Name: Hasan Mahdi Alhussain **ID:201729330**

Mini-Programming Project-Phase III

This mini-programming project is related to a client-server file transfer application that is built using Python. It uses TCP connection as a transport layer to send and receive files from a server. There are a menu shows up and has three choices for the user, get, put, and quiet. However, it is tested on two machines, each one has its IP-address and the server's IP-addresses will be hardcoded to the client, so that it connects to the server immediately. This short report will show screenshots of testing the application after adding authentication part in phase 3 of the project.

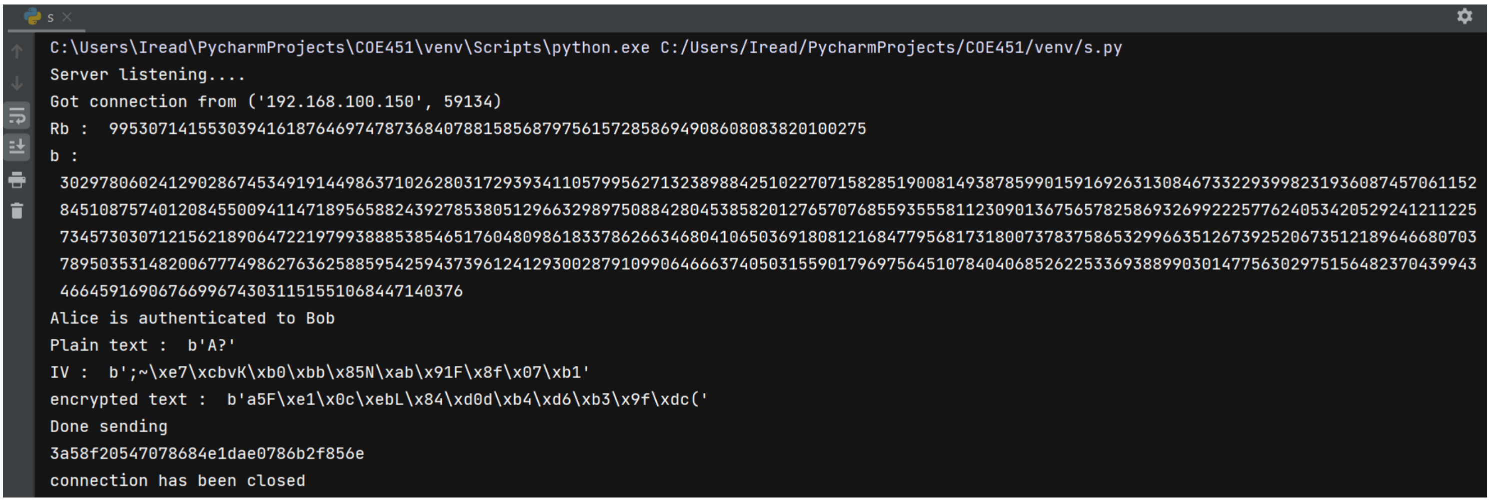
Note: In all test cases the server has an IP-address 192.168.100.6, and the client has IPaddress 192.168.100.150. Also, this application can be tested on virtual machines. Only it needs to hardcode the IP address of the server. Preferable, run the code on Pycharm IDE.

Note: the key is printed after the user chooses quiet (choice 3).

Test case 1:

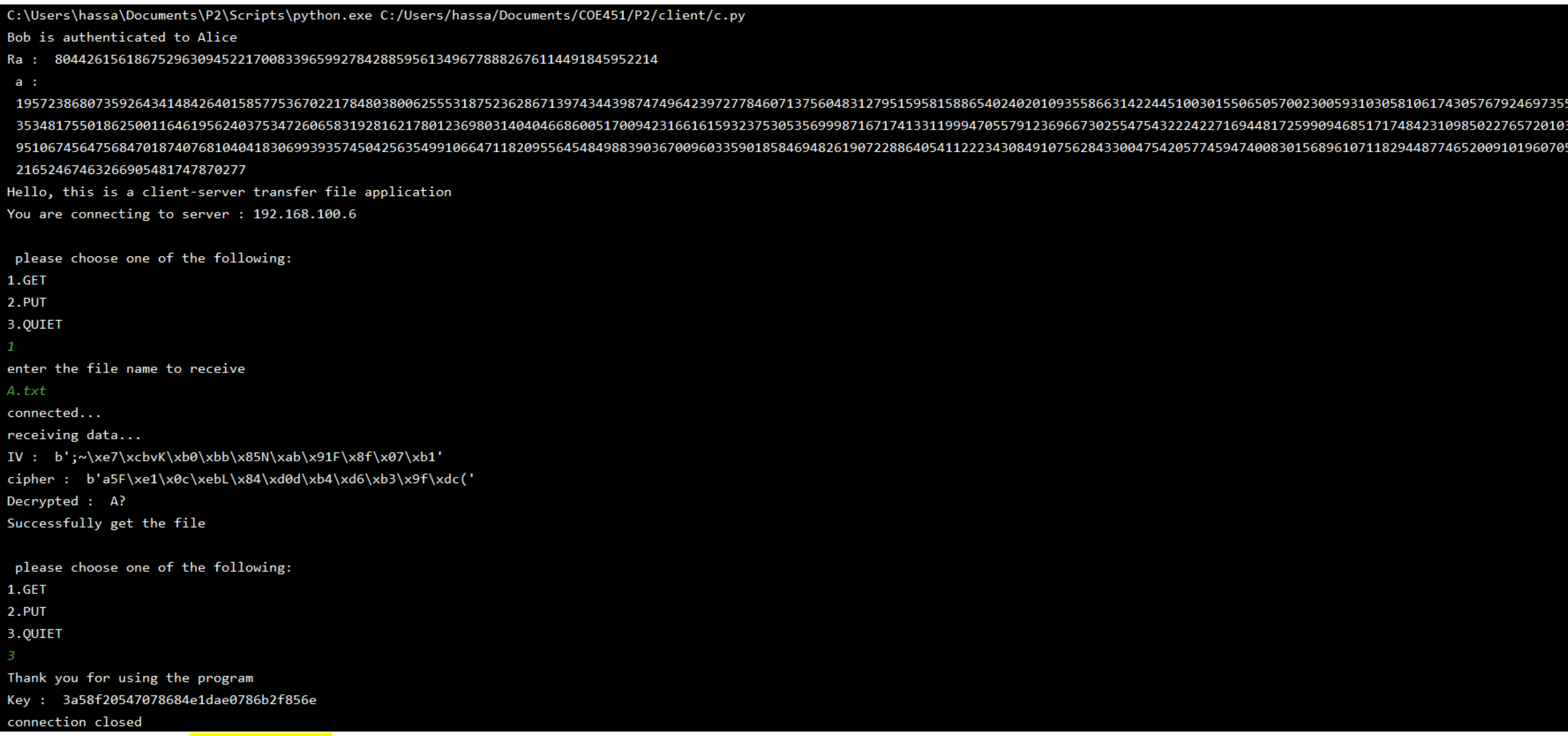
Session 1:

Server side



```
C:\Users\Iread\PycharmProjects\COE451\venv\Scripts\python.exe C:/Users/Iread/PycharmProjects/COE451/venv/s.py
Server listening....
Got connection from ('192.168.100.150', 59134)
Rb :  99530714155303941618764697478736840788158568797561572858694908608083820100275
b :
 302978060241290286745349191449863710262803172939341105799562713238988425102270715828519008149387859901591692631308467332293998231936087457061152
 845108757401208455009411471895658824392785380512966329897508842804538582012765707685593555811230901367565782586932699222577624053420529241211225
 734573030712156218906472219799388853854651760480986183378626634680410650369180812168477956817318007378375865329966351267392520673512189646680703
 789503531482006777498627636258859542594373961241293002879109906466637405031559017969756451078404068526225336938899030147756302975156482370439943
 46645916906766996743031151551068447140376
Alice is authenticated to Bob
Plain text :  b'A?'
IV :  b';~\xe7\xcbvK\xb0\xbb\x85N\xab\x91F\x8f\x07\xb1'
encrypted text :  b'a5F\xe1\x0c\xebL\x84\xd0d\xb4\xd6\xb3\x9f\xdc('
Done sending
3a58f20547078684e1dae0786b2f856e
connection has been closed
```

