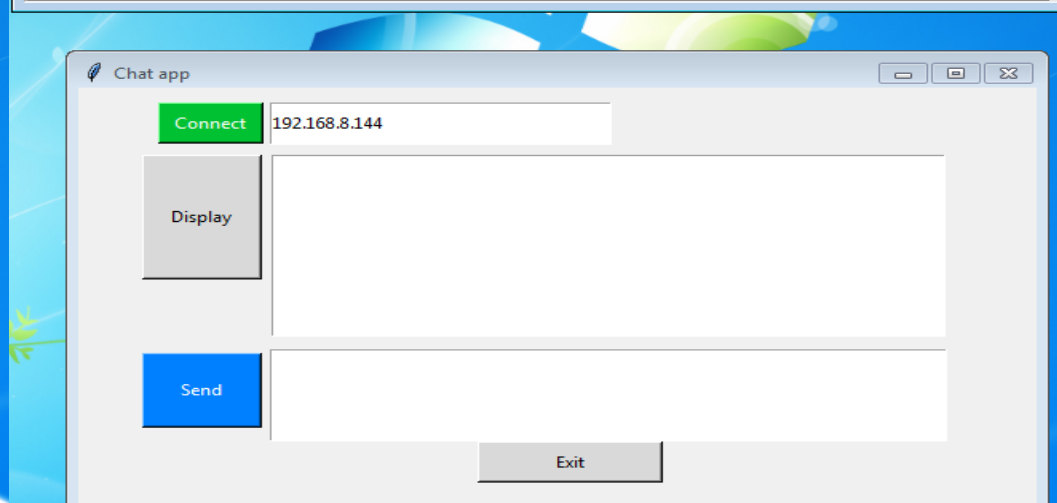
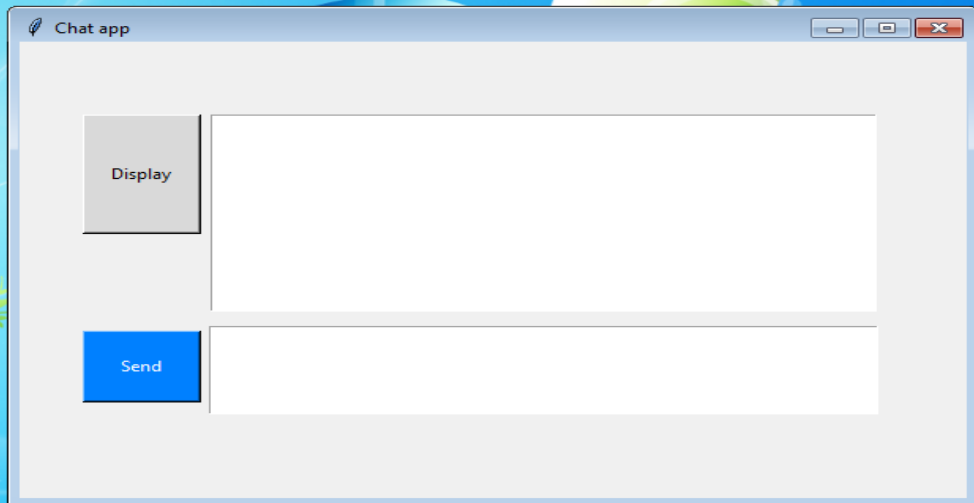
```
C:\Windows\py.exe
Client IP: 192.168.8.145

Please enter the server IP and press connect to start chatting...

a: 2180026910002092136511104355004634937097403352229363868216263527379251182737
13423647296527456578468505113351643143532834701828711957528767265705512719407366
54879573383814015835238456136962023548122486614636093167475339257005213848871517
88978324098029137338738371677421804704080428450080173446155842683584171046414700
89925354812154660264479781854479364455650781797336944233674568177722048190493259
67724522668356548348742639675465460633437768509595093347459324596107019644224242
6627377357159330009415081523759498635417966071478139477695573812957290713119072
8159196270910105315758713633143310682329578533685928667419340

RA: 589665523320632614562980350054125594490053565767429259929557266556251382071
6
RB: 544520198687852320574829265319351999860398017774930691739620424425874723311
32
k: c420267cee76cf37647a8657c05bfd584f52218f314030f22e171eadf0d46dd9
IU: 6cf2574f71d6ab7b4ba36c93f7af9bcb

Bob was authenticated
```



- After clicking connect, as you can see the values have changed

```
C:\Windows\py.exe
Initializing....
Server IP: 192.168.8.144
Waiting for the client to call...

b: 1772125174041072349095591244324112183144816788439698365250526948767913931706
14446652548471328361906155085833152619973450012134931703253045919305655522358844
32109100454012769514929188072415393683247827367534934261423827335048181102466168
59595309192709492530831366867664875151981463084839891571518344669131571062234280
63349577916370825198575506023562592476954455466468197469474820261224838990256726
22529712825911946611650444971311665517654532473354548757627756877094194905105
4171273396738277731256736398192658454265921520861519575487108276436117403356851
4233598200202889534014150186425395617134786703838109985519226

RA: 589665523320632614562980350054125594490053565767429259929557266556251382071
6
RB: 544520198687852320574829265319351999860398017774930691739620424425874723311
32
k: c420267cee76cf37647a8657c05bfd584f52218f314030f22e171eadf0d46dd9
IU: 6cf2574f71d6ab7b4ba36c93f7af9bcb

Alice was authenticated
```

```
C:\Windows\py.exe
Client IP: 192.168.8.145

Please enter the server IP and press connect to start chatting...

a: 2180026910002092136511104355004634937097403352229363868216263527379251182737
134236472296527456578468505113351643143532834701828711957528767265705512719407366
54879573383814015835238456136962023548122486614636093167475339257005213848871517
88978324098029137338738371677421804704080428450080173446155842683584171046414700
89925354812154660264479781854479364455650781797336944233674568177722048190493259
67724522668356548348742639675465460633437768509595093347459324596107019644224242
66273777357159330009415081523759498635417966071478139477695573812957290713119072
81591962709710105315758713633143310682329578533685928667419340

RA: 589665523320632614562980350054125594490053565767429259929557266556251382071
6
RB: 544520198687852320574829265319351999860398017774930691739620424425874723311
32
k: c420267cee76cf37647a8657c05bfd584f52218f314030f22e171eadf0d46dd9
IU: 6cf2574f71d6ab7b4ba36c93f7af9bcb

Bob was authenticated
```

Chat app

Display

Client's ciphertext: c92a9e3c861b468ffe2d6013b695676e  
Shared IV: 6cf2574f71d6ab7b4ba36c93f7af9bcb  
Client's plaintext: Hi  
  
My plaintext: Hello  
Shared IV: 6cf2574f71d6ab7b4ba36c93f7af9bcb  
My ciphertext: 983e13986cfe14975ae7dcf62f7cd698

Send

Hello

Chat app

Connect

192.168.8.144

Display

My plaintext: Hi  
Shared IV: 6cf2574f71d6ab7b4ba36c93f7af9bcb  
My ciphertext: c92a9e3c861b468ffe2d6013b695676e  
  
Server's ciphertext: 983e13986cfe14975ae7dcf62f7cd698  
Shared IV: 6cf2574f71d6ab7b4ba36c93f7af9bcb  
Server's plaintext: Hello