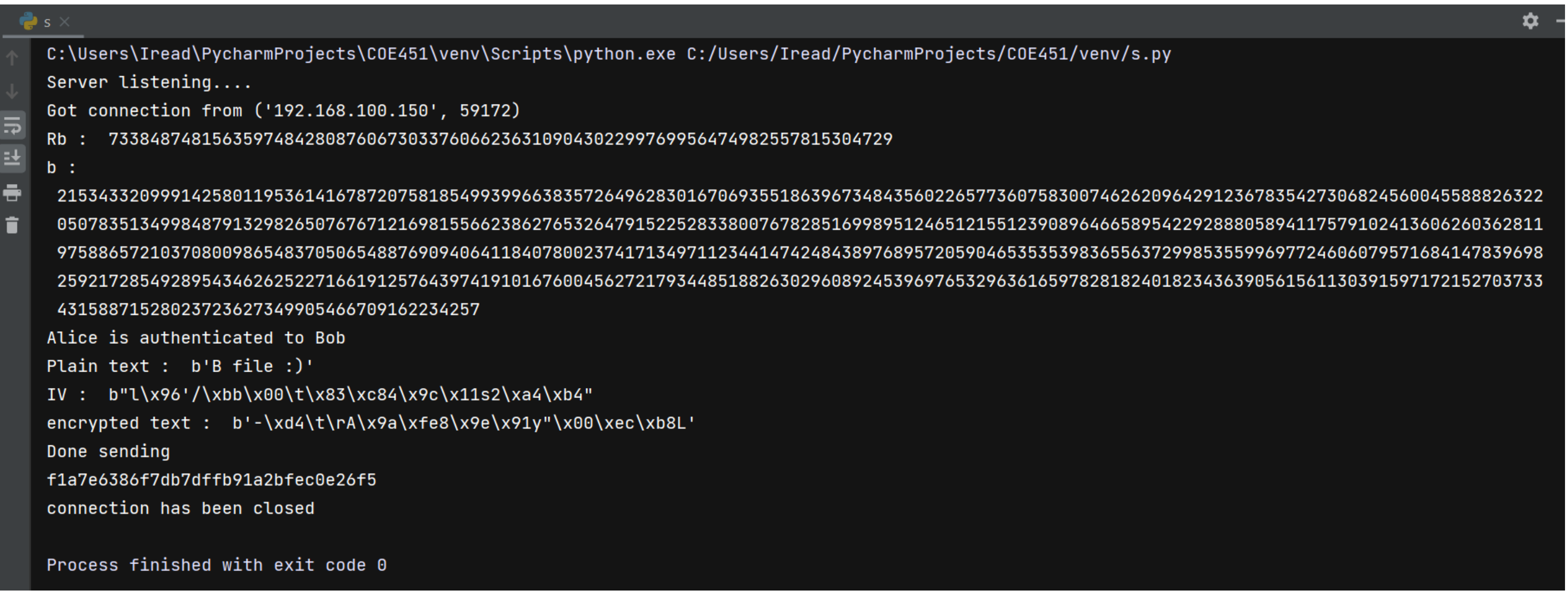
Client side



```
C:\Users\hassa\Documents\P2\Scripts\python.exe C:/Users/hassa/Documents/COE451/P2/client/c.py
Bob is authenticated to Alice
Ra :  80442615618675296309452217008339659927842885956134967788826761144918459522 14
 a :
 1957238680735926434148426401585775367022178480380062555318752362867139743443987474964239727784607137560483127951595815886540240201093558663142244510030155065057002300593103058106174305767924697355
 3534817550186250011646195624037534726065831928162178012369803140404668600517009423166161593237530535699987167174133119994705579123696673025547543222422716944817259909468517174842310985022765720103
 9510674564756847018740768104041830699393574504256354991066471182095564548498839036700960335901858469482619072288640541122234308491075628433004754205774594740083015689610711829448774652009101960705
 21652467463266905481747870277
Hello, this is a client-server transfer file application
You are connecting to server : 192.168.100.6

 please choose one of the following:
1.GET
2.PUT
3.QUIET
1
enter the file name to receive
A.txt
connected...
receiving data...
IV :  b';~\xe7\xcbvK\xb0\xbb\x85N\xab\x91F\x8f\x07\xb1'
cipher :  b'a5F\xe1\x0c\xebL\x84\xd0d\xb4\xd6\xb3\x9f\xdc('
Decrypted :  A?
Successfully get the file

 please choose one of the following:
1.GET
2.PUT
3.QUIET
3
Thank you for using the program
Key :  3a58f20547078684e1dae0786b2f856e
connection closed
```

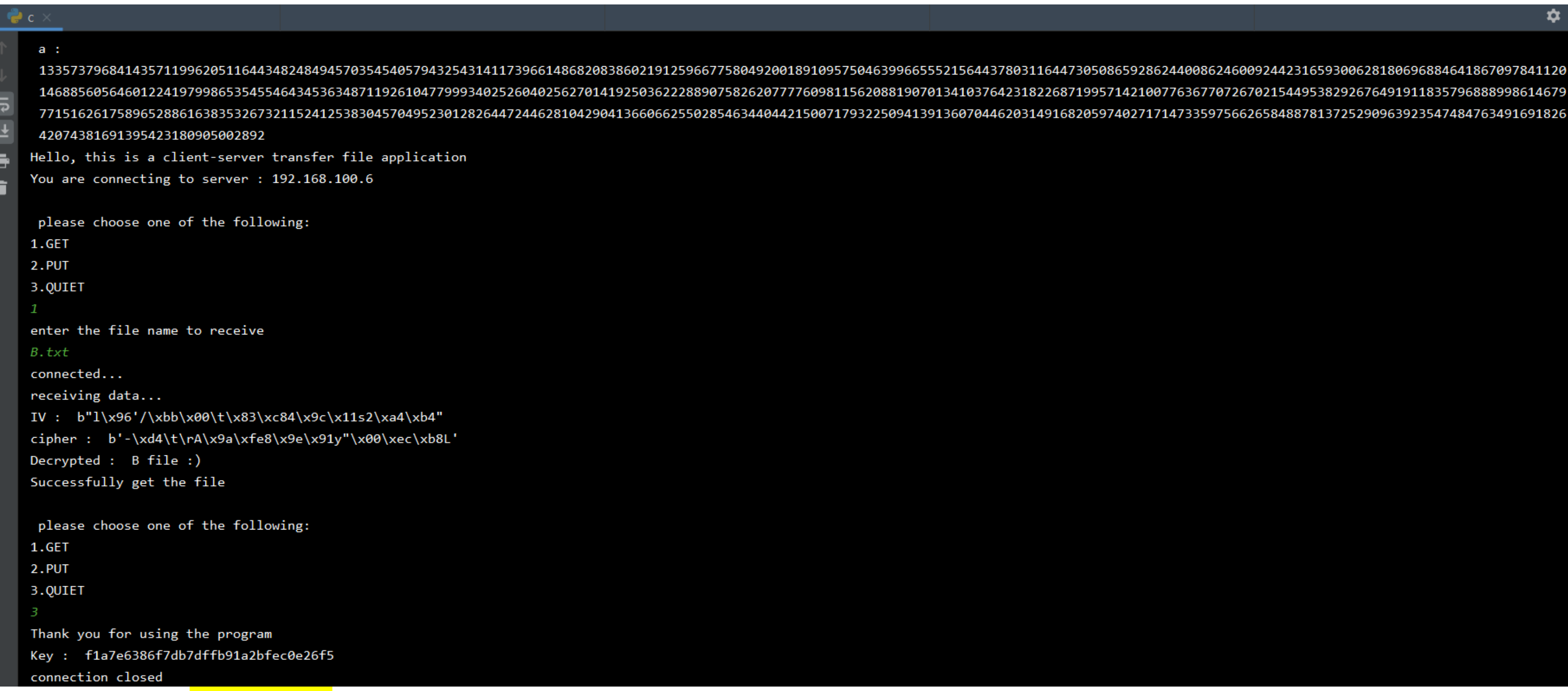
Session 2

Server side



```
C:\Users\Iread\PycharmProjects\COE451\venv\Scripts\python.exe C:/Users/Iread/PycharmProjects/COE451/venv/s.py
Server listening....
Got connection from ('192.168.100.150', 59172)
Rb :  73384874815635974842808760673033760662363109043022997699564749825578153047 29
b :
 215343320999142580119536141678720758185499399663835726496283016706935518639673484356022657736075830074626209642912367835427306824560045588826322
 050783513499848791329826507676712169815566238627653264791522528338007678285169989512465121551239089646658954229288805894117579102413606260362811
 975886572103708009865483705065488769094064118407800237417134971123441474248438976895720590465353539836556372998535599697724606079571684147839698
 259217285492895434626252271661912576439741910167600456272179344851882630296089245396976532963616597828182401823436390561561130391597172152703733
 43158871528023723627349905466709162234257
Alice is authenticated to Bob
Plain text :  b'B file :)'
IV :  b"l\x96'/\xbb\x00\t\x83\xc84\x9c\x11s2\xa4\xb4"
encrypted text :  b'-\xd4\t\rA\x9a\xfe8\x9e\x91y"\x00\xec\xb8L'
Done sending
f1a7e6386f7db7dffb91a2bfec0e26f5
connection has been closed

Process finished with exit code 0
```