Send

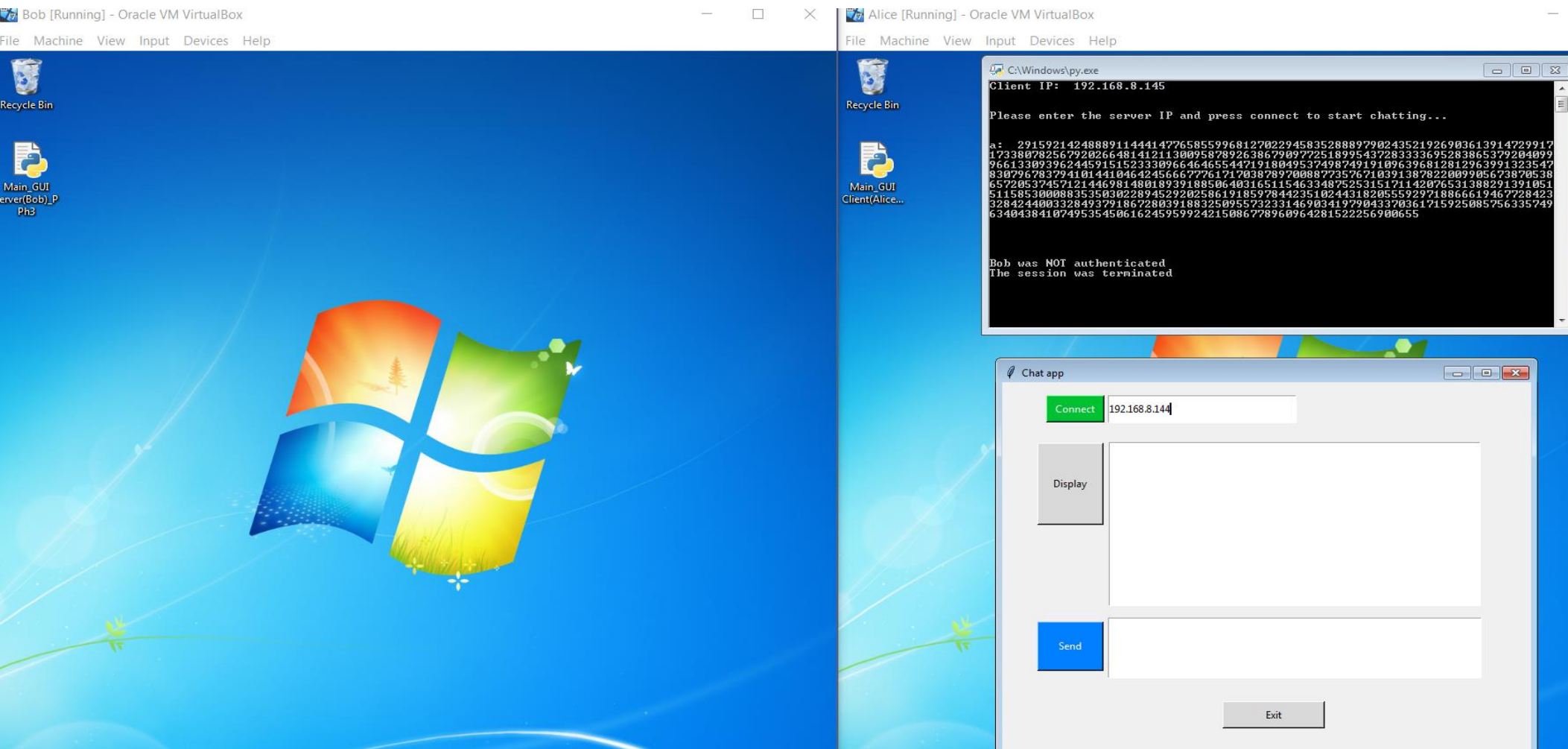
Hi

Exit

- They can chat as in phase II but with the key k



## Test case 2



- After connecting to Bob, the following will happen, (a) will be printed at Alice's side and (b) will be printed at Bob's side then the program find that H\_Bob is not as H then Alice will terminate the connection.

```
Python 3.8.6 Shell
File Edit Shell Debug Options Window Help
initializing....

Server IP: 192.168.8.144

Waiting for the client to call...

b: 7845198997250989345670884583642883691575036970071662386313642564729796710085
01985284658893079951446416821527348184977834582451758585165306002407917736425467
99025378145157875533217740321076510727774717234934827945596019539361192523656953
30969846558681351176480873962975323147882268756989243790999677319367442837830172
68150144417567984639809572520375659508258445712568226087243082844182382632477493
13078404010545010750353281943194005983507063397359452194857597553406109916934537
02793629329113703192167918067815401951160432774889764835158879447213030652602425
494003188652735465616768353035973823788297665842942311937166

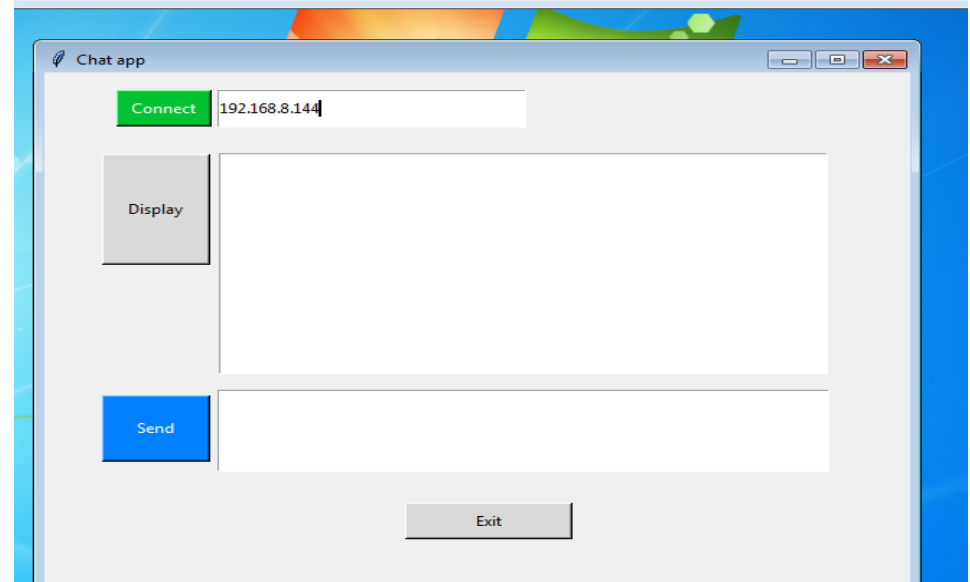
Traceback (most recent call last):
  File "C:\Users\BobAlice\Desktop\Main_GUI server(Bob)_PPH3.py", line 130, in <module>
    pt = unpad(cipher2.decrypt(ct),16)#----- The decryption of Alice's encrypted message
  File "C:\Users\BobAlice\AppData\Local\Programs\Python\Python38\lib\site-packages\Crypto\Util\Padding.py", line 88, in unpad
    padding_len = bord(padded_data[-1])
IndexError: index out of range
>>>
```

```
C:\Windows\py.exe
Client IP: 192.168.8.145

Please enter the server IP and press connect to start chatting...

a: 2915921424888911444147765855996812702294583528889790243521926903613914729917
17338078256792026648141211300958789263867909772518995437283333695283865379204099
96613309396244591515233309664646554471918049537498749191096396812812963991323547
3302967837941014410464245666776171703878970088773576710391387822009905673870538
65720537457121446981480189391885064031651154633487525315171142076531388291391051
51158530008835350302289452920258619185978442351024431820555929718866619467728423
32842440033284937918672803918832509557323314690341979043370361715925085756335749