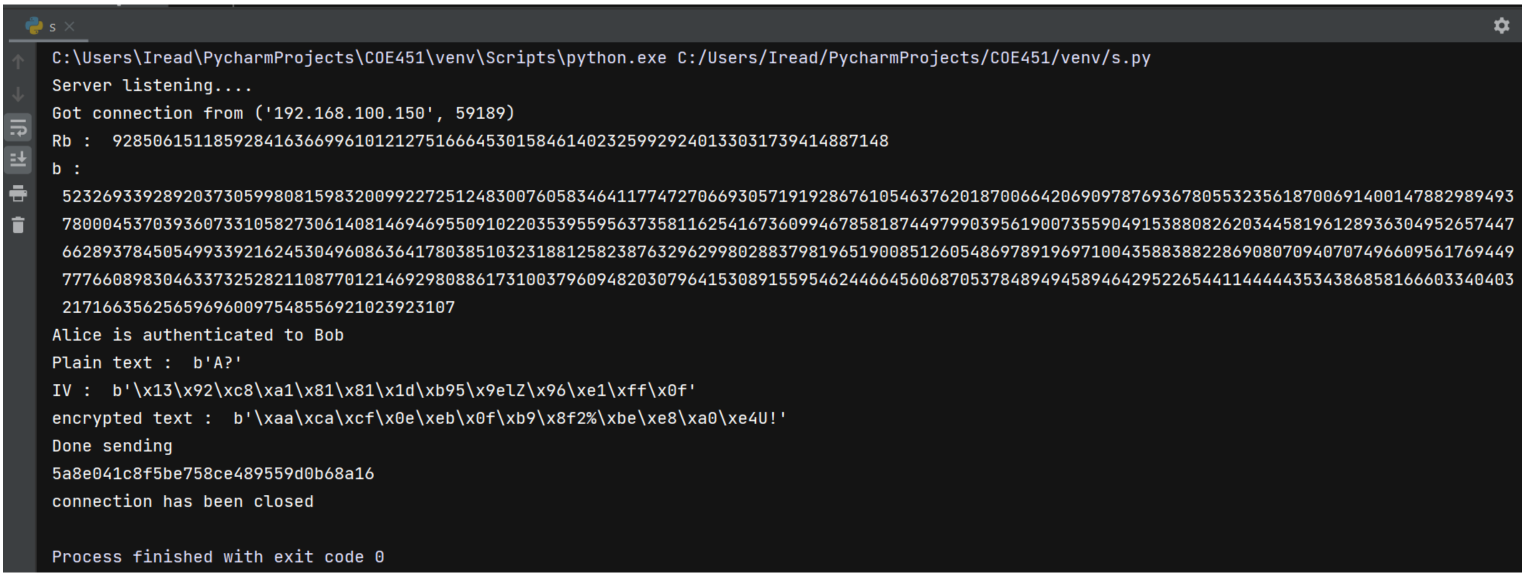
Client side



```
 a :
 1335737968414357119962051164434824849457035454057943254314117396614868208386021912596677580492001891095750463996655521564437803116447305086592862440086246009244231659300628180696884641867097841120
 1468856056460122419799865354554643453634871192610477999340252604025627014192503622288907582620777760981156208819070134103764231822687199571421007763677072670215449538292676491911835796888998614679
 7715162617589652886163835326732115241253830457049523012826447244628104290413660662550285463440442150071793225094139136070446203149168205974027171473359756626584887813725290963923547484763491691826
 42074381691395423180905002892
Hello, this is a client-server transfer file application
You are connecting to server : 192.168.100.6

 please choose one of the following:
1.GET
2.PUT
3.QUIET
1
enter the file name to receive
B.txt
connected...
receiving data...
IV :  b"1\x96'/\xbb\x00\t\x83\xc84\x9c\x11s2\xa4\xb4"
cipher :  b'-\xd4\t\rA\x9a\xfe8\x9e\x91y"\x00\xec\xb8L'
Decrypted :  B file :)
Successfully get the file

 please choose one of the following:
1.GET
2.PUT
3.QUIET
3
Thank you for using the program
Key :  f1a7e6386f7db7dffb91a2bfec0e26f5
connection closed
```

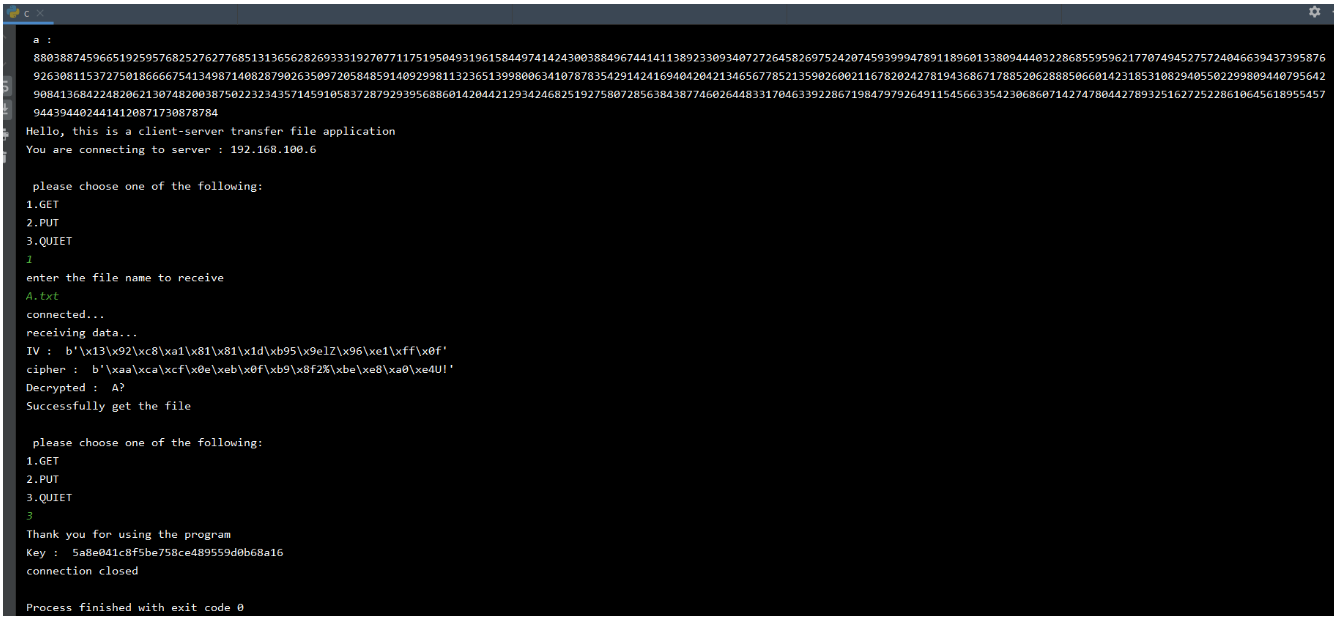
Session 3

Server side



```
C:\Users\Iread\PycharmProjects\COE451\venv\Scripts\python.exe C:/Users/Iread/PycharmProjects/COE451/venv/s.py
Server listening....
Got connection from ('192.168.100.150', 59189)
Rb :  928506151185928416366996101212751666453015846140232599292401330317394148871 48
b :
 52326933928920373059980815983200992272512483007605834641177472706693057191928676105463762018700664206909787693678055323561870069140014788298 9493
 780004537039360733105827306140814694695509102203539559563735811625416736099467858187449799039561900735590491538808262034458196128936304952657447
 662893784505499339216245304960863641780385103231881258238763296299802883798196519008512605486978919697100435883882286908070940707496609561769449
 777660898304633732528211087701214692980886173100379609482030796415308915595462446645606870537848949458946429522654411444443534386858166603340403
 21716635625659696009754855692102392310 7
Alice is authenticated to Bob
Plain text :  b'A?'
IV :  b'\x13\x92\xc8\xa1\x81\x81\x1d\xb95\x9elZ\x96\xe1\xff\x0f'
encrypted text :  b'\xaa\xca\xcf\x0e\xeb\x0f\xb9\x8f2%\xbe\xe8\xa0\xe4U!'
Done sending
5a8e041c8f5be758ce489559d0b68a16
connection has been closed

Process finished with exit code 0
```

Client side

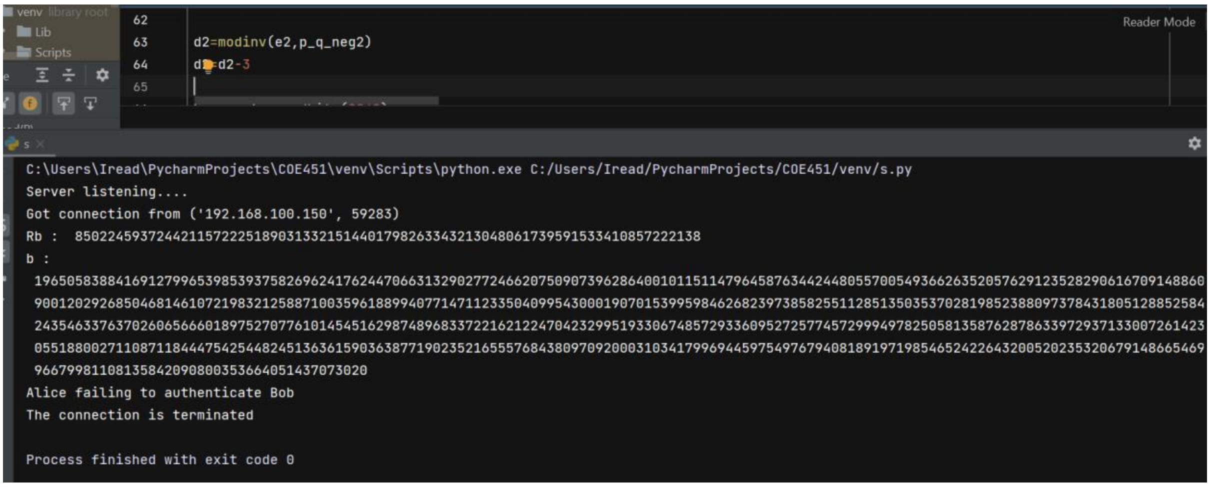


```
 a :
 8803887459665192595768252762776851313656282693331927077117519504931961584497414243003884967441411389233093407272645826975242074593999478911896013380944403228685595962177074945275724046639437395876
 9263081153727501866667541349871408287902635097205848591409299811323651399800634107878354291424169404204213465677852135902600211678202427819436867178852062888506601423185310829405502299809440795642
 9084136842248206213074820038750223234357145910583728792939568860142044212934246825192758072856384387746026448331704633922867198479792649115456633542306860714274780442789325162725228610645618955457
 9443944024414120871730878784
Hello, this is a client-server transfer file application
You are connecting to server : 192.168.100.6

 please choose one of the following:
1.GET
2.PUT
3.QUIET
1
enter the file name to receive
A.txt
connected...
receiving data...
IV :  b'\x13\x92\xc8\xa1\x81\x81\x1d\xb95\x9elZ\x96\xe1\xff\x0f'
cipher :  b'\xaa\xca\xcf\x0e\xeb\x0f\xb9\x8f2%\xbe\xe8\xa0\xe4U!'
Decrypted :  A?
Successfully get the file

 please choose one of the following:
1.GET
2.PUT
3.QUIET
3
Thank you for using the program
Key :  5a8e041c8f5be758ce489559d0b68a16
connection closed

Process finished with exit code 0
```

Test case 2 – Trudy posing as Bob

Bob acting as a Trudy is done via subtracting the private key by 3.