6340438410749535450616245959924215086778960964281522256900655

Bob was NOT authenticated
The session was terminated
```



- The same as above but on the shell, so you can see b was printed and the error shown is due to the termination from Alice's side.

## Test case 3

```
C:\Windows\py.exe
Initializing....
Server IP: 192.168.8.144
Waiting for the client to call...

h: 1553841402750753701509734392972117069273386574354888155050715999272889245061
08306700824432999036706611815340101469962261836075442829571893819569671596447423
54663613313039176606398048948903064307070105831552668467847223348556426680548560
4501817976065933246660597970027502156641905452106309316874705595987810139653161
29147634391307807922050375249866605422367543853446474108105869883863689376631200
65477702092562377358939388064452044566323471090098467267116601658360998313910807
7362528282562820510306857024567912941960732701970335294178684888278004947623712
3416962903381424074583720064258132321969940753621376768680649

Alice was NOT authenticated
The session was terminated
```

```
C:\Windows\py.exe

a: 2611735594399089091415055290433368978404912081335432792584381145135785200748
17778948489327607638440363433617064149864233655485161889958280981125196307974874
97548310891397395231371330486325713208098663098031528336391163291931885374714420
34668568824751690295842608424294212098142403344309380935174275011313676153669084
56422856860258552239556649946571356182981464687690630001161783003282614008064995
1977086473592260807449009631306517800612462765514678986039398058858106892881254
91516669258857409519003855926349963212588688612755569404986356433883524077363594
316183307577756725945351450562071935945885116609399005113184

Ra: 226290390603077223680703846993882933093656952261479594702308388609812286983
23

RB: 771836877922761215315308401576211653399800453735883530217110286868200509057
6

k: 36a43066c7a739b99c7fb76c0b1ff299f6759c4d694d259999de27b14e4e60bb

IU: 14045b02dd6de373c51c28066537ece5

Bob was authenticated
```

Chat app

Display

Send

Chat app

Connect 192.168.8.144

Display

Send

Exit

- Bob was authenticated by Alice but Alice was not authenticated by Bob so the connection was terminated by Bob after Bob had compared  $H_{\text{Alice}}$  with  $H$  and he found it not matching.