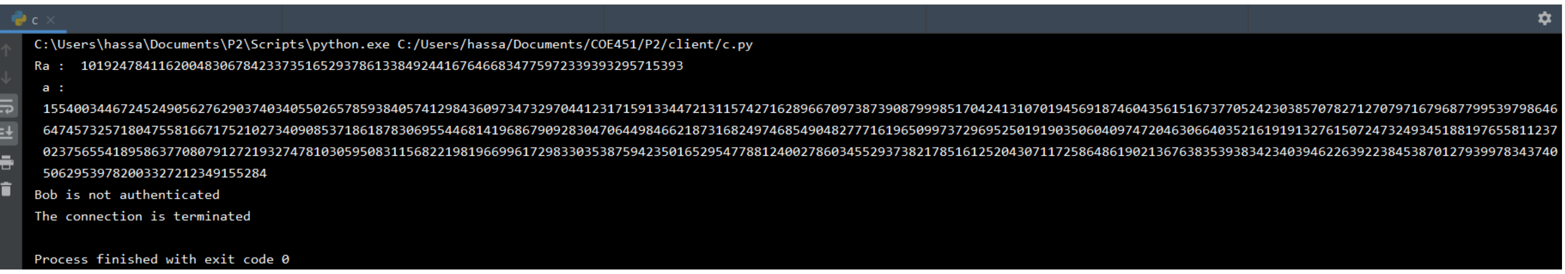
SERVER SIDE



```
d2=modinv(e2,p_q_neg2)
d2=d2-3
```

```
C:\Users\Iread\PycharmProjects\COE451\venv\Scripts\python.exe C:/Users/Iread/PycharmProjects/COE451/venv/s.py
Server listening....
Got connection from ('192.168.100.150', 59283)
Rb :  85022459372442115722251890313321514401798263343213048061739591533410857222138
b :
 196505838841691279965398539375826962417624470663132902772466207509073962864001011511479645876344244805570054936626352057629123528290616709148860
 900120292685046814610721983212588710035961889940771471123350409954300019070153995984626823973858255112851350353702819852388097378431805128852584
 243546337637026065666018975270776101454516298748968337221621224704232995193306748572933609527257745729994978250581358762878633972937133007261423
 055188002711087118444754254482451363615903638771902352165557684380970920003103417996944597549767940818919719854652422643200520235320679148665469
 96679981108135842090800353664051437073020
Alice failing to authenticate Bob
The connection is terminated

Process finished with exit code 0
```

Client side

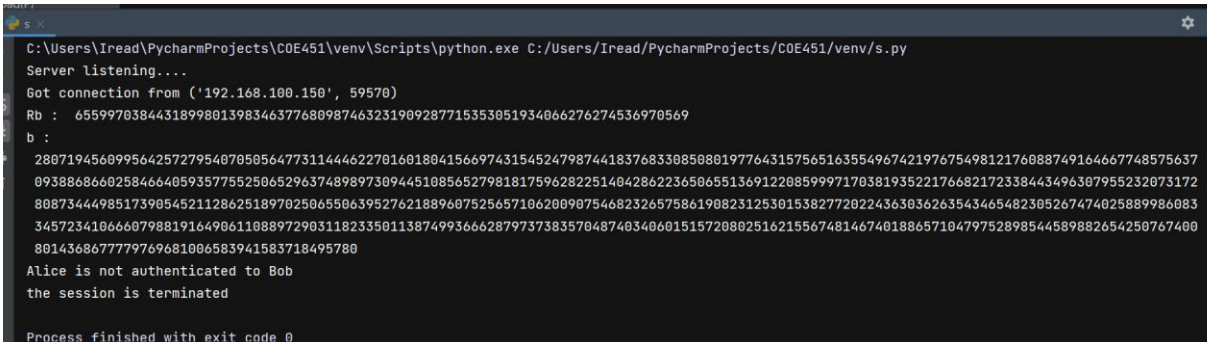


```
C:\Users\hassa\Documents\P2\Scripts\python.exe C:/Users/hassa/Documents/COE451/P2/client/c.py
Ra :  101924784116200483067842337351652937861338492441676466834775972339393295715393
 a :
 1554003446724524905627629037403405502657859384057412984360973473297044123171591334472131157427162896670973873908799985170424131070194569187460435615167377052423038570782712707971679687799539798646
 6474573257180475581667175210273409085371861878306955446814196867909283047064498466218731682497468549048277716196509973729695250191903506040974720463066403521619191327615072473249345188197655811237
 0237565541895863770807912721932747810305950831156822198196699617298330353875942350165295477881240027860345529373821785161252043071172586486190213676383539383423403946226392238453870127939978343740
 50629539782003327212349155284
Bob is not authenticated
The connection is terminated

Process finished with exit code 0
```

Test case 3-Trudy posing as Alice

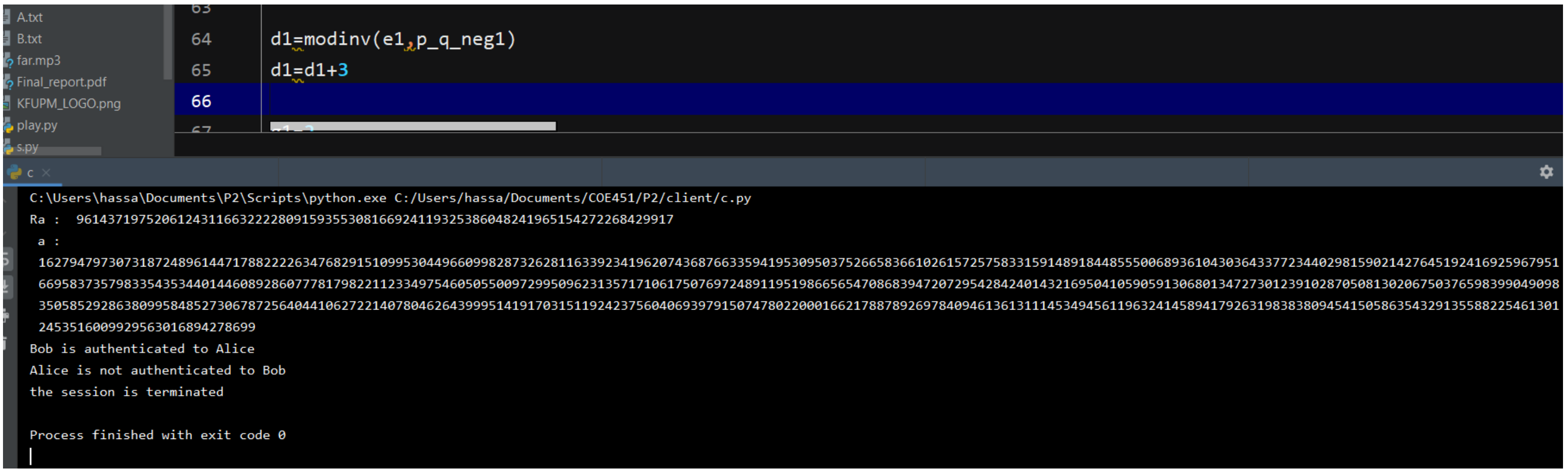
This test is changing the private key of Alice by adding 3 to it, as shown below in the client side.

Server side



```
C:\Users\Iread\PycharmProjects\COE451\venv\Scripts\python.exe C:/Users/Iread/PycharmProjects/COE451/venv/s.py
Server listening....
Got connection from ('192.168.100.150', 59570)
Rb :  655997038443189980139834637768098746323190928771535305193406627627453697056 9
b :
 28071945609956425727954070505647731144462270160180415669743154524798744183768330850801977643157565163554967421976754981217608874916466774857563 7
 09388686602584664059357755250652963748989730944510856527981817596282251404286223650655136912208599971703819352217668217233844349630795523207317 2
 80873444985173905452112862518970250655063952762188960752565710620090754682326575861908231253015382772022436303626354346548230526747402588998608 3
 34572341066607988191649061108897290311823350113874993666287973738357048740340601515720802516215567481467401886571047975289854458988265425076740 0
 801436867777976968100658394158371849578 0
Alice is not authenticated to Bob
the session is terminated

Process finished with exit code 0
```

Client side



```
d1=modinv(e1,p_q_neg1)
d1=d1+3
```

```
C:\Users\hassa\Documents\P2\Scripts\python.exe C:/Users/hassa/Documents/COE451/P2/client/c.py
Ra :  96143719752061243116632222809159355308166924119325386048241965154272268429917
 a :
 16279479730731872489614471788222263476829151099530449660998287326281163392341962074368766335941953095037526658366102615725758331591489184485550068936104303643377234402981590214276451924169259679 51
 66958373579833543534401446089286077781798221123349754605055009729950962313571710617507697248911951986656547086839472072954284240143216950410590591306801347273012391028705081302067503765983990490 98
 35058529286380995848527306787256404410627221407804626439995141917031511924237560406939791507478022000166217887892697840946136131114534945611963241458941792631983838094541505863543291355882254613 01
 245351600992956301689427869 9
Bob is authenticated to Alice
Alice is not authenticated to Bob
the session is terminated

Process finished with exit code 0
